AUDIT AND GOVERNANCE COMMITTEE

DATE 05/11/2026

REPORT OF Assistant Director of Law and Governance

SUBJECT Counter Fraud and Corruption Policy

STATUS OPEN

CONTRIBUTION TO OUR AIMS

Effective Anti-Fraud and corruption arrangements support the delivery of the Council's strategic objective of having an engaging and effective council by contributing to effective governance arrangements designed to underpin them.

EXECUTIVE SUMMARY

This report introduces the council's updated Counter Fraud and Corruption Policy. The endorsement of the policy provides a clear and consistent message that the risk of fraud and corruption is real, will not be tolerated, and is the responsibility of all council employees to minimise. It provides a framework for the effective deterrence, detection, investigation, and sanction of fraudulent or corrupt activity.

The report also provides the Committee with the updated Ani-Bribery Policy and Anti-Money Laundering Policy.

RECOMMENDATIONS

The Audit and Governance Committee is requested to:

- To review the draft Counter Fraud Policy, and where appropriate provide comment, prior to it being formally approved by the Portfolio Holder for Finance, Resources and Assets.

- To note the contents, and where appropriate provide comment, on the updated Anti-Bribery Policy and the Anti Money Laundering Policy .

REASONS FOR DECISION

The Committee's responsibilities include monitoring and reviewing the effectiveness of the council's arrangements in relation to fraud and corruption. Consideration of the Anti-Fraud and Corruption Policy, and awareness of its supporting policies, is a key part of those responsibilities.

1. BACKGROUND AND ISSUES

Most of the Council's fraud related policies are due for their cyclical review, and therefore the Fraud Lead (supported by the Head of Audit and Assurance) has reviewed the following policies:

- Counter Fraud and Corruption Policy
- Anti- Bribery Policy
- Anti- Money Laundering Policy

The Counter Fraud and Corruption Policy requires formal adoption by the Portfolio Holder, but the Audit and Governance Committee, as part of the discharge of its responsibilities, is required to seek assurance on it and also provide any feedback (if appropriate) prior to its formal adoption. In relation to the Anti-Bribery and Anti-Money Laundering Policies though they do not require formal approval they are shared with the Committee to note and for comment.

Since they were last reviewed in 2022 there has been relatively little change in the regulatory framework relating to Fraud, with the exception of:

- **Economic Crime and Corporate Transparency Act 2023**, which puts the Council under a legal duty to prevent fraud and may be subject to prosecution if it is found not to have sufficient preventative measures in place.
- **Money Laundering and Terrorist Financing (Amendment) Regulations 2026,** which have updated regulations to take account of developments in the landscape such as crypto assets, but has also emphasised that organisation's approaches to anti-money laundering should be proportionate and risk based.

Consequently, significant changes to the policies have not been required, with most of the focus being to update the wording of them to help understanding**.** A summary of the changes is discussed below:

- **Counter Fraud and Corruption Policy:** It reflects the failure-to-prevent-fraud provisions introduced by the Economic Crime and Corporate Transparency Act 2023, broadens the policy's scope to those acting for or on behalf of the Council, identifies current and emerging fraud risks. It also more clearly documents expectations around appropriate checks on individuals and organisations acting for or on behalf of the Council, reporting, investigation and recovery.

- **Anti-Bribery Policy**: The updated policy retains the Council's zero-tolerance approach but more clearly explains the standards expected of employees, Members and third parties. It strengthens the requirements placed on contractors, suppliers and partners, clarifies the main bribery offences, and reinforces arrangements for preventing bribery and reporting concerns without fear of unfair treatment.

- **Anti-Money Laundering Policy:** The updated policy further clarifies

when the rules apply, Council activities are most at risk, the roles of the Money Laundering Reporting Officer and deputies. It also provides clearer guidance on handling sensitive information, checks on the identity and sources of funds, reporting concerns and pausing transactions.

2. RISKS, OPPORTUNITIES AND EQUALITY ISSUES

Every pound lost to fraud is a pound that the council cannot invest in the place and people of North East Lincolnshire. Failure to have an adequate anti-fraud and corruption policies increases the risk of the council suffering losses due to fraud.

Effective and coordinated anti-fraud arrangements are essential to protect the council against the loss of resources and reputation, and to ensure help and support reaches those in need and entitled to it.

Furthermore, the Economic Crime and Corporate Transparency Act 2023 introduced a corporate offence of failure to prevent fraud which, where the statutory criteria are met, can make an organisation criminally liable where an associated person commits a specified fraud offence intending to benefit the organisation or, in certain circumstances, a person to whom services are provided on its behalf. In addition, there are both the Bribery Act and Anti-Money Regulations

3. OTHER OPTIONS CONSIDERED

No other options were considered. The review and updating of the Counter Fraud and Corruption Policy is essential to ensure the council's response to the risk of fraud is robust and appropriate.

4. REPUTATION AND COMMUNICATIONS CONSIDERATIONS

As well as financial loss caused by fraud, there can also be reputational impacts for those organisations which do not manage the risk of fraud effectively, and potentially legal implications.

Once approved the Counter Fraud and Corruption Policy, and supporting policies, will be promoted across the Council. This will include highlighting to employees their responsibilities to support the Council's approach to counter fraud

5. FINANCIAL CONSIDERATIONS

Effective implementation of this policy should help prevent and detect financial loss, improve recovery of fraud losses and associated costs where economically appropriate, and protect Council resources available for service delivery.

6. CHILDREN AND YOUNG PEOPLE IMPLICATIONS

There are no specific implications for Children's Services.

7. CLIMATE CHANGE, NATURE RECOVERY AND ENVIRONMENTAL IMPLICATIONS

There are no climate change or environmental implications arising from this report.

8. PUBLIC HEALTH, HEALTH INEQUALITIES AND MARMOT IMPLICATIONS

Though there are no direct implications to public health and health inequalities our processes involve the acknowledgement of vulnerabilities which inform statutory safeguarding referrals, signposting to relevant support to improve outcomes, and ensure decisions in respect of investigations and sanctions are based on public interest in addition to evidence.

9. FINANCIAL IMPLICATIONS

There are no direct additional financial implications arising from approval of the policies. Implementation, including training, due diligence and monitoring, is expected to be managed within existing resources. Any future requirement for additional investment will be subject to the Council's normal budget and governance processes. Effective implementation should help prevent financial loss and support recovery where lawful, proportionate and economically appropriate.

10. LEGAL IMPLICATIONS

It is a matter of good governance to be cognisant of statutory and regulatory change, along with good practice. Timely reviews of pertinent policies is supported and endorsed. The reports are presented as part of the constitutional remit of the Audit and Governance Committee in its assurance role.

11. HUMAN RESOURCES IMPLICATIONS

There are no direct Human Resources implications arising from this report; however, employees will need to be made aware of the updated policies and their responsibilities for preventing and reporting suspected fraud, bribery and money laundering.

12. WARD IMPLICATIONS

There are no specific ward implications associated with this report.

13. BACKGROUND PAPERS

Fighting Fraud Locally Strategy

https://www.local.gov.uk/sites/default/files/documents/FFCL%20-%20Strategy%20for%20the%202020s.pdf

14. CONTACT OFFICER(S)

Peter Hanmer, Head of Audit and Assurance, peter.hanmer@nelincs.gov.uk

John Shepherd, Fraud Lead, john.shepherd@nelincs.gov.uk

SIMON JONES

ASSISTANT DIRECTOR LAW AND GOVERNANCE

Internal Ref:	NEL AFCS
Review date	November 2029
Version No.	V1.0

Counter Fraud and Corruption Policy

DRAFT

Foreword (to be confirmed)

North East Lincolnshire Council is committed to protecting public funds, maintaining public confidence, and ensuring that resources are preserved for the benefit of the communities it serves.

Fraud, corruption, bribery and financial misconduct reduce the resources available to deliver vital services and undermine public trust. The Council therefore adopts a zero-tolerance approach to fraud and corruption and is committed to preventing, detecting, investigating and responding to fraud and associated risks wherever they arise.

The Council will seek to impose sanctions where appropriate and will always act to recover funds which have been obtained as a result of fraud or other associated offending.

This Counter Fraud Policy sets out the Council's approach for the period 2026-2029.

Signed

Chief Executive

Signed

Portfolio Holder for Finance,

Assets and Resources

DRAFT

Introduction

The Council is responsible for the delivery of a wide range of local services – delivered by employees and persons contracted to act on behalf of the Council. It is vital that fraud, and associated offending, is kept to a minimum to ensure those funds are used to provide vital services to the communities served. Funds lost to fraud and error deprive the public of the services they deserve.

The Council has a responsibility to maintain effective arrangements for preventing and detecting fraud and protecting the public funds it administers. The Economic Crime and Corporate Transparency Act 2023 introduced a corporate offence of failure to prevent fraud which, where the statutory criteria are met, can make an organisation criminally liable where an associated person commits a specified fraud offence intending to benefit the organisation or, in certain circumstances, a person to whom services are provided on its behalf. The Council is therefore committed to maintaining reasonable and proportionate fraud prevention procedures alongside its wider arrangements for preventing fraud against the Council.

It is the responsibility of the entire workforce to drive a culture where fraud and corruption are not tolerated.

Purpose

The purpose of the policy is to set out the Council's approach to:

- Protecting public money from fraud, corruption, bribery and financial abuse.
- Promoting a strong anti-fraud culture.
- Reducing opportunities for fraud.
- Improving fraud detection capabilities.
- Delivering effective and proportionate investigations.
- Recovering losses and maximise deterrence.
- Ensuring compliance with professional standards and best practice.

The benefits of a robust policy and proactive delivery of an effective approach to counter fraud include:

- Increased ability to prevent losses due to fraud by improving the understanding of the risk.
- Being more resilient to fraud and scanning for new fraud risks.
- Providing support to the national agenda for fighting fraud.

- Being able to clearly account for the effectiveness of the council's counter fraud arrangements to the public, partners, and national stakeholders. This will feature as a core element in the Annual Governance Statement.
- Providing assurance on counter fraud arrangements.
- Ensuring resources are proportionate to the perceived threat and risk.

Scope

This policy applies to all Council employees, elected members, contractors, consultants, agency workers, volunteers and other persons or organisations acting for or on behalf of the Council.

The Council also expects suppliers, partners and organisations receiving Council funding to maintain high standards of integrity and to cooperate with the Council in preventing, detecting and investigating fraud, bribery and corruption. Appropriate counter-fraud requirements will be incorporated into contractual and partnership arrangements where proportionate to the risk.

Fraud Risk Areas

Fraud risk falls into two distinct categories:

Internal Fraud

- Recruitment fraud
- Payroll fraud
- Abuse of position
- Procurement fraud
- Expenses fraud
- Corruption and bribery
- Theft and misuse of Council assets
- Mandate fraud
- Conflict of interest

DRAFT

External Fraud

- Council Tax fraud – including empty properties, single person discount, and Council Tax Support
- Business rate fraud
- Housing-related fraud
- Insurance fraud
- Adult Social Care
- Grant fraud
- Procurement and supplier fraud
- Blue Badge Fraud

It is important to be aware of emerging risks; many offences committed in the digital world involve at least an element of fraud to 'trick' or gain access to data or information:

- Identity fraud
- Insider risk
- Cyber-enabled fraud
- Organised crime
- Artificial intelligence enabled fraud
- Digital payment fraud

Legal Framework

There are numerous ways in which the Council can become a victim to fraud, or other associated offending, and the below are some of the main definitions involved:

Fraud

Fraud is defined in the Fraud Act 2006 and carries a maximum term of imprisonment of 10 years. There are three main ways in which fraud is committed:

- Fraud by false representation

- Fraud by failing to disclose information
- Fraud by abuse of position

Fraud involves a dishonest act and is carried out to cause a gain to one person, or a loss to another.

Bribery

The Bribery Act 2010 establishes four principal offences:

- Offering, promising or giving a bribe
- Requesting, agreeing to receive or accepting a bribe
- Bribing a foreign public official
- Failure of an organisation to prevent bribery

Bribery occurs where a financial or other advantage is offered, promised, given, requested or accepted in order to improperly influence a decision, function or activity.

Corruption

Fraud and bribery are specific offences in law, corruption can include elements of both, but is a breach of standards as opposed to a criminal offence:

Corruption is the abuse of entrusted power, position or influence for an improper benefit or purpose, whether financial or non-financial.

Money Laundering

Money laundering is the process by which money obtained through criminality is altered in some way to give it the appearance of being legitimate. The Council must operate in such a way to deter involvement in any activity which could be linked to an act of money laundering and is under a duty to report specific information to the authorities.

DRAFT

Strategic Priorities

This policy is developed in line with the five principles included in the **Fighting Fraud and Corruption Locally – a Strategy for the 2020s.**

Govern

Tackling fraud starts with strong governance, clear accountability and a culture of integrity. By embedding robust counter-fraud arrangements throughout the

organisation, the Council protects public funds, supports ethical decision-making and demonstrates zero tolerance towards fraud and corruption. Our approach includes:

- Maintaining an effective counter fraud framework.
- Having a "Counter Fraud Champion" at Cabinet level to demonstrate the Council's commitment to Counter Fraud.
- Ensuring oversight by the Audit and Governance Committee.
- Completing regular fraud risk assessments.
- Regularly review policies and procedures.
- Benchmarking against recognised good practice.

Acknowledge

Recognising and understanding fraud risks enables the Council to take informed action to prevent loss, protect public resources and maintain public trust. We do this by:

- Monitoring emerging threats.
- Maintaining a fraud risk profile.
- Supporting managers in identifying vulnerabilities.

Prevent

By strengthening controls, raising awareness and using intelligence-led approaches, the Council seeks to prevent fraud, protect public resources and minimise opportunities for financial misconduct. This includes:

- Delivering fraud awareness training.
- Promoting reporting methods via documents such as the fraud response plan
- Embedding fraud prevention within service design.
- Supporting managers in implementing effective controls.
- Undertaking proportionate due diligence on persons and organisations acting for or on behalf of the Council.
- Ensuring fraud risks are considered when establishing or changing services, contracts, partnerships and funding arrangements.
- Maintaining proportionate procedures designed to prevent associated persons committing fraud for the benefit of the Council.

Pursue

Those who commit fraud will be investigated, sanctioned and held to account, with the Council seeking to recover losses and protect the public purse. We will do this by:

- Investigating allegations promptly and proportionately in line with the Fraud Response Plan

- The Council will seek to recover fraud losses and associated costs wherever it is lawful, proportionate and economically appropriate to do so, using available civil, criminal and administrative remedies.
- Applying appropriate sanctions.
- Seeking criminal, civil, disciplinary or administrative action where appropriate.
- Working alongside partner agencies such as the Police, the Department of Work and Pensions, Cabinet Office, National Anti-Fraud Network (NAFN), and other Local Authorities

Protect

Protecting public funds, services and information from fraud helps ensure resources are available to support the residents and communities we serve. Our approach includes:

- Strengthening measures across the Council by working in partnership.
- Lessons identified through investigations will be used to strengthen controls and reduce the risk of recurrence.
- Participating fully in the National Fraud Initiative and other lawful data-matching exercises to prevent and detect fraud, identify error and support assurance over the effective management of public funds.
- Developing operational procedures on relevant themes of offending, for example Council Tax empty property fraud.
- Data processing and counter-fraud activity will be undertaken in line with requirements of the Data Protection Act and GDPR.

Responsibilities for Managing Fraud Risk

It is the responsibility of everyone to support the Council's Anti-Fraud culture, and to manage its fraud risks. Appendix 1 summarises these.

Employees, elected members and those working on behalf of the Council are expected to report suspicions of fraud, bribery or corruption promptly in accordance with the Fraud Response Plan or, where appropriate, the Reporting a Concern (Whistleblowing) Policy.

Individuals should not attempt to investigate suspected fraud themselves where doing so could compromise evidence or an investigation.

Members of the public, contractors and partner organisations are also encouraged to report suspected fraud affecting the Council through the Council's published reporting methods.

Delivery of Counter Fraud and Corruption Activity

Whilst the Council is at risk of fraud, there are many areas of offending which overlap or involve an element of fraud, for this reason it is essential that the framework of policies and procedures is considered. These include:

- Fraud Response Plan, which lays out how allegations of fraud are investigated.
- Reporting a Concern (Whistleblowing) Policy
- Anti-Bribery Policy
- Anti-Money Laundering Policy
- Code of Corporate Governance
- The Constitution including Contract Procedure Rules and Financial Regulations
- Employee Code of Conduct
- Gifts and Hospitality Policy
- Risk Management Policy
- Information Security Policy

Each year the Council publishes a fraud plan, this is informed by the previous year's fraud performance and activity, along with regional and national trend information, and identifies where resources will be targeted to achieve objectives around fraud prevention and detection.

Review

The policy will be reviewed every three years, or more regularly if legislation changes or with significant changes to the fraud risk profile.

DRAFT

Appendix 1: Roles and Responsibilities

Chief Executive	• Provide visible executive leadership supporting a strong counter-fraud culture. • Ensure fraud and corruption risks receive appropriate organisational attention. • Support appropriate access, independence and authority for those responsible for counter-fraud activity.
Councillors	• Facilitate an anti-fraud and anti-corruption culture. • Demonstrate a commitment to this policy and ensure it has the appropriate profile within the council.
Portfolio Holder	• Act as the Cabinet's Fraud champion. • On be behalf of the Cabinet approve the Fraud Policy. • Promote the Policy throughout the Council, and obtain assurance that is complied with.
Audit and Governance Committee	• To provide feedback to the Cabinet on the content of the corporate Fraud Policy. • To monitor and review the effectiveness of the council's anti-fraud and corruption arrangements. • Ensure that there is strong political and executive support for work to counter fraud and corruption. • Ensure consistency across the council in the implementation of this strategy.
Section 151 Officer	• Ensure that those working to counter fraud and corruption are professionally trained and accredited for their role, and attend regular refresher courses to ensure they are up to date with new developments and legislation. • Ensure that there is a level of financial investment in counter fraud and corruption work that is proportionate to the risk that has been identified. • Ensure that reports on investigations include a section on identified policy and system weaknesses that allowed the fraud/corruption to take place where appropriate.
Directors, Assistant Directors, and Heads of Service	• Ensure the risks of fraud and corruption are identified, recorded on the risk register as required, and action plans implemented to reduce the risk to an acceptable level.

DRAFT

	• Ensure the anti-fraud and anti-corruption policy is compliant within their area of responsibility. • Ensure that any allegations or suspicions of fraud are reported in line with the Fraud Response Plan, or if appropriate, the Reporting a Concern (Whistleblowing) policy. • Ensure the risk of fraud and corruption is considered in all new processes.
Monitoring Officer	• Regularly publicise and monitor compliance with expected standards of ethical conduct. • Ensure that progress in raising standards is communicated to stakeholders. • Ensure that effective whistleblowing arrangements are established. • Ensure registers of interests, gifts & hospitality are maintained. • Ensure councillors and officers are fully aware of their obligations in relation to probity. • Ensure that those working to counter fraud and corruption are undertaking this work in accordance with a clear ethical framework and standards of personal conduct.
Audit and Assurance	• Produce an annual counter fraud plan. • Support Directors, Assistant Directors, Heads of Service, and their managers in identifying and mitigating risks for fraud and corruption. • Promote an anti-fraud culture, including awareness campaigns, risk assessments, and development of tools to identify potentially fraudulent activity. • Ensure all allegations are recorded and risk assessed • conduct investigations in line with legislation, standards, and rule of conduct. • Ensure that those carrying out fraud investigations are adequately trained. • Notify HR and Legal Services (at the outset of investigations into employees). • Make recommendations where weaknesses are identified, and ensure action plans implemented to prevent reoccurrences. • Undertake proactive exercises into areas where the risk of fraud is greatest.

DRAFT

	• Consider fraud risks when determining the annual Audit Plan and the content of specific audit assignments.
People and Culture	• Ensure that there is an effective propriety checking system (i.e., safe recruitment) implemented by appropriately trained staff. • Ensure employment policies support the anti-fraud and anti-corruption framework. • Monitor effective and appropriate sanctions are applied in all appropriate cases. • Ensure that all staff in People and Culture are aware of the Fraud Response Plan and the action to take if they suspect fraudulent activity. • Inform Audit and Assurance at the outset of any conduct investigation.
Managers	• Ensure all employees are aware of their responsibilities under the anti-fraud and anti-corruption policy. • Ensure all employees have read the Employee Code of Conduct and understand their responsibilities. • Ensure all employees understand the Reporting a Concern (Whistleblowing) policy and reporting arrangements. • Ensure employees are aware of the process for reporting allegations of fraud. • Ensure accurate and timely reporting of gifts and hospitality.
Employees	• Understanding of expected behaviour and of their responsibility to report suspected fraud or corruption and the appropriate methods to do so.

DRAFT

Internal Ref:	NEL ABP
Review date	November 2029
Version No.	V1.0

Anti Bribery Policy

DRAFT

Contents

1 Purpose

2 Scope

3 Introduction

4 Corporate responsibilities

5 Employee and Member responsibilities

6 Reporting a concern

DRAFT

Purpose

The purpose of this policy is to set out the Council's commitment to preventing, detecting and responding to bribery and corruption and to establish the standards of conduct expected of elected Members, employees and persons acting for or on behalf of the Council.

The Council has zero tolerance of bribery and corruption and is committed to conducting its activities fairly, openly, honestly and with integrity.

Scope

This policy applies to all Council employees and elected Members and, where appropriate, to agency workers, contractors, consultants, volunteers and other persons acting for or on behalf of the Council.

The Council also expects contractors, suppliers, partners and organisations acting on its behalf to maintain appropriate standards designed to prevent bribery and corruption. Appropriate anti-bribery provisions will be incorporated into contractual and partnership arrangements where proportionate to the risk.

Introduction

Bribery is the act of offering an advantage, financial or otherwise, in return for influence over decisions or actions (or omissions). It may be linked to personal gain, or for gain of another. Bribery can also involve third parties who act on behalf of the person seeking beneficial treatment.

The Bribery Act 2010 introduced the below key areas in which offences can be committed:

- Section 1 – Bribing another person
  Covers where an offer, or promise, is made to give an advantage, financial or otherwise, intending to induce the other person to act improperly, or to reward the other person for acting improperly. The offence also covers the situation where the receipt of the advantage would amount to acting improperly, regardless of influencing further action or decisions.

- Section 2 – Offences relating to being bribed
  Makes it an offence to request, agree to receive, or accept, a bribe.

- Section 6 – Bribery of foreign public officials

Covers bribery intending to obtain or retain business, or an advantage in the conduct of such business.

- Section 7 – Failure of commercial organisations to prevent bribery Commercial organisations have a responsibility to prevent offences of bribery which intend to obtain or retain business, or an advantage in the conduct of such business. In the event of such an offence being committed the organisation could raise a defence by demonstrating they had adequate procedures designed to designed to prevent people from engaging in such acts.

The Act interprets the improper performance as breaching a relevant expectation and includes the failure to complete a particular function, i.e. to 'turn a blind eye'.

North East Lincolnshire Council will not offer bribes or any other improper inducements to anyone for any purpose, nor will they accept bribes or improper inducements.

This policy does not change the requirements of the Council's Code of Practice for Employees relating to Interests, Gifts and Hospitality.

Corporate Responsibilities

Section 7 of the Bribery Act 2010 creates a corporate offence where a relevant commercial organisation fails to prevent bribery by a person associated with it where the bribery is intended to obtain or retain business, or an advantage in the conduct of business, for the organisation.

Irrespective of the extent to which section 7 applies to particular activities undertaken by the Council, the Council is committed to maintaining robust and proportionate arrangements to prevent bribery. In doing so, the Council has regard to the six principles contained within Ministry of Justice guidance on preventing bribery.

1. **Proportionate Procedures**

The council ensures that its procedures to prevent bribery are proportionate to the bribery risk it faces and to the nature, scale and complexity of its activities It ensures that they are clear, practical, accessible, effectively implemented and enforced.

2. **Top Level Commitment**

The Council, through its Executive and Non-Executive roles are committed to preventing bribery by persons associated with the council. Cabinet Members and Senior Officers will continue to foster a culture within the council in which bribery is not tolerated.

The Council has a strong Counter Fraud Strategy that is regularly reviewed and approved by the Audit Committee. The message is clear that fraud and corruption will not be tolerated.

3. **Risk Assessment**

The Council assesses the nature and extent of its exposure to potential external and internal risks of bribery on a periodic basis. It is assessed on both financial risk and reputation risk.

4. **Due Diligence**

The Council applies due diligence procedures, taking a proportionate and risk-based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, to mitigate identified bribery risks.

5. **Communication and training**

The Council seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the Council through internal and external communication, including training and e-learning that is proportionate to the risks it faces.

6. **Monitoring and review**

The council monitors and reviews its procedures designed to prevent bribery and will make improvements where necessary.

Employee and Member Responsibilities

All employees and Members are required to act honestly and with integrity at all times, and to safeguard the organisation's resources for which they are responsible.

Employees and Members must comply with the spirit, as well as the letter of the laws and regulations of all jurisdictions in which the Council operates, in respect of the lawful and responsible conduct of activities.

Employees and Members must:

- Ensure that they read, understand, and comply with this policy.
- Raise concerns at the earliest opportunity if they believe or suspect that a conflict with this policy has occurred or may occur in the future.

Employees and Members must **not**:

- Give, promise to give, or offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.

- Give, promise to give, or offer a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure.

- Accept payment from a third party that you know, or suspect is offered with the expectation that it will obtain a business advantage for them.

- Accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by the Council in return.

- Harass or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy.

- Accept facilitation payments (unofficial payments to public officials) in order to secure or expedite actions.

Persons found to have breached this policy, may be subject to disciplinary action, in addition to the prospect of civil or criminal proceedings.

Reporting a Concern

The prevention, detection, and reporting of bribery and other forms of corruption are the responsibility of all those working for the Council or under its control. All employees and Members are required to report activity that breaches (or may breach) this policy.

Employees may be the first persons to suspect that wrongdoing may be taking place; they may however be hesitant to report the matter for fear of being subject to retaliation, harassment, victimisation or other detrimental treatment. This presents a risk of missing opportunities to act. A positive working environment must be encouraged to support the reporting of concerns under the **Reporting a Concern Policy.** A supportive culture must exist to allow serious concerns to be investigated with no detrimental effect on the person making the report.

Reporting-a-Concern-Whistleblowing-Policy.pdf

Review

This policy will be reviewed every three years, or earlier in the event of changes to legislation.

DRAFT

Internal Ref:	NELC.AML
Review date	November 2029
Version No.	V1.0

Anti-Money Laundering Policy

DRAFT

Contents

1 Introduction
2 Definition
3 Legislation
4 Scope
5 Individual Responsibilities
6 Council Responsibilities
7 Money Laundering Reporting Officer
8 Customer Due Diligence Measures
9 Enhanced Due Diligence
10 Record keeping
11 Guidance and Training
12 Monitoring and Review

Appendix 1 – Examples of Local Authority Risk Areas

Appendix 2 – Requirement for Due Diligence

Appendix 3 – Action where Money Laundering Activity is Suspected

Appendix 4 – Money Laundering Disclosure Form

DRAFT

Introduction

Money laundering is the process by which criminals disguise, convert, transfer or use the proceeds of crime so that they appear to originate from a legitimate source. The aim is to conceal the true origin of criminal funds and integrate them into the legitimate economy without attracting suspicion

Action against money laundering is a key part of the Council's framework to prevent fraud, corruption, and associated offending. This policy explains what money laundering is, what the Council's duties are, and how local authorities may become involved in acts of money laundering where the appropriate preventative measures are not in place.

Money laundering risk within a local authority is most likely to arise through property and land transactions, procurement activity, regeneration schemes, grant funding, treasury management, licensing, housing transactions, cash collection services and dealings with third-party organisations. The Council must maintain effective anti-money laundering arrangements, including appropriate due diligence, staff training, clear reporting routes, and oversight by the Money Laundering Reporting Officer, to ensure that suspicious activity is identified, reported and managed in accordance with legal requirements and a risk-based approach.

North East Lincolnshire Council will:

- prevent its services, assets and transactions being used to launder the proceeds of crime;
- identify and manage money-laundering and terrorist-financing risks;
- comply with applicable legal requirements;
- require employees and Members to report suspicions promptly;
- cooperate appropriately with law-enforcement agencies; and
- take a proportionate, risk-based approach.

Legislation and Regulations

This is a complex area of law and there are several pieces of legislation which Councils need to consider in their response including

Legislation and Regulations	Key Significance
Terrorism Act 2000	Created offences relating to terrorist property and established reporting obligations where terrorist financing is suspected.

Proceeds of Crime Act 2002 (POCA)	The cornerstone of UK anti-money laundering law. Created the principal money laundering offences (concealing, arranging, acquiring, using or possessing criminal property) and established the Suspicious Activity Report (SAR) regime.
Money Laundering Regulations 2003	Introduced formal customer due diligence and internal control requirements for regulated businesses.
Money Laundering Regulations 2007	Introduced a more explicit risk-based approach and strengthened customer due diligence requirements.
Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017	Replaced the 2007 Regulations. Introduced enhanced risk assessment requirements, beneficial ownership checks, stronger governance arrangements, policies, procedures, training requirements and customer due diligence requirements.
Money Laundering and Terrorist Financing (Amendment) Regulations 2026	Amends specified aspects of the 2017 Regulations. Relevant provisions and commencement dates must be checked against the Council activities to which they apply; the Regulations should not be treated as imposing the regulated-sector regime on all Council functions.

The Proceeds of Crime Act 2002 defines the main money laundering offences including:

- **Concealing –** conceals, converts, disguises, transfers, removes (from the UK) criminal property
- **Arrangements –** enters / becomes concerned in arrangements that he knows or suspects to involve acquisition, retention, use or control of criminal property, for or on behalf of another.
- **Acquisition –** acquires, uses, or has, possession of criminal property.
- **Failure to Disclose –** creates an offence for the regulatory sector where suspected offending is not reported.
- **Tipping off (regulated sector) –** discloses information subject to formal reporting requirements, likely to prejudice an investigation.

Scope

This policy relates to everyone across the council and includes:

- all employees;
- elected Members;

- agency and temporary workers;
- contractors and consultants;
- volunteers where appropriate; and
- anyone acting on behalf of the Council.

Council Responsibilities

The Council is not a “relevant person” for all of its activities. The general money laundering offences under the Proceeds of Crime Act 2002 (POCA), and relevant offences and reporting provisions under the Terrorism Act 2000, may apply irrespective of whether an activity is within the regulated sector. The more prescriptive requirements of the Money Laundering Regulations, including customer due diligence, enhanced due diligence, governance, training and record-keeping requirements, apply only where the Council is carrying on an activity within the regulated sector. The Council will nevertheless maintain proportionate, risk-based arrangements across its functions to prevent its services and transactions being used for money laundering or terrorist financing.

Examples of where money laundering can take place within councils are provided at appendix 1. These include:

- property and land purchases/sales;
- housing;
- revenues and benefits;
- council tax and business rates refunds;
- grants;
- procurement;
- debtor payments/refunds;
- treasury management;
- licensing;
- adult social care financial transactions;
- legal services;
- regeneration;
- high-value payments; and
- acceptance/refund of cash.

Key responsibilities include:

- Maintaining an Anti-Money Laundering Policy and associated procedures.
- Appointing a Money Laundering Reporting Officer (MLRO) and deputy.
- Providing staff training and awareness.
- Undertaking appropriate due diligence where higher-risk transactions occur.

- Identifying and reporting suspicious activity through internal reporting arrangements and, where appropriate, Suspicious Activity Reports (SARs).
- Maintaining records of investigations and reports.
- Ensuring staff understand their obligations under POCA and the Terrorism Act 2000.
- Adopting a risk-based approach, reflecting the 2026 regulatory changes.

To discharge its duties the Council will ensure the following procedures are maintained:

- Processes for reporting suspicious activity
- Record keeping
- Guidance and training
- Customer due diligence measures

Money Laundering Reporting Officer

The Council has designated **The Section 151 Officer (Chief Finance Officer)** as the Money Laundering Reporting Officer (MLRO), with the **Head of Audit and Assurance and the Deputy Monitoring Officer (Head of Legal)** as the Deputy MLROs. The MLRO responsibilities will include the following actions:

- receiving internal disclosures;
- maintaining confidential records;
- obtaining further information when necessary;
- assessing disclosures;
- deciding whether an external SAR is appropriate;
- liaising with the National Crime Agency (NCA);
- providing advice to employees;
- maintaining the Council's AML framework;
- monitoring trends and risks; and
- reporting appropriate anonymised management information.

Where suspicious activity meets the threshold for reporting, in the opinion of the MLRO, the National Crime Agency (NCA) are the receiving body for reports.

All **Members and employees** must promptly report any knowledge or suspicion of money laundering or terrorist financing to the MLRO in accordance with this policy. Statutory failure-to-disclose offences apply in specified circumstances, principally within the regulated sector; the maximum penalty of 14 years' imprisonment relates to the principal money laundering offences under POCA and should not be stated as the general penalty for failing to make an internal report. Failure to follow this policy may

also result in disciplinary or other appropriate action. **Appendix 3 explains what to do if money laundering activity is suspected.**

Customer Due Diligence and Identification

Where the Council is carrying out an activity within the regulated sector, customer due diligence must be undertaken when required by the Regulations. Outside the regulated sector, proportionate identity, ownership and source-of-funds checks may still be appropriate where the risk warrants them. Appendix 2 provides further guidance. Depending on the nature and level of risk, checks may include:

- who the person or organisation is;
- who ultimately owns or controls a company;
- whether someone is acting for somebody else;
- the purpose of the transaction;
- source of funds where appropriate;
- whether payment details correspond with the party to the transaction; and
- whether additional due diligence is necessary because of elevated risk.

Enhanced due diligence may be required in cases where the person has not been present as part of the identification process and consequently may require the acquisition of other identifiable information. An additional level may also be required in cases highlighted as posing a higher risk of money laundering.

Record Keeping

Records created under this policy must be retained only for the period required by applicable law and the Council's retention schedule. Customer due diligence records relating to regulated-sector activity will normally be retained for five years from the end of the business relationship or completion of the occasional transaction, subject to any lawful extension or overriding requirement. Internal disclosures, SARs and related material must be held securely by the MLRO with access restricted to those who need it for their role.

Guidance and Training

- In support of this policy the Council will: Make all employees and members aware of the requirements and obligations placed on the Council and on themselves as individuals by the anti-money laundering legislation;

- Provide advice and guidance through targeted training to those employees most likely to be exposed to or suspicious of money laundering situations;

- Provide written operational guidance to support the appropriate and timely referral of money laundering suspicions.

Monitoring and Review

This policy will be reviewed by the MLRO at least every three years or earlier in the event of new legislation / best practice.

DRAFT

Appendix 1

Examples of money laundering risk areas.

1. Property and Land Transactions

This is often the highest-risk area .

Examples include:

- Purchasing land with criminal funds.
- Selling council assets through complex corporate structures that obscure beneficial ownership.
- Property development and regeneration schemes involving overseas investors.
- Cash-funded property purchases.

Indicators:

- Unusual ownership arrangements.
- Use of offshore companies.
- Requests for rapid transactions without clear commercial rationale.

2. Right to Buy and Housing Transactions

Examples include:

- Criminal proceeds being used to fund purchases.
- Third parties providing unexplained funding.
- False identities being used in tenancy or housing applications.

3. Procurement and Supplier Payments

Examples include:

- Suppliers established solely to launder money.
- Shell companies winning contracts.
- Over-invoicing or false invoicing arrangements.
- Suppliers with opaque ownership structures.

Indicators:

- Recently formed companies.
- Complex chains of subcontractors.

DRAFT

- Payments requested to unrelated bank accounts.

4. Grants and External Funding

Examples include:

- Community grants awarded to organisations controlled by criminals.
- False grant applications.
- Recycling public funds through associated entities.

Indicators:

- Limited evidence of activity.
- Closely connected organisations applying for multiple grants.
- Unusually complex governance arrangements.

5. Treasury Management and Investments

Examples include:

- Investments involving entities with links to high-risk jurisdictions.
- Complex fund structures obscuring beneficial ownership.

Although treasury activities are generally well regulated, large-value transactions can present AML risks.

6. Cash Collection Services

Examples include:

- Parking income.
- Leisure centres.
- Markets.
- Cemeteries.
- Licensing services.

Cash-intensive services are traditionally more vulnerable because illicit cash can potentially be mixed with legitimate income.

7. Licensing Functions

Examples include:

- Taxi licensing.
- Gambling premises.
- Alcohol licensing.

DRAFT

These sectors are recognised nationally as potentially attractive to organised crime groups because they may involve significant cash transactions.

8. Regeneration and Economic Development

Examples include:

- Large-scale investment projects.
- Joint ventures.
- Development partnerships.
- Town-centre regeneration schemes.

High-value transactions and complex funding arrangements can increase money laundering risk.

9. Adult Social Care

Examples include:

- Third parties paying care charges without a clear source of funds.
- Complex trust arrangements.
- Financial abuse linked to criminal proceeds.

10. Fraud Investigations and Trading Standards

Increasingly, investigations may involve:

- Crypto assets.
- Online fraud.
- Organised crime.
- Modern slavery.
- Counterfeit goods networks.

Red Flags for Council Employees

Employees should be alert to:

- Requests to pay or receive large amounts of cash.
- Complex ownership structures with no obvious reason.
- Reluctance to provide identification.
- Transactions involving high-risk countries.
- Unusual urgency or secrecy.
- Payments from unconnected third parties.

DRAFT

- Use of multiple bank accounts.
- Overly complex funding arrangements.

DRAFT

Appendix 2

When to carry out Customer Due Diligence

The customer due diligence requirements are fact-specific. The questions below are an initial screening tool only and are not exhaustive. Advice should be sought from the MLRO where there is uncertainty about whether an activity falls within the regulated sector or when due diligence is required.

- Is the service you are providing a regulated activity?
- Is the Council charging for the service i.e. is it ‘by way of business?

- Is the Service being provided to a customer other than a UK public authority?

If the answer to all three questions is “yes”, customer due diligence is likely to be required before business is undertaken. Customer due diligence may also be required in other circumstances prescribed by the Regulations, including where there is a suspicion of money laundering or terrorist financing, doubt about previously obtained identification information, an occasional transaction meeting an applicable threshold, or a material change in the customer’s circumstances. If in doubt, consult the MLRO before proceeding.

Regulated activity

The Regulations apply to “relevant persons” acting in the course of business carried on by them in the UK and identify “relevant persons” as:

- credit institutions;
- financial institutions;
- auditors, insolvency practitioners, external accountants and tax advisers;
- independent legal professionals;
- trust or company service providers;
- estate agents and letting agents;
- high value dealers;
- casinos;
- art market participants;
- cryptocurrency exchange providers;
- custodian wallet providers.

Although Local Authorities are not “relevant persons” for the purpose of the Regulations, certain activities undertaken by accountancy, audit and legal services undertaken may fall within the Regulations.

Regulated activity is defined as the provision ’by way of business’ of advice about tax affairs; accounting services; treasury management, investment or other financial services; audit services; estate functions; services involving the formation, operation

or arrangement of a company or trust or, dealing in goods wherever a transaction involves a cash payment of £10,000 or more.

By way of business

Most Council activities are not 'by way of business' even if there is a charge for the service. If the service provided is part of our statutory duties or provided to members of the public on a not-for-profit basis, then this is not captured by the Regulations.

Likewise, if services provided are funded by the Council and not the service user they do not fall under the Regulations.

Services to UK public authorities

Where services are provided to other UK public bodies (or 3rd parties authorised to act on their behalf) these services do not fall within the Regulations and customer due diligence is not necessary (unless there are grounds to suspect money laundering).

If you are unsure whether you need to carry out customer due diligence, then you should contact the MLRO.

Identity checks

Where you need to carry out customer due diligence then you must seek evidence of identity, for example:

- Checking with the customer's website to confirm their business address;
- Conducting an on-line search via Companies House to confirm the nature and business of the customer and confirm the identification of any directors;
- Seeking evidence from the key contact of their personal identity, for example, their passport, and position within the organisation.

The requirement for customer due diligence applies immediately for new customers and should be applied on a risk sensitive basis for existing customers. Ongoing customer due diligence must also be carried out during the life of a business relationship but should be proportionate to the risk of money laundering and terrorist funding, based on the officer's knowledge of the customer and a regular scrutiny of the transactions involved.

If at any time, you suspect that a client or customer for whom you are currently, or are planning to carry out a regulated activity, is carrying out money laundering or terrorist financing, or had lied about their identify then you must report this to the MLRO.

In certain circumstances enhanced customer due diligence must be carried out. For example, where:

- The customer has not been physically present for identification;

- The customer is a politically exposed person (PEP), or a family member or known close associate of a PEP. This includes domestic and foreign PEPs and persons entrusted with prominent public functions by an international organisation. The nature and extent of enhanced due diligence must reflect the assessed risk and the applicable statutory requirements;

- There is a beneficial owner who is not the customer – a beneficial owner is any individual who holds more than 25% of the shares, voting rights or interest in a company, partnership or trust.

Enhanced customer due diligence could include any additional documentation data or information that will confirm the customer's identity and/or the source of the funds to be used in the business transaction. If you believe that enhanced customer due diligence is required, then you must consult the MLRO prior to carrying it out.

Customer due diligence records and details of the relevant transactions(s) for that client must be retained for at least 5 years after the end of the business relationship.

Customer due diligence records must be stored securely in the approved Council system and made available to the MLRO or relevant supervisory authority when lawfully required. Copies should not routinely be emailed to the MLRO unless requested or required by an approved procedure. Personal data and SAR-related information must be handled on a need-to-know basis in accordance with data-protection, confidentiality, retention and information-security requirements.

DRAFT

Recognising suspicious activity that may be linked to Money Laundering

It is impossible to give a definitive list of ways to spot money laundering but the following suggested areas which taken alone or with other factors, may increase the risk of potential money laundering:

- A new client;

- A secretive client e.g. refuses to provide requested information without a reasonable explanation;

- Concerns about the honesty, integrity, alleged association with criminality, or location of a client;

- Illogical third-party transactions: unnecessary routing or receipting of funds from third parties or through third party accounts;

- Involvement of an unconnected third party without logical reason or explanation;

- Payment of substantial sums in cash or a large cash deposit (a single transaction or a series of linked transactions totalling £10,000 or more). The Council expects large value payments to be made by other means, so any request to make such payments in cash should be treated as suspicious;
  (It should be noted that the threshold for large cash payments has been amended to £10,000 where previously stated as Euros. Legislative changes in 2026 resulted in this amendment but Councils must still consider equivalent sums in other currency with the same suspicion.

- Absence of obvious legitimate source of funds;

- Payment of monies then cancellation of transactions and request for return of funds;

- Over-payment of invoices with a subsequent request for a refund;

- Movement of funds overseas, particularly to a higher risk country or tax haven;

- Where, without reasonable explanation, the size, nature, and frequency of transaction or instructions (or the size, location of type of client) is out of line with normal expectations;

- Cancellation or reversal of an earlier transaction;

- Requests for release of client account details other than on the normal course of business;

- Companies and trusts: extensive use of corporate structures and trusts in circumstances where the client's needs are inconsistent with the use of such structures;

- Over complicated financial systems;

- Poor business records or internal accounting controls;

- A previous transaction for the same client that has been or should have been reported to the MLRO;

- Unusual property investment transactions if there is no linked substantive property transaction involved (surrogate banking);

- Property related transactions where funds are received for deposits or prior completion from an unexpected source or where instructions are given for the settlement of funds to be paid to an unexpected destination;

- More than one solicitor used in a sale or purchase or there is an unexplained or unusual geographical use of the solicitor in relation to property transactions.

DRAFT

Appendix 3

What to do if money laundering activity is suspected?

Where you know or suspect that money laundering or terrorist-financing activity is taking or has taken place, or you are concerned that your involvement may amount to a prohibited act, report the matter to the MLRO as soon as practicable. Urgent, ongoing or imminent transactions must be escalated immediately and must not proceed contrary to the MLRO's direction. The referral should be made using the form at Appendix 4.

If in any doubt, seek advice from the MLRO or a Deputy MLRO. If the MLRO is unavailable or has a conflict of interest, report the matter to a Deputy MLRO using the confidential reporting route.

You must comply with this policy and report concerns promptly. A statutory failure-to-disclose offence may arise where the relevant legal conditions are met, particularly in the regulated sector.

The report must include as much detail as possible, for example:

- Full details of the people involved (including yourself, if relevant). For example, name, date of birth, address, company names, directorships, phone numbers (this list is not exhaustive);
- Full details of the nature of their/your involvement;
- The types of money laundering activity involved;
- The dates of such activities, including whether the transactions have happened, are ongoing or are imminent;
- Where they took place;
- How they were undertaken;
- The (likely) amount of money/assets involved;
- Why, exactly, you are suspicious – the NCA will require full reasons;
- Any other available information to enable the MLRO to make a sound judgment as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable him to prepare his report to the NCA, where appropriate;

- You should also enclose copies of any relevant supporting documentation.

Once you have reported the matter to the MLRO you must follow any directions given to you. You must not make any further enquiries into the matter yourself. All members of staff are required to cooperate with the MLRO and the authorities during any subsequent money laundering investigation.

Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering; otherwise, you may commit an offence.

MLRO actions

On receipt of a report, the MLRO is required to determine if a disclosure is required to the NCA.

The MLRO will consider the report and any other available internal information thought to be relevant, For example:

- other transaction patterns and volume;
- the length of any business relationship involved;
- the number of any one-off transactions and linked one-off transactions;
- any identification evidence held; and
- undertake such other reasonable inquiries he thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required.

When the report and any other relevant information have been evaluated the MLRO will make a determination as to whether:

- there is evidence of actual money laundering taking place or
- there are reasonable grounds to suspect that is the case.

If, after considering the disclosure and available information, the MLRO knows or suspects, or has reasonable grounds to know or suspect, money laundering or terrorist financing in circumstances requiring an external report, the MLRO will submit a Suspicious Activity Report (SAR) to the National Crime Agency. Where a proposed act may constitute a prohibited act and a defence is required before it can proceed, the MLRO will consider whether to seek a Defence Against Money Laundering (DAML). Only the affected transaction or activity should be paused, and only where required by law or directed by the MLRO.

If the MLRO concludes that an external report is not legally required, the decision and reasons must be recorded. Any reliance on a statutory exception, reasonable excuse

or other legal basis must be considered carefully and, where appropriate, with Legal Services. The decision whether an underlying transaction may proceed is separate from the decision whether to submit a SAR.

Where the MLRO concludes that there are no reasonable grounds for suspicion, that conclusion and the reasons for it must be recorded. The MLRO may then advise the relevant service whether there is any AML reason why the transaction should not proceed, without disclosing confidential SAR-related information more widely than necessary.

Where a DAML has been requested, the relevant act must not proceed unless and until a defence is available under the statutory process, including through expiry of the applicable notice period without refusal. The MLRO will provide directions on the affected transaction and record the outcome.

All disclosure reports referred to the MLRO and subsequent reports to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

DRAFT

Appendix 4

MONEY LAUNDERING REPORTING OFFICER DISCLOSURE FORM

Date of disclosure	
Officer making the disclosure (including job title)	
Contact details	

Subject details	
Surname	
Forename(s)	
Date of Birth	
Or if the matter relates to a company	
Company name	
Address	
Company number (if known)	
Reason for disclosure	

DRAFT