Nottinghamshire County Council

Information Compliance Policy

Introduction

1. This policy sets out the approach that Nottinghamshire County Council (NCC) will follow in respect of information compliance.

2. The policy and associated standards and procedures are **mandatory** and must be followed. It forms part of the Council's **Information Governance Framework**. The Framework also includes:

    - Our **Information Rights policy** which sets out the rights the public and employees have to access personal and public information.

    - Our **Information Security policy** which sets out the approach that NCC will follow with regard to information security.

3. We will apply this policy and good information governance to all our work and the information we handle, in recognition of our duty to the public as well as complying with legislation.

Definitions

4. "We" means the County Council and includes all members, employees, trainees / apprentices and volunteers of the County Council and contractors, suppliers and partners delivering County Council services on our behalf.

5. Information is used here as a collective term to cover terms such as data, documents, records and content whether in paper or electronic format.

6. Personal information means any identifiable data or information relating to a living individual (i.e. a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, online identifier etc).

7. Processing is any operation or set of operations which is performed on personal information such as collection, recording, storing, alteration, retrieval, use, disclosure, destruction etc.

8. A data controller is the individual or organisation responsible for deciding how and why personal data is processed.

9. Council information includes any data or information that is held by us on behalf of individuals, business, partners or we create in order to carry out our services.

Scope

10. The principles and commitments set out in this policy 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.

11. Members of the Council should note that in respect or their constituency duties as an elected representative they are data controllers in their own right and are responsible for ensuring any personal information they hold/use in this capacity is treated in accordance with the relevant legislation.

12. This policy does not apply to information held by schools which are data controllers in their own right and are individually responsible for ensuring that they comply with Data Protection and Freedom of Information legislation. If a request concerns data protection in a school or a wish to access school records, the requester should contact the Head Teacher of the relevant school.

Protecting personal and confidential information

13. We will meet our obligations in line with the principles of the Data Protection and Human Rights Acts, the UK General Data Protection Regulation (UK GDPR) and other relevant legislation, recognising the rights to privacy of living and deceased individuals.

14. We will maintain an up to date entry in the Public Register of Data Controllers or any other register required by the appropriate regulatory authority (currently the Information Commissioner's Office). The Council's registration number is Z5557238.

15. We will need to share some personal data in order to deliver services, perform our duties and legal obligations but will only do so where we have a legal obligation, power or permission to do so.

16. We will make available and signpost to privacy notices which explain why we collect personal information, how we use and share information and the rights that people have over their data.

17. We will process and keep personal and confidential information safe and secure at all times, including at the office, in public areas, home or in transit. Such information will not be disclosed or discussed except in the performance of normal work duties where there is a business need to know.

18. We will ensure that privacy risks are formally considered, addressed and documented where there are plans for any new (or change to an existing) system or business process which collects or uses personal data. This will typically be done through a Data Protection Impact Assessment (DPIA).

19. We will put in place and communicate standards, procedures and guidance documents to underpin the delivery of this policy.

Creating, storing and managing information

20. When designing and reviewing data collection processes we will ensure that established data quality principles (i.e. data relevance; accuracy; timeliness; accessibility; coherence; comparability) are applied so that our data is fit for the purpose for which it will be used.

21. We will only collect the minimum personal data required for a particular purpose and, where it is feasible and appropriate to do so, will employ data minimisation techniques such as pseudonymisation and anonymisation.

22. We will take reasonable steps to ensure that personal data held is accurate, up to date and not misleading. Where opinions or intentions about service users are recorded, this will be done carefully and professionally.

23. We will maintain record of our information assets and associated data processing activities. We will also maintain a record of systems which process personal information.

24. We will classify and use information according to its risk, sensitivity, value, and importance.

25. Personal and Council information will only be stored in approved locations (e.g. paper storage sites, office cabinets, devices, networks, systems) and in accordance with our Information Security Policy and associated standards and procedures.

26. We will consider the audience and presentation format to make information accessible.

Giving access to information

27. We will respect people's right to access personal and public information that the Council creates, owns or holds and assist them in accessing it.

28. Requests from individuals or their representatives for access to, or copies of, their personal data, will be referred to the Complaints & Information team and handled in line with the Council's Access to Information Procedure.

29. Requests from individuals or their representatives to exercise other rights conferred on them by the General Data Protection Regulation and Data Protection Act 2018 such as the right of erasure, restriction or objection will be handled in line with the Council's Data Subject Rights Procedure.

Sending and sharing information

30. We will ensure that any information sharing is undertaken confidentially, securely, legally and consistently and in line with our service standards and procedures.

31. We will ensure that Information Sharing Agreements (ISAs) are in place, where deemed necessary, and that the terms of those agreements are observed. Responsibility for the implementation an ISAs lies with the relevant Information Asset Owner.

32. We will not transfer personal data outside the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation.

33. Where it is identified that an international transfer of personal data is necessary, we will seek appropriate legal advice. Any systematic sharing of personal data outside of the UK will be subject to a DPIA.

.

Archiving, preserving and disposing of information

34. We will have a Records Retention and Disposal Schedule to ensure information is retained in accordance with legislation and NCC standards. The Schedule will be periodically reviewed for changes in legislation and the Council's business needs.

35. We will retain and dispose of information in accordance with the Records Retention and Disposal Schedule. This refers to arrangements for records retention during the period of the Independent Inquiry into Child Sexual Abuse (IICSA).

36. Staff will use the Records Management Service for paper files that are no longer in active use but need to be retained.

37. We will dispose of paper and electronic information classified as personal or confidential using the Confidential Waste Procedure and other relevant the standards and procedures.

Third Party suppliers and Contracts

38. We will ensure processing carried out by third parties on our behalf complies with the provisions of the General Data Protection Regulation, data protection and other appropriate legislation and standards.

39. Our staff (including Managers, Commissioners, Contract Managers and Project Managers) will ensure that information processed by third parties on behalf of the Council is done so in line with legal requirements and good practice.

40. If a contractor, partner organisation or agent of the Council is appointed or engaged to process personal data on behalf of the Council, or if they will do so as part of the services they provide to the Council, the lead Council officer must ensure that appropriate contractual clauses for security and data protection requirements are in place, and that personal data is kept and used in accordance with the principles of the UK GDPR and this policy.

41. If the County Council processes personal data on behalf of another party who is the data controller, the lead Council officer must make every effort to ensure that the appropriate agreements are in place to ensure the processing is undertaken in keeping with the requirements of UK GDPR.

Alternative Service Delivery Models

42. Our staff (particularly including Project Sponsors and Project Managers) will be responsible for considering information governance implications and addressing risk from the outset when planning alternative models of service delivery. A Data Protection Impact Assessment will document this process.

Accessing and securing information

43. Our staff and those working on our behalf will only view or attempt to view personal information that is necessary for their role and business need.

44. Our staff and those working on our behalf using NCC IT equipment will do so in accordance with our Acceptable Use Standard and will keep all mobile equipment secure and out of sight when taken out of Council premises.

45. Our staff and those working on our behalf will not allow unauthorised access to Council equipment and information, or knowingly introduce any security threat.

46. Staff and their managers will ensure that all Council information and equipment is returned to us before they leave the Council.

Information breaches

47. Information breaches are not always obvious and can result from a wide range of situations. For example, the loss or theft of a mobile phone, paper documents or laptop, unauthorised people having access to information, the accidental or malicious deletion of information.

48. Our staff, partners and those working on our behalf will immediately report any potential or actual losses of information or equipment holding information, potential or actual security incidents (e.g. inappropriate access, hacking, misuse of password, viruses), using the Council's data breach reporting procedure.

49. The Council will investigate reported incidents and information breaches, assist those conducting investigations and take appropriate remedial action.

50. The Council will treat any information breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

Training

51. We will ensure all staff are trained to an appropriate level and frequency, based on their roles and responsibilities, to be able to handle personal data securely and confidentially.

52. Our staff will consult and seek advice from their line manager if further training or guidance is required. The manager will arrange further training or support.

Surveillance / CCTV systems

53. Images and audio recordings of identifiable individuals captured by surveillance camera systems (including CCTV; body worn cameras, drones etc) are personal data and will be subject to the same provisions and safeguards afforded by data protection legislation as other types of personal information.

54. We will have a Surveillance Camera (CCTV) Procedure setting out data protection and other legal obligations when using such a system. The Procedure will take account of the Surveillance Camera Commissioner's Code of Practice.

55. We will ensure that use of surveillance camera systems is necessary and proportionate to achieve their objective and that the introduction of surveillance camera system for a new purpose will be subject to a DPIA prior to being used.

The Information Commissioner's Office

56. We will comply with all requests from the Information Commissioner's Office to investigate and/or review our data processing / access to information activities.

57. We will have regard to codes of practice, advice and guidance produced by the Information Commissioner's Office and shall endeavour to align our own procedures and practices with them

Responsibilities

58. The Council's Information Governance Framework sets out the key roles and responsibilities in delivering the Framework, of which this Policy forms part. These are also available on the Council's intranet, page titled Information Governance decision making, roles and responsibilities.

59. The Information Governance Board has responsibility for developing and monitoring compliance with this policy, supported by the Data Protection Officer.

60. Managers have specific information governance responsibilities, for instance in respect of information asset management. These are set out in the Information Governance Roles for Managers Standard.

61. The NCC competency framework references information governance responsibilities. All staff must adhere to this policy and its associated standards, procedures and guidance.

62. 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.

Monitoring and review

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

Council Standards and Procedures supporting this Policy

64. NCC information standards, procedures and guidelines which support this policy, at the time its approval include:

- Data Protection Impact Assessment Procedure
- Information Sharing Procedure
- Privacy Notice Procedure
- Information Security Classification Standard
- Surveillance and CCTV Procedure
- Audio Recording Procedure (under development)
- Data Security Incident and Breach Management Procedure
- Data Subject Rights Procedure
- Access to Information Procedure
- Confidential Waste Procedure
- Managers Information Governance Roles Standard
- System Owner Responsibilities Standard
- Information Retention and Destruction Standard
- Trusted Data / Data Quality Procedure (under development)
- Data Depersonalisation Procedure (under development)

65. These may be added to or replaced and are subject to regular updates as approved by the Information Governance Board, its Standards and Procedures Sub-Group or the Data Protection Officer, depending on delegation levels agreed by the Board.

66. The latest version(s) of the related standards, procedures and guidelines can be found at information governance, policies, standards and procedures.

Other Nottinghamshire County Council related policies

67. Other NCC policies which relate to this Information Compliance policy includes:

- NCC Information Governance Framework
- NCC Information Rights Policy
- NCC Information Security Policy
- NCC employee and employer code of conduct
- NCC terms and conditions of employment
- NCC accommodation standards - clear desk principles

External Legislation

68. External legislation related to this policy includes

- General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts
- Copyright, Design and Patents Act 1998

Further Information

69. 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	Jason Monks, Acting Data Protection Officer
Approver	Senior Information Risk Owner (SIRO) under delegation from Policy Committee
Date of Approval	30/10/2019
Date of next review	16/01/2025
Version	2.1
Classification	Public

Version	Date	Changes

1.0	28/03/19	Original document approved by Policy Committee
2.0	30/10/19	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	16/01/23	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.