Nottinghamshire County Council

Information Compliance Policy

Introduction

1. This policy sets out Nottinghamshire County Council's (the Council's) approach to ensuring compliance with information governance (IG) requirements. It defines the expectations for managing information lawfully, responsibly and in line with regulatory, organisational and ethical obligations.

2. It supports the Information Governance Framework and should be read alongside the Information Rights Policy and Information Security Policy. Detailed operational requirements are set out in supporting standards, procedures and guidance

Scope

3. This policy applies to all elected members, employees, trainees, volunteers, contractors, suppliers and partners who process information on behalf of the Council.

4. It applies to all information held by the Council, regardless of format or location.

5. Elected members should note that, in relation to their constituency duties, they act as independent data controllers. In this capacity, they are responsible for ensuring that any personal data they process is handled in accordance with applicable data protection legislation.

6. Schools are independent data controllers and are responsible for their own compliance with relevant legislation.

Definitions

7. For the purposes of this policy:

   - **Information** includes data, records, documents and content, regardless of format or location.
   - **Personal data** means any information relating to an identified or identifiable living individual.
   - **Processing** means any use of personal data, including collection, storage, use, sharing or disposal.

- **The Council** refers to Nottinghamshire County Council and those acting on its behalf, except where individuals are acting as independent data controllers (for example, elected members carrying out constituency duties).

Policy Principles

8. This policy is underpinned by the Council's Information Governance Principles. All information must be:

   a) Processed lawfully, fairly and transparently
   b) Collected for specified, explicit purposes and limited to what is necessary
   c) Accurate, up to date and fit for purpose
   d) Protected through appropriate security and resilience measures
   e) Managed throughout its lifecycle from creation to disposal
   f) Accountable, with clear ownership and auditability
   g) Used responsibly to support service delivery and public trust.

Governance and Accountability

9. The Council operates a defined governance structure for managing information risk and compliance, as set out in the Information Governance Framework, with clear roles and accountability across all levels.

10. Compliance is overseen through corporate governance arrangements, including reporting to the Information Governance and Cyber Security Board.

11. The Council will establish, maintain and communicate standards, procedures and guidance to support the effective implementation of this policy and ensure ongoing compliance with information governance requirements.

Managing information

Collection and use

12. The Council will maintain an up-to-date entry in the register of data controllers (or any successor register required by the relevant regulatory authority, currently the Information Commissioner's Office) and ensure that its registered details accurately reflect its processing activities.

13. Information must only be collected and used only where there is a clear legal basis and business need. Only the minimum amount of personal data necessary for a particular purpose must be collected and used.

14. Privacy risks must be formally identified, assessed and documented for all new or changed systems, services or processes that involve the use of personal data. This will be undertaken through the Council's Data Protection Impact Assessment (DPIA) process, which provides a mechanism for assessing and triaging risk, and ensures that higher-risk processing is subject to more detailed evaluation and governance oversight.

15. The Council will ensure that clear and accessible privacy information is made available to individuals, explaining how their personal data is collected, used and shared, and the rights available to them.

Information quality and records

16. Information must be accurate, relevant and maintained to support its intended use. The Council will take reasonable steps to ensure that personal data is accurate, up to date and not misleading. Where opinions or intentions about individuals are recorded, this must be done carefully, objectively and professionally, in line with Council standards.

17. The Council will maintain an Information and Processing Register (IPR) which fulfils its obligation to maintain records of processing activities (ROPA) in line with data protection legislation. The register supports the Council's ability to demonstrate compliance and must be kept accurate and up to date by services.

18. The Council will also maintain a record of systems used to process personal data.

Storage and security

19. Information must only be stored in approved systems and locations. Security requirements are defined in the Information Security Policy and associated standards, including the Acceptable Use Standard.

20. Information should be classified and handled in accordance with its sensitivity, value and risk, in line with the Council's standards and guidance.

21. Personal and confidential information must be handled securely at all times, including when working in offices, public locations, from home or in transit. Such information must only be disclosed or discussed where there is a legitimate business need and in the course of authorised duties.

22. Access to personal and confidential information must be limited to those with a legitimate business need and only where necessary to carry out their role. Staff and those working on the Council's behalf must not access or attempt to access information unless they are authorised to do so.

23. Access to systems and information must be appropriately managed throughout the employment lifecycle. This includes ensuring that access rights are granted, reviewed and removed in a timely manner, particularly when individuals change roles or leave the Council. Managers and system owners are responsible for ensuring that access permissions remain appropriate and reflect current duties.

24. Council information and equipment must be kept secure at all times, including when used outside Council premises. All use of Council IT equipment must be in accordance with the Council's standards, including acceptable use requirements, and appropriate steps must be taken to prevent unauthorised access or security threats.

25. Staff and managers must ensure that Council information and equipment are appropriately managed and returned when no longer required.

Sharing and disclosure

26. Information must only be shared where there is a lawful basis and a clear business need, including to support the effective delivery of services. Sharing must be undertaken in a secure, proportionate and consistent manner in line with Council standards and procedures.

27. Where regular or routine sharing is taking place, Information Sharing Agreements (ISAs) must be in place to govern the sharing of personal data, and the terms of those agreements must be adhered to.

28. Where personal data is shared on a one-off or non-routine basis, appropriate records must be maintained to document the purpose of the sharing, the information disclosed, the recipient, and the lawful basis for the disclosure. This will ensure that such sharing is transparent, justified and can be reviewed where necessary.

29. Personal data must not be transferred outside the United Kingdom unless this is permitted under data protection legislation and appropriate safeguards are in place. Where international transfers are required, appropriate advice must be sought and risks assessed, including through the use of Data Protection Impact Assessments (DPIAs).

30. The Council will provide access to information in accordance with its legal obligations. This includes enabling individuals to exercise their rights in relation to their personal data under data protection legislation and

responding to requests for recorded information under access to information legislation.

31. The Council will also make certain information publicly available in line with its transparency obligations and publication arrangements.

32. Personal data will only be disclosed where this is lawful and appropriate.

33. Further detail on how requests are handled is set out in the Information Rights Policy and supporting procedures.

Retention and disposal

34. The Council will maintain, and periodically review, its Records Retention and Disposal Schedule which will reflect legal, regulatory and business requirements. Information must be retained only for as long as necessary and in accordance with the Schedule.

35. Services must ensure that information is retained and disposed of in line with the Schedule, including any specific retention requirements arising from statutory inquiries or other obligations.

36. Records that are no longer in active use but require ongoing retention must be managed appropriately. Physical records not in active use must be transferred to the Council's Records Management Service for secure off-site storage, unless alternative arrangements have been formally approved.

37. Information must be disposed of securely and appropriately at the end of its lifecycle, in accordance with Council standards and procedures.

Surveillance and CCTV

38. The use of surveillance camera systems (including CCTV, body worn cameras, drones and other recording technologies) involves the processing of personal data and must comply with data protection legislation and Council requirements.

39. Such systems must be used only where necessary and proportionate to achieve a legitimate purpose, and must be subject to appropriate assessment, including a Data Protection Impact Assessment (DPIA). Further detail is set out in the Council's Surveillance Camera and Drone procedures and associated guidance.

Risk management, information incidents and data breaches

40. Information risks relating to the use, sharing and management of information must be identified, assessed and managed appropriately within services.

41. Information incidents and personal data breaches can arise from a wide range of situations, including loss or theft of equipment or documents, unauthorised access to information, or the accidental or deliberate destruction or disclosure of data.

42. All actual or suspected information incidents, including personal data breaches, must be reported immediately in accordance with the Council's breach and incident procedures. This includes any loss of information or equipment, unauthorised access, or other events that may compromise the confidentiality, integrity or availability of information.

43. Reported incidents will be assessed and investigated to determine their cause, impact and severity, including whether they meet the threshold for regulatory reporting under data protection legislation.

44. Appropriate remedial action will be taken to mitigate risks and prevent recurrence. Learning from incidents will be used to inform improvements to processes, controls and staff awareness.

45. Information incidents and data breaches will be treated seriously. Failure to comply with information governance requirements, including failure to report incidents, may result in disciplinary action.

Third parties and service delivery

46. Where information is processed by third parties on behalf of the Council, appropriate contractual, security and governance controls must be in place.

47. Services must ensure that third-party arrangements comply with legal and Council requirements, including where the Council acts as a data processor on behalf of another organisation.

48. Information governance requirements must be considered from the outset of new projects, procurements and alternative service delivery arrangements. Where personal data is involved, these must be subject to the initial stage of the Council's Data Protection Impact Assessment (DPIA) process to identify and assess potential risks and determine whether a more in-depth assessment is required.

Emerging technologies and data use

49. The Council recognises the increasing use of advanced data processing, including analytics, cloud-based systems and artificial intelligence.

50. These activities must be subject to appropriate governance, including risk assessment, DPIAs and ethical considerations, to ensure lawful and responsible use of information.

Training and awareness

51. The Council will maintain and annually review, a Training Needs Assessment which sets out information governance training requirements of employees and other individuals processing information on the Council's behalf. This ensures that training is proportionate to roles, responsibilities and levels of information risk.

52. All staff must complete mandatory information governance training appropriate to their role, at the required intervals. This will include core awareness training and, where appropriate, additional role-specific training relating to data protection, information security, information rights and information risk.

53. Managers must ensure that staff are supported to understand and meet their information governance responsibilities. This includes promoting good practice, reinforcing key messages, and ensuring that required training is completed.

54. Compliance with training requirements will be monitored through corporate governance arrangements, and appropriate action will be taken where training is not completed or standards are not met.

Responsibilities

55. The Council is responsible for ensuring compliance with information governance legislation and requirements in relation to the information it holds and processes. These obligations are overseen by the Information Commissioner's Office and, where applicable, the courts.

56. Responsibilities for implementing this policy are as follows:

Staff member / group	Responsibility
All staff and those working on the council's behalf	• Understand and comply with this policy and associated standards, procedures and guidance • Handle information in a lawful, secure and appropriate manner • Complete required information governance training • Report information risks, incidents and breaches

	promptly
Managers	• Ensure that this policy is implemented within their areas of responsibility • Support staff in understanding and meeting their information governance responsibilities • Ensure training requirements are met • Ensure that access to systems and information is appropriate for staff roles, and is updated promptly when responsibilities change
Information System Owners	• Ensure that appropriate controls are in place to manage and secure information within systems • Ensure that access permissions are appropriate to user roles and are regularly reviewed • Ensure that Data Protection Impact Assessments (DPIAs) are undertaken where required • Identify and respond to information security incidents and personal data breaches • Work with Information Asset Owners to ensure that information is accurate, appropriately managed and compliant with Council requirements
Information Asset Owners (IAOs)	• Ensure that personal data processing within their area is compliant with legal and Council requirements, including effective access management arrangements delivered through system owners and administrators • Identify, assess and manage information risks • Ensure appropriate controls are in place, including DPIAs, information sharing arrangements and records of processing etc.
Data Protection Officer (DPO)	• Provide independent advice and guidance on data protection and information governance matters • Monitor compliance with this policy and legal requirements • Support DPIAs, incident management and risk mitigation • Act as a point of contact for the Information Commissioner's Office
Senior Information Risk Owner (SIRO)	• Provide strategic oversight of information risk and compliance • Ensure that information risks are identified, managed and reported appropriately • Promote a culture of responsible information use and protection across the Council |
Information Governance and Cyber Security Board	• Provide oversight of the Council's information governance and cyber security arrangements • Monitor compliance, performance and risk

	• Review incidents, risks and mitigation actions and support continuous improvement

57. Wilful or negligent failure to comply with 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 agreements or service contracts.

Monitoring and review

58. The Council will cooperate with the Information Commissioner's Office and comply with its regulatory requirements. The Council will also have regard to relevant codes of practice, guidance and advice issued by the Information Commissioner's Office.

59. This policy and the supporting standards will be monitored and reviewed every two years in line with legislation and codes of good practice.

Supporting Standards and Procedures

60. This policy is supported by a range of standards, procedures and guidance which define how information governance requirements are implemented in practice. These include, but are not limited to, arrangements for data protection impact assessments, information sharing, information security, records management and incident management.

61. The latest versions of these documents are available on the Council's intranet Information Governance pages and Policy Library, with relevant external documents available via the website Policy Library.

- Website – Policy Library (external)
- Intranet – Policy Library (internal)
- Intranet - Data Protection and Information Governance pages (internal)

Legislation and Regulatory Framework

62. The Council will comply with all applicable legislation and regulatory requirements relating to information governance, including data protection, information access and confidentiality laws.

- 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

63. Further information, advice or guidance related to 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	2.2
Classification	Public

Version	Date	Changes
1.0	28/03/2019	Original document approved by Policy Committee
2.0	30/10/2019	Updates in line with developments since GDPR enforcement, includes reference to surveillance camera systems, data quality, data minimization, includes links to procedures / standards etc
2.1	16/01/2023	General review and minor update to include inclusion of the updated term of UK GDPR from GDPR and to reflect the requirements for when NCC acts a data processor on behalf of other parties.
2.2	06/08/2026	Review and update to align with the Information Governance Framework, including revised structure, strengthened compliance controls and improved consistency across the policy suite.