Anti-Fraud and Corruption Strategy

Gedling Borough Council

June 2026

This strategy sets out the Council's corporate framework for preventing, detecting, investigating and responding to fraud, bribery, corruption and wider economic crime. It supports strong governance, protects public funds and aligns with CIPFA good practice and the relevant legislative framework.

Executive Summary

This Anti-Fraud and Corruption Strategy sets out Gedling Borough Council's corporate approach to preventing, detecting, investigating and responding to fraud, bribery, corruption and wider economic crime. It is designed to protect public funds, public assets and public confidence, and to provide a clear framework for governance, accountability, reporting and continuous improvement.

- The strategy is aligned to the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption and **Fighting Fraud and Corruption Locally**, reflecting recognised good practice for local government.
- It references the key legislative framework, including the **Fraud Act 2006**, the **Bribery Act 2010**, the **Public Interest Disclosure Act 1998**, the **Proceeds of Crime Act 2002**, and the **Economic Crime and Corporate Transparency Act 2023**, including the **failure to prevent fraud** offence that came into force on **1 September 2025**.
- The Council adopts a zero-tolerance approach and expects high standards of honesty, integrity and accountability from members, employees, contractors, suppliers, partners and others acting on its behalf.
- The strategy promotes a risk-based approach built around strong leadership, fraud risk assessment, proportionate controls, due diligence, effective reporting routes, proactive counter fraud activity, proper investigation and organisational learning.
- It reflects the reasonable procedure's themes associated with the failure to prevent fraud offence: top-level commitment, risk assessment, proportionate

procedures, due diligence, communication8 and training, and monitoring and review.

- The accompanying appendices provide supporting detail through a whistleblowing summary, a fraud response plan, a practical anti-fraud and corruption action plan for 2026-27, and a standalone anti-money laundering policy.
- Together, the strategy and appendices provide the Council with a clear framework for prevention, response, assurance and continuous improvement.

Table of Contents **Page**

1. Introduction

1.1 Legislative and Regulatory Framework

The Council's counter fraud arrangements are shaped by a range of statutory, regulatory and professional requirements. This strategy should therefore be read in the context of the legal framework for fraud, bribery, corruption, economic crime, whistleblowing, recovery of criminal property, and good governance in local government. In particular, the Council recognises the importance of maintaining proportionate and well-evidenced controls that reflect both CIPFA good practice and the expectations associated with the Economic Crime and Corporate Transparency Act 2023.

- **Public Interest Disclosure Act 1998** – supports protection for individuals who raise concerns in the public interest.
- **Proceeds of Crime Act 2002** – provides powers relevant to the recovery of criminal property and the handling of criminal proceeds.
- **Fraud Act 2006** – establishes the principal criminal offences of fraud, including fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.
- **Bribery Act 2010** – provides the framework for preventing and addressing bribery and includes the corporate offence of failure to prevent bribery.
- **Economic Crime and Corporate Transparency Act 2023** – strengthens the UK response to economic crime and introduced the corporate offence of **failure to prevent fraud**, effective from **1 September 2025**. The Council will have regard to the reasonable procedure's principles associated with that offence, including top-level commitment, risk assessment, proportionate procedures, due diligence, communication and training, and monitoring and review.
- **Local Government legislation and governance requirements** – place duties on the Council to secure proper administration of its financial affairs, maintain sound internal control, and uphold high standards of conduct and governance.
- **Public Sector Fraud Authority** – provides leadership, guidance, standards and initiatives to help public bodies understand, prevent, detect and respond to fraud against the public sector. This includes support for data-led prevention, fraud risk assessment, counter fraud capability and the operation of the National Fraud Initiative.
- **CIPFA Code of Practice on Managing the Risk of Fraud and Corruption** and **Fighting Fraud and Corruption Locally** – provide the professional good practice framework that underpins this strategy and its implementation.

The reasonable procedures model is the framework set out in UK government guidance to help organisation's prevent fraud committed by employees or other associated persons for the organisation's benefit or, in some cases, for the benefit of a client. It is not a fixed checklist; rather, it is a set of six risk-based principles intended to help

organisation's design, evidence and keep under review proportionate fraud prevention arrangements that reflect their size, structure, activities and exposure to risk.

- **Top-level commitment** – senior leadership should set a clear tone that fraud is unacceptable, support an open and ethical culture, and ensure fraud prevention is taken seriously across the organisation.
- **Risk assessment** – organisation's should identify and assess where and how fraud risks may arise, including risks linked to services, transactions, third parties, incentives and control weaknesses.
- **Proportionate risk-based fraud prevention procedures** – controls and procedures should be designed in proportion to the risks identified, with practical measures that are realistic, targeted and capable of operating effectively.
- **Due diligence** – organisation's should carry out appropriate checks on employees, contractors, suppliers, agents, partners and other associated persons, particularly where activities are higher risk.
- **Communication and training** – policies, expectations and reporting routes should be communicated clearly, with training and awareness activity tailored to the level of fraud risk and the roles involved.
- **Monitoring and review** – organisation's should test, review and update their arrangements regularly so that they remain effective, reflect lessons learned and respond to changing risks.

Gedling Borough Council is committed to protecting public funds, public assets and public trust. Fraud, bribery, corruption and wider economic crime divert resources from essential local services, damage confidence in the Council and undermine effective governance. This strategy sets out how the Council will prevent, detect, investigate and respond to fraud and corruption across its services, systems, partnerships, companies, contractual arrangements and wider delivery models.

The strategy aligns with the principles of **Fighting Fraud and Corruption Locally** and the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption. It reflects the expectation that counter fraud arrangements should be led from the top, integrated into governance and risk management, informed by regular fraud risk assessment, supported by proportionate controls and resources, and strengthened through reporting, action and continuous review.

The Council recognise's the significance of the **Economic Crime and Corporate Transparency Act 2023**, including the corporate offence of **failure to prevent fraud** that came into force on **1 September 2025**. Although that offence applies directly to organisation's meeting the statutory threshold, the Council regards the associated reasonable procedures model as relevant good practice for public sector fraud prevention and for the management of risks arising from employees, contractors,

suppliers, agents, delivery partners and other associated persons acting on the Council's behalf or in connection with Council business.

The Council adopts a zero-tolerance approach to fraud, bribery, corruption and dishonest conduct. This strategy applies to members, employees, agency workers, contractors, consultants, suppliers, partners, volunteers and any other person or organisation working for, with or on behalf of the Council.

The intended outcomes of this strategy are to reduce the risk of loss, strengthen the Council's control environment, promote a culture of integrity and openness, ensure allegations are handled properly, support recovery and enforcement action including civil and criminal action and sanctions where appropriate, and provide assurance that the Council is meeting its governance responsibilities in relation to fraud and corruption risk.

2. Policy Statement

Gedling Borough Council will maintain a proportionate, risk-based and intelligence-led counter fraud framework embedded within its governance arrangements. The Council's policy is to prevent fraud and corruption wherever possible, detect concerns early, investigate them professionally and fairly, take robust action where wrongdoing is identified, and learn from incidents so that controls and arrangements continue to improve.

To give effect to this policy statement, the Council will apply the following core principles and commitments across its counter fraud arrangements:

- Demonstrate clear leadership and a strong tone from the top that fraud, bribery, corruption and economic crime are unacceptable.
- Identify and assess fraud and corruption risks across services, systems, partnerships, projects, contracts and new delivery models.
- Maintain proportionate controls, due diligence, oversight and assurance arrangements, including in relation to third parties and associated persons.
- Encourage concerns to be reported promptly and protect those who raise them in good faith.
- Use proactive and reactive counter fraud techniques, including intelligence, data matching, analytics and targeted review work.
- Pursue disciplinary, regulatory, civil and criminal action and sanctions where it is lawful, proportionate and in the public interest to do so.
    - **Civil action and sanctions** may include civil recovery, compensation, injunctions, insurance claims and other financial remedies.
    - **Criminal action and sanctions** may include referral to the police, prosecution, cautions and confiscation proceedings.

- Monitor effectiveness, report through governance channels and review this strategy regularly in light of changing risks, legislation and good practice.

3. Culture

An effective anti-fraud culture depends on visible leadership, ethical behaviour, openness and accountability. In line with CIPFA and Fighting Fraud and Corruption Locally, the Council will foster a culture in which fraud risk is understood as a core management issue rather than solely an audit or investigation issue. Counter fraud responsibilities must therefore be embedded within governance, operational management, commissioning, procurement, contract management and decision-making.

This culture is supported through clear expectations, effective supervision, robust controls, declarations of interest, gifts and hospitality arrangements, safe speaking-up channels, and consistent action when standards are breached. Key supporting documents and mechanisms include:

- Financial Regulations and scheme of delegation
- Local Code of Corporate Governance
- Contracts and Procurement Rules
- Codes of conduct for members and employees
- Declarations of interest, gifts and hospitality requirements
- HR policies, recruitment checks and disciplinary procedures
- Whistleblowing, fraud response, risk management and information governance arrangements

4. Responsibilities

4.1 Overall Responsibility

Countering fraud and corruption is a shared responsibility. The governing body, statutory officers, senior managers, employees, members and those acting on the Council's behalf all have a role in preventing wrongdoing, maintaining effective controls, identifying risks, challenging poor practice and reporting concerns.

- **Members and the Audit Committee** are responsible for setting expectations around ethical conduct, receiving assurance on the adequacy of counter fraud arrangements and supporting a strong control environment.
- **The Senior Leadership Team and Assistant Directors** are responsible for embedding this strategy, assessing risk, maintaining proportionate controls, ensuring staff awareness and taking prompt action where issues arise.
- **The Section 151 Officer** is responsible for ensuring appropriate financial stewardship and for supporting robust arrangements to prevent, detect and respond to fraud and corruption.

- **The Monitoring Officer** is responsible for supporting compliance, standards and proper governance arrangements, including matters relating to conduct and legality.
- **Internal Audit and other assurance functions** support the Council through review, advice, proactive work and investigation or referral arrangements as appropriate.
- **All employees and members** must act with honesty and integrity, comply with policies and procedures, remain alert to risk and report concerns promptly.
- **Contractors, suppliers, partners and other associated persons** are expected to comply with the Council's standards, maintain accurate records, report concerns and cooperate with any review or investigation.

4.2 Reasonable Procedures and Associated Persons

In line with the Council's approach to the Economic Crime and Corporate Transparency Act 2023, services must consider where fraud risks may arise through associated persons and third parties. This includes ensuring appropriate due diligence, contractual expectations, oversight, segregation of duties, record keeping, escalation routes and review arrangements in areas where external parties act for or on behalf of the Council.

5. Prevention

Prevention is the Council's first line of defence. Consistent with CIPFA's framework and with the reasonable procedures approach associated with the **Economic Crime and Corporate Transparency Act 2023**, the Council will apply fraud prevention measures that are proportionate to the nature, scale and complexity of the risks it faces. This includes taking steps to prevent fraud committed for the benefit of the organisation or in connection with Council business by employees or by associated persons such as contractors, suppliers, agents, subsidiaries, delivery partners and others acting on the Council's behalf.

5.1 Council Approach to Prevention

The Council's prevention approach is based on visible leadership, fraud risk assessment, proportionate internal controls, due diligence, secure systems, clear procedures, transparency requirements, training and ongoing review. It is designed to reflect both CIPFA good practice and the reasonable procedures model associated with the failure to prevent fraud offence, while remaining proportionate to the Council's scale, operating environment and risk profile. The prevention approach is supported by the Anti-Fraud and Corruption Action Plan 2026-27, which translates these principles into practical actions on governance, fraud risk assessment, reasonable procedures, third-party due diligence, awareness and training, data-led proactive work, whistleblowing and reporting, and monitoring and assurance.

- **Leadership and governance:** members, senior officers and statutory officers will set the tone, endorse expectations, review arrangements regularly and ensure counter fraud remains a governance priority.

- **Fraud risk assessment:** fraud and corruption risks will be identified and reviewed across key services, systems, projects, grants, procurement, commissioned services and partnerships, with priority actions taken forward.
- **Reasonable procedures and internal controls:** the Council will maintain proportionate procedures, approval routes, reconciliations, supervisory checks, exception reporting, secure systems access and documented processes, and will review these against the six reasonable procedures themes where relevant.
- **Third-party due diligence:** appropriate checks, contract clauses, transparency requirements and monitoring arrangements will be applied to suppliers, contractors, delivery partners, grant recipients and other relevant third parties.
- **Awareness, training and reporting:** expectations, risks, whistleblowing arrangements and reporting routes will be communicated clearly, with enhanced awareness for higher-risk roles and activities.
- **Data and proactive work:** the Council will use data matching, data analytics, exception reporting, targeted review work and the National Fraud Initiative to strengthen prevention and early identification of risk.
- **Monitoring and assurance:** prevention arrangements, incidents, control weaknesses, lessons learned and progress against the action plan will be reviewed so that the Council can strengthen its response over time.

5.2 National Fraud Initiative

The National Fraud Initiative (NFI) is a data matching exercise operated by the Public Sector Fraud Authority on behalf of the Cabinet Office to help prevent and detect fraud and error across the public sector. It matches electronic data within and between participating organisations to identify inconsistencies that may require further review. A match does not in itself prove fraud or wrongdoing, but it may highlight cases that warrant enquiry, verification or investigation.

The Council can use the NFI to support both prevention and detection work. This may include reviewing data matches relating to areas such as payroll, pensions, creditors, council tax, business rates, housing, licensing, parking permits, insurance claims and other datasets specified through the NFI programme. The Council will use NFI outputs as part of a wider risk-based counter fraud approach, including prioritising review work, identifying control weaknesses, following up potential anomalies, recovering losses where appropriate and improving local controls and awareness.

The Council may also use guidance, standards, tools and good practice published by the **Public Sector Fraud Authority** to strengthen its wider counter fraud arrangements. This may include support for fraud risk assessment, prevention planning, data-led counter fraud activity, training and awareness, and the continuous improvement of local controls, governance and assurance.

Participation in the NFI must be managed in accordance with the relevant statutory powers, the Code of Data Matching Practice, data protection requirements and the Council's own governance arrangements. The Council will ensure that NFI matches are reviewed appropriately, that decisions and outcomes are recorded, and that learning from the exercise is used to strengthen fraud prevention arrangements. The Council will also have regard to relevant guidance, standards and good practice published by the **Public Sector Fraud Authority** in developing its wider counter fraud arrangements.

5.3 Types of Fraud and Who May Commit Them

Fraud and corruption can take many forms and may be committed by individuals or organisations both inside and outside the Council. Understanding the main fraud risks helps services design proportionate controls, target training and respond appropriately when concerns arise. The following examples are not exhaustive but reflect common risks in local government.

- **Internal fraud** – for example payroll fraud, false overtime claims, expenses abuse, misuse of purchasing cards, theft, falsification of records or abuse of position. This type of fraud may be committed by employees, agency workers or others with access to Council systems, assets or information.
- **External fraud** – for example false applications, identity fraud, false claims, undeclared changes in circumstances, creditor fraud or mandate fraud. This type of fraud may be committed by members of the public, businesses, customers, claimants, tenants, suppliers or organised fraud networks.
- **Procurement and contract fraud** – for example collusion, bid rigging, false invoicing, duplicate invoicing, overcharging, undisclosed conflicts of interest or manipulation of contract processes. This type of fraud may be committed by suppliers, contractors, delivery partners or by employees working alone or in collusion with external parties.
- **Bribery and corruption** – for example offering, giving, requesting or accepting an improper payment, gift, hospitality or other advantage to influence a decision. This may involve employees, members, contractors, suppliers, agents or other third parties.
- **Grant, scheme and financial support fraud** – for example false declarations, misuse of grant funding, ineligible claims or diversion of funds. This may be committed by applicants, recipients, partner bodies or, in some cases, internal officers where controls are weak.
- **Tenancy, housing, council tax and business rates fraud** – for example subletting, false occupancy claims, discount abuse, false exemptions or misrepresentation of liability. This may be committed by tenants, residents, ratepayers, landlords, businesses or third parties acting on their behalf.

- **Cyber-enabled and data-related fraud** – for example phishing, impersonation, payment diversion, business email compromise or misuse of data to facilitate fraud. This may be committed by external attackers, organised crime groups or individuals seeking to exploit weaknesses in systems or processes.
- **Fraud involving associated persons** – for example fraud committed by a contractor, agent, subsidiary, consultant or delivery partner acting for or on behalf of the Council or in connection with Council business. This is particularly relevant to the Council's approach to third-party risk, due diligence and the reasonable procedures model.

6. Reporting Concerns

Anyone who suspects fraud, bribery, corruption or related misconduct should report it as soon as possible. Concerns may be raised through any of the following routes:

- **Your Line Manager**
- **Directors:** Mike Avery, Franchesca Whyley, Sarah Troman, Mike Hill
- **Internal Audit:** Max Armstrong - BDO
- **Section 151 Officer:** Tina Adams, Chief Finance Officer
- **Monitoring Officer:** Franchesca Whyley
- **Human Resources:** Jennifer Lovett
- **Whistleblowing Contact / Route:** Appendix 1.

The Council will support a speak-up culture and will not tolerate retaliation against any person who raises a concern in good faith. Where appropriate, matters will also be referred to external bodies such as the police, external audit, insurers, the Department for Work and Pensions, HMRC, the National Fraud Initiative, professional regulators or other agencies with relevant powers or responsibilities. Further information on the National Fraud Initiative should be made available through the Council's privacy notice and the Cabinet Office National Fraud Initiative guidance.

Concerns should be raised honestly, responsibly and in good faith. The Council recognises that some allegations may not be substantiated after investigation, and this will not in itself amount to wrongdoing where the concern was raised genuinely. However, malicious, vexatious or deliberately false allegations are unacceptable. Where it is established that a concern has been raised as part of a personal vendetta or for another improper purpose, the Council may take appropriate action in line with its relevant policies, procedures and contractual arrangements.

7. Detection and Investigation

The Council will use both proactive and reactive counter fraud techniques. These may include data matching, data analytics, management review, internal audit work,

intelligence sharing, whistleblowing disclosures, exception reporting and targeted exercises in high-risk areas. Investigations will be conducted lawfully, proportionately and fairly, with appropriate referrals to enforcement or regulatory bodies where required.

7.1 Investigation and Response

Allegations will be assessed promptly to determine the appropriate response, including whether immediate safeguarding action is required to secure records, systems, assets or evidence. Investigations will be carried out by officers with the appropriate skills, independence and authority. Where appropriate, outcomes may include the following forms of action and sanctions:

- **Civil action and sanctions** such as civil recovery, compensation, injunctions, insurance claims and other financial remedies.
- **Criminal action and sanctions** such as referral to the police, prosecution, cautions and confiscation proceedings.
- **Other action** such as management action, disciplinary action, regulatory notification, insurance notification, recovery action or wider control improvements.

7.2 Learning and Recovery

Where fraud or corruption is identified, the Council will consider opportunities to recover losses, protect future public funds and strengthen its arrangements. Significant cases should lead to a review of root causes, control weaknesses, assurance findings and learning points so that improvements can be implemented promptly and shared where useful.

8. Training and Communications

Training and communication are essential to maintaining an effective anti-fraud culture. The Council will ensure that members and employees understand expected standards of behaviors, the fraud risks relevant to their roles, warning signs that may indicate wrongdoing, and how to report concerns. Awareness activity will be proportionate, refreshed regularly and targeted where risk is higher.

Training may include corporate induction, periodic refresher learning, manager briefings, targeted sessions for higher-risk services and updates following legislative or policy change. Communication should also reinforce the Council’s zero-tolerance approach, speak-up culture, whistleblowing arrangements and expectations of third parties working with the Council.

9. Monitoring and Review

The Council will monitor the effectiveness of this strategy through its governance framework, including management oversight, Internal Audit, risk management

arrangements and Audit Committee reporting. Performance information, emerging threats, investigation outcomes, control weaknesses and progress against improvement actions will be reviewed so that the Council can respond to changing risks and maintain effective arrangements.

- **Strategy and policy review:** this strategy and related documents will be reviewed periodically and updated to reflect legislative change, CIPFA and sector guidance, organisational learning and changing fraud risk.
- **Post-incident review:** following significant cases or control failures, the Council will identify lessons learned and implement improvement actions.
- **Audit Committee oversight:** the Audit Committee will receive appropriate assurance on the adequacy of counter fraud arrangements, key risks and progress against any action plan.

10. Associated Policies

This strategy should be read alongside the Council's wider governance and risk and control framework, including the following documents where applicable:

- Corporate Code of Governance
- Financial Regulations and scheme of delegation
- Contracts and Procurement Rules
- Member and employee codes of conduct
- Whistleblowing Policy
- Fraud Response Plan
- Anti-Fraud and Corruption Action Plan
- Risk Management Strategy
- Anti-Money Laundering Policy
- Policies and procedures relevant to declarations, gifts and hospitality, recruitment, disciplinary action, information governance and system security

Appendix 1 - Whistleblowing Policy Summary

The Council is committed to the highest standards of openness, integrity and accountability. Whistleblowing is an important part of the Council's wider counter fraud and governance framework because it helps concerns to be raised at an early stage and supports the prevention, detection and investigation of wrongdoing. This summary should be read alongside the Council's full Whistleblowing Policy and related procedures.

1.1 Purpose and Scope

The purpose of the Whistleblowing Policy is to encourage employees and others working with the Council to raise genuine concerns about suspected wrongdoing, unsafe practice, unlawful conduct, fraud, bribery, corruption, financial irregularity, abuse of authority, safeguarding concerns or attempts to conceal such matters. The policy supports the principles of the **Public Interest Disclosure Act 1998** by making clear that concerns raised appropriately and in the public interest will be taken seriously.

The Councils Whistleblowing policy is a separate policy document available to both Council Employees and Members of the Public. The Policy is available on the Councils Internet.

Appendix 2 - Fraud Response Plan

This Fraud Response Plan sets out the Council's high-level approach when allegations or suspicions of fraud, bribery, corruption or related irregularity arise. It is designed to support a prompt, proportionate and well-governed response that protects evidence, secures public funds, supports fair treatment and ensures the right officers are involved at the right time.

2.1 Objectives

- Protect public funds, assets, systems and records.
- Ensure allegations are assessed and handled consistently, fairly and without unnecessary delay.
- Secure and preserve evidence, including digital records and financial information.
- Support appropriate referrals to HR, legal services, insurers, police, regulators or other external bodies.
- Identify lessons learned, recovery opportunities and control improvements.

2.2 Immediate Actions

- Record the allegation or concern promptly and preserve the initial information received.
- Notify the appropriate senior officer, Internal Audit, the Section 151 Officer, the Monitoring Officer, HR or other designated officer, depending on the circumstances.
- Consider whether urgent action is needed to secure systems access, suspend payments, retain documents, protect assets or prevent further loss.
- Avoid alerting the subject of the allegation where this could compromise evidence or prejudice an investigation.
- Consider whether legal, HR, ICT, insurance, safeguarding or communications advice is required at an early stage.

2.3 Assessment and Investigation

An initial assessment should determine the seriousness of the allegation, the potential financial or reputational impact, the immediate control risks, whether criminal conduct may be involved, and who should lead the response. Investigations should be proportionate and carried out by officers with the appropriate independence, authority and expertise. The Council will maintain appropriate records of decisions, evidence, actions taken and outcomes.

2.4 Possible Outcomes

- No further action where concerns are not substantiated.
- Management action to address process weakness or control failure.
- Disciplinary action or contract management action.

- Civil action and sanctions, including civil recovery, compensation, injunctions, insurance claims or other financial remedies.
- Criminal action and sanctions, including referral to the police, prosecution, cautions, confiscation proceedings, or referral to regulators, external audit or other external agencies.
- Post-incident review and strengthening of controls, training or oversight arrangements.

2.5 Associated Persons and Reasonable Procedures

Where a case involves a contractor, supplier, partner, agent or other associated person, the Council should consider whether contractual controls, due diligence, oversight, record keeping, escalation routes and monitoring arrangements operated as intended. In line with the Council's approach to the **Economic Crime and Corporate Transparency Act 2023**, cases of this kind should also be reviewed to identify whether improvements are needed in top-level commitment, risk assessment, proportionate procedures, due diligence, communication and training, or monitoring and review.

Appendix 3 - Anti-Fraud and Corruption Action Plan 2026-27

This action plan translates the strategy into practical activity for 2026-27. It is intended to support continuous improvement, provide a basis for monitoring by management and the Audit Committee, and demonstrate alignment with CIPFA good practice, Fighting Fraud and Corruption Locally and the Council's approach to the reasonable procedures model associated with the failure to prevent fraud offence.

Theme	Action	Lead	Target / Measure	Timescale	RAG Status
Leadership and governance	Review the Anti-Fraud and Corruption Strategy, Fraud Response Plan and supporting arrangements annually and report progress through the Council's governance framework.	Section 151 Officer / Internal Audit	Annual review completed and reported to Audit Committee.	Q1 2026-27	Green
Fraud risk assessment	Update the fraud risk assessment for key services.	Service Managers	Updated risk assessment completed and priority actions identified.	Q2 2026-27	Amber
Reasonable procedures	Review current arrangements against the six reasonable procedures themes linked to the failure to prevent fraud offence and identify any gaps requiring improvement.	Section 151 Officer / Monitoring Officer / Internal Audit	Gap assessment completed and improvement actions agreed.	Q2 2026-27	Amber

Third-party due diligence	Strengthen due diligence, fraud clauses, transparency requirements and monitoring arrangements for suppliers, contractors, delivery partners and other relevant third parties.	Procurement / Legal / Service Managers	Revised approach embedded in relevant procurement and contract management activity.	Q3 2026-27	Amber
Awareness and training	Deliver counter fraud awareness activity for members and staff, with targeted training for higher-risk areas such as procurement, finance, system administration and contract management.	HR / Internal Audit / Relevant Managers	Training delivered and attendance or completion monitored.	Q3 2026-27	Amber
Data and proactive work	Use proactive counter fraud techniques such as data matching, analytics, exception reporting and targeted review work in higher-risk areas.	Internal Audit / Relevant Services	Programme of proactive work completed and outcomes reported.	Q4 2026-27	Amber
Whistleblowing and reporting	Review awareness of whistleblowing and reporting routes to ensure that staff,	Monitoring Officer / HR / Internal Audit	Updated communications issued and	Q2 2026-27	Amber

	members and third parties know how to raise concerns.		routes clearly signposted.		
Monitoring and assurance	Develop periodic reporting on fraud risk, cases, outcomes, lessons learned and progress against this action plan.	Section 151 Officer / Internal Audit	Regular update reports provided through the governance framework to Audit Committee.	Quarterly	Amber

The action plan should be kept under review during the year and updated to reflect changes in legislation, risk, organisational priorities, emerging threats, completed actions and lessons learned from cases or assurance work. Timescales and RAG status should be reviewed regularly so that progress, slippage and emerging issues can be clearly reported through the Council's governance framework. An ongoing agenda item at Senior Leadership Team will also support the identification of high-risk areas and help inform priorities, oversight and any further action required.

In the first instance, the actions within this plan have been assigned an amber RAG status to reflect that further work is needed to define the detailed scope, baseline position, delivery requirements and measures of success for each area.

Appendix 4 - Anti-Money Laundering Policy

4.1 Introduction

The Council is committed to maintaining the highest standards of honesty, integrity and accountability and to protecting public funds and the wider public interest. Although local authorities are not generally within the regulated sector for the purposes of the UK money laundering regime, they may still encounter transactions, arrangements or behaviours that give rise to suspicion of money laundering, terrorist financing or the handling of criminal property. The Council therefore adopts this Anti-Money Laundering Policy to support proportionate safeguards, clear reporting arrangements and staff awareness.

This policy should be read alongside the Council's Anti-Fraud and Corruption Strategy, Financial Regulations, procurement and contract management arrangements, Whistleblowing Policy, information governance requirements and any relevant guidance issued by the Section 151 Officer, Monitoring Officer. It reflects the principles set out in the Proceeds of Crime Act 2002, the Terrorism Act 2000 and current sector good practice for local authorities.

4.2 Scope and Purpose

This policy applies to all employees, agency workers, contractors, consultants, members and others working for or on behalf of the Council where they may encounter financial transactions, property dealings, payments, grants, contracts, settlements, disposals, debtor arrangements, licensing, enforcement or other activities that could create a money laundering risk. It aims to maintain high standards of conduct, help officers recognise potential warning signs and ensure that concerns are reported appropriately and without delay.

- Set out the Council's proportionate approach to anti-money laundering risk.
- Support employees and members to identify and escalate suspicious activity.
- Reduce the risk that Council services, assets, contracts or financial systems are used to launder criminal property.
- Ensure concerns are considered lawfully, confidentially and with appropriate referral where necessary.

4.3 What is Money Laundering?

Money laundering is the process by which criminal property is handled, disguised, transferred, converted or integrated into legitimate business or financial activity so that its origins are obscured. Criminal property is broadly defined and is not limited to cash. It may include money, goods, land, rights, assets or any benefit derived from criminal conduct. The offences are wide in scope and may apply even where the underlying criminal conduct took place elsewhere.

- Concealing, disguising, converting, transferring or removing criminal property.
- Entering into or becoming concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property.
- Acquiring, using or possessing criminal property.
- Failing to disclose knowledge or suspicion where there is a reporting obligation.
- Tipping off, namely disclosing information in a way that could prejudice an investigation or alert a person that a report has been made.

Possible indicators may include unusual cash payments, requests to make or receive payments through third parties, overpayments followed by refund requests, pressure for urgent transactions without clear rationale, complex ownership or beneficial ownership arrangements, reluctance to provide information, property or land transactions with unclear funding sources, settlement proposals that do not appear commercially rational, and patterns of activity inconsistent with the known purpose of a transaction. These indicators do not prove wrongdoing, but they may warrant further review or reporting.

4.4 Council Approach and Key Controls

The Council will take a proportionate and risk-based approach to anti-money laundering, recognising that higher-risk situations may arise in areas such as property transactions, land disposals and acquisitions, grants and external funding, debtor and creditor arrangements, insurance settlements, procurement, licensing, enforcement activity, and transactions involving third parties, agents or complex ownership structures. The Council will apply appropriate internal controls, escalation arrangements and professional advice where necessary.

- Avoid accepting large cash payments except where expressly permitted by Council arrangements and supported by appropriate controls.
- Ensure transactions are properly authorised, recorded and supported by a clear business rationale.
- Undertake appropriate checks on counterparties, ownership information and payment arrangements where the risk justifies it.
- Be alert to requests for refunds to different accounts, payments routed through third parties, or arrangements that lack transparency.
- Retain relevant records of due diligence, decisions, approvals and referrals.
- Seek advice promptly where a transaction or arrangement appears unusual, high risk or inconsistent with normal expectations.

4.5 Reporting Procedure

Where an employee or member knows, suspects or has reasonable grounds to suspect that a transaction, arrangement or person may be involved in money laundering or terrorist financing, they must report the matter as soon as possible through the Council's internal reporting arrangements to the Chief Finance Officer. They should record the

concern factually, preserve relevant information and avoid taking any further step that could prejudice a review or investigation.

- Do not confront the individual concerned or attempt to investigate the matter personally unless this forms part of your authorised role.
- Do not disclose to any other person that a suspicion has been raised if doing so could amount to tipping off.
- Continue to follow any immediate lawful instructions given by the Chief Finance Officer or authorised senior officer.
- Where necessary, the Council will consider whether an external disclosure or Suspicious Activity Report should be made through the appropriate route.

4.6 Money Laundering Reporting Officer

The Council hs designated the Chief Finance officer as the Money Laundering Reporting Officer to receive internal reports, consider whether there is a need for further review or advice, determine whether an external disclosure is required and maintain appropriate confidential records. The MLRO should work closely with the Monitoring Officer, Legal Services, Internal Audit and other relevant officers where appropriate.

- Receive and assess internal disclosures of suspected money laundering.
- Maintain secure records of referrals, decisions and actions taken.
- Consider whether the matter should be referred externally through the appropriate reporting route.
- Provide or coordinate advice to services on the handling of suspicious matters.
- Support periodic review of the Council's anti-money laundering arrangements.

4.7 Training, Awareness and Review

Appropriate awareness of money laundering risk should be maintained across the Council, with more targeted guidance or briefing for services and roles more likely to encounter higher-risk transactions or arrangements. This policy should be reviewed periodically and updated to reflect legislative change, organisational learning, changes in service delivery and emerging risks. Any supporting guidance, forms or internal reporting templates should also be kept up to date.