Internal ref:	NELC 16.60.05
Version No:	5
Last updated:	July 2025
Review date:	July 2027

Confidentiality Policy

1. Purpose and Scope

This policy supports those acting on behalf of North East Lincolnshire Council to follow good practice in the handling of confidential information and personal data to which they have access in the course of their work.

Examples of confidential information include service user, councilor and / or employee records, enforcement activities, complaint information and contractual details. The Cyber Security – Protective Monitoring Policy sets out the labels that are applied to information to indicate its sensitivity based on its content, and that the labels should be reviewed to ensure they remain relevant when content is amended.

This policy applies to anyone acting on behalf of the Council (hence forward referred to as employees), it also applies to anyone working within the premises of the Council.

2. Policy Statement

The Council recognises that, given the nature of their work, employees will be party to personal and confidential information about individuals and organisations. Employees must always err on the side of caution in considering whether information is sensitive or confidential.

Specific statutory provisions apply to certain activities (such as the requirement to conduct investigations confidentially) and these must be strictly applied. This policy and the Data Protection Policy set out the main requirements.

Anyone who is in any doubt about the application of the policies and the confidential handling of information must discuss the issue with their line manager or the Council's Information Governance team transparency@nelincs.gov.uk.

3. Implementation, monitoring and review of the policy

The Senior Management Team have overall responsibility for the implementation, monitoring and adherence to this policy across all service areas.

The Information Security and Assurance Board are responsible for raising awareness of this policy and providing advice and guidance in relation to its application.

People and Organisation are responsible for overseeing the Disciplinary Policy and procedures in respect to this policy.

Everyone covered by the scope of the policy is obliged to adhere to and facilitate implementation of the policy.

Appropriate action will be taken to inform all new and existing employees and others covered by the scope of the existence of the policy and their role in adhering to it.

The policy will be reviewed at least every 2 years by the Information Security and Assurance Board, or at such times as legislation or a change to the Council policy position requires it.

The policy will be published on our website.

4. Requirements

Disclosure of Information

The Council is committed to making the organisation as open, accountable and transparent as possible. To support this, we aim to make as much official information, which is not subject to confidence or otherwise protected from publication, easily accessible to all through our website. Our Publication Scheme

outlines the specific information we make available to the public about our activities without the need for them to make a formal request and how it can be obtained.

Employees must not, without proper authorisation, disclose confidential information which they acquire in the course of their work, or which has been received in confidence from others.

It is important that all employees:

- only access information related to work they have been required to carry out,
- remember, that even if confidential or personal information appears trivial or widely known, it should not be disclosed to anyone internally or externally except in the terms of this policy or with specific authorisation,
- ensure that all papers and electronic files associated with the work of the organisation are kept protected and secure.

Employees must not disclose knowledge gained in the course of their work in social settings or on social media and should avoid discussions of a confidential nature in any setting where they may be overheard. For more details about the acceptable use of social media, employees should consult our Social Media Policy.

Employees must ensure when they are working with confidential information, be that in hard copy or electronically, that others who are not party to the information do not inadvertently see it. Laptops, computers and other devices used to view information must have password protected log in screens and / or screensavers so that their contents cannot be viewed without the proper authorisation if they are left unattended for any time. Employees should follow a Clear Desk and Screen Policy.

The duty of confidentiality continues to apply after an employee leaves the Council's employment.

5. Data Protection Act

The Council recognises that information about individuals, whether held electronically or on paper, falls within the scope of the Data Protection Act 2018

and UK General Data Protection Regulation (UK GDPR) and must be handled in such a way as to comply with the data protection principles.

6. Grievances or Concerns

Employees who are concerned about the conduct or actions of others working for the Council in any capacity should raise this with their line manager or the Council's Monitoring Officer and not discuss their concerns outside of the office. The Reporting A Concern (Whistleblowing) Policy details how to do this and can be found on the Council's intranet.

Members of the public or organisations can raise their concerns through the Council's Feedback Policy.

7. Breaches of the Policy

Anyone who does not comply with this policy, and is directly employed by the Council, may be subject to disciplinary action as set out in the disciplinary procedures.

Any other person covered by this policy, and found not to comply, will be reported to the relevant office / employer. This may also result in Council terminating any contract.