Nottinghamshire County Council

Information Compliance Policy

Version: To be inserted upon approval
Author: Caroline Agnew
Date of Issue: To be inserted upon approval
Review date: To be inserted upon approval
Protective Marking: Official

Approvals

	V	Approval Body	Date

Review

V	Reviewing Body	Change Description	Date

Introduction

1. This policy sets out the approach that Nottinghamshire County Council (NCC) will follow with regard to 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. 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

9. 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.

10. Members of the Council should note that they are also data controllers in their own right, and are responsible for ensuring any personal information they hold/use in their role as Members is treated in accordance with the relevant legislation.

11. This policy does not apply to information held by schools who 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

12. We will meet our obligations in line with the principles of the Data Protection and Article 8 of the Human Rights Acts and other relevant legislation, recognising the rights to privacy of living and deceased individuals.

13. 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).

14. 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 consent or a legal power to do so.

15. We will only rely on consent as a condition for processing personal data if there is no relevant legal power or other condition. Consent will be obtained for any promoting or marketing of goods and services.

16. We will provide and publish complete and current 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 only collect and process the minimum amount of personal data necessary to deliver services.

18. We will process and keep personal and confidential information safe and secure at all times, including at the office, public areas, home or in transit. Such information will not be disclosed or discussed except in the performance of normal work duties and only where the recipient is authorised to receive it.

19. Our staff will ensure that their working time is used efficiently on delivering our business outcomes, they maintain our reputation and that IT and other facilities resources are used effectively.

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

Creating, storing and managing information

21. We will take reasonable steps to ensure the 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.

22. We will maintain record of information assets and associated data processing activities.

23. We will classify and use information according to its risk, sensitivity, value, and importance in accordance with our Information Classification and Handling Standard.

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

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

26. We will follow the relevant procedure when personal data needs to be anonymised or pseudonymised, for example for research purposes.

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. 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.

28. Access Requests will be centrally coordinated as set out in the Subject Access Requests procedure. LINK to be inserted upon approval.

Sending and sharing information

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

a) use of secure email and encryption for sending electronic information and tracking for paper documents.
b) ensuring that Information Sharing Agreements and Data Processing Agreements are in place, where deemed necessary and that the terms of those agreements are observed.
c) That personal data is only shared with external bodies where there is an Information Sharing Agreement or other legal basis for sharing.
d) That personal data is not shared with an individual or organisation based in any country outside of the European Economic Area (EEA) unless there is express permission to do so following a Data Protection Impact Assessment.

Archiving, preserving and disposing of information

30. We will have a Retention Standard [LINK to be inserted upon approval] to ensure information is retained in accordance with legislation and NCC standards. The Retention Standard will be periodically reviewed for changes in legislation and the Council's business needs.

31. We will only retain information for the time period applicable to the Retention Standard.

32. We will dispose of paper and electronic information classified as personal or confidential using the appropriate standards and procedures.

Third Party suppliers and off-site hosting

33. 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.

34. Our staff (including Managers, Commissioners, Contract Managers and Project Managers) will make appropriate contractual arrangements, in conjunction with legal services, where information is processed by third parties on behalf of the Council to ensure its security, transfer, appropriate use, disposal and/or return at the end of the contract.

Alternative Service Delivery Models

35. Our staff (particularly including Project Sponsors and Project Managers) are responsible for considering information governance implications and addressing risk from the outset when planning alternative models of service delivery.

Accessing and securing information

36. 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. They

will follow system user guidance or other formal processes which are in place and ensure that only those with a business need to access personal data are able to do so.

37. We will keep all NCC paper information locked away when not in use and take all reasonable measures to keep information secure and out of sight when taken out of NCC premises.

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

39. We will ensure that all Council information and equipment owned or held by us is recorded and is transferred or returned to us by staff or other approved users before they leave the Council.

Information breaches

40. 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.

41. 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 data breach reporting procedure. [LINK to be inserted upon approval]

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

43. 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, addressed accordingly.

Training

44. 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. This will be set out in the Council's information training standard.

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

Responsibilities

46. The NCC competency framework [LINK to be inserted upon approval] references information governance responsibilities for all staff who must adhere to this policy and its associated standards, procedures and guidelines.

47. Managers have specific information governance responsibilities, for instance in respect of information asset management. These are set out in an information governance role descriptor [LINK to be inserted upon approval].

48. Departmental Risk, Safety and Emergency Management Groups are accountable for the effective management of information risk and information governance compliance, as well as supporting and promoting the policies, standards and procedures.

49. 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

50. This policy and the supporting standards will be monitored and reviewed annually in line with legislation and codes of good practice.

Appendices

51. NCC information standards, procedures and guidelines which support this policy, which at the time of this policy's approval include:

    - List to be inserted upon completion of work on procedures

52. These may be added to or replaced and are subject to regular updates as approved by the NCC Information Governance Group.

53. The latest version(s) of the related standards, procedures and guidelines can be found at [LINK to be inserted upon approval] for the latest version(s).

Other Nottinghamshire County Council related policies

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

    - NCC information governance framework
    - NCC information rights policy
    - NCC employee and employer code of conduct

- NCC terms and conditions of employment
- NCC accommodation standards - clear desk principles

External Legislaton

55. External legislation related to this policy includes

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