Borough Council of
King's Lynn &
West Norfolk

ANTI-FRAUD & ANTI-CORRUPTION STRATEGY 2025-2028

March 2025

1. INTRODUCTION

1.1 Where people commit fraud against the public sector and public services, they take money away from the services on which the public depend on, and damage citizens' trust in the government. The Borough Council of King's Lynn and West Norfolk (the Council) is committed to protecting the public funds entrusted to it and to upholding the highest standards of financial probity and accountability. We cannot afford to be complacent, and we urge all our members, employees, contractors, and partners to assist us in tackling fraud by having regard to this policy and the risks of fraud when carrying out their duties, recognising that, if uncontrolled, fraud diverts much needed resources from our communities.

1.2 The "Annual Fraud Indicator 2023" produced by Crowe Clark Whitehall estimated that annual UK fraud losses could be £219 billion, with Public Sector fraud losses estimated to be £50.2 billion. The Government's "Economic Crime Plan 2023-2026" states that Fraud accounted for an estimated 41% of all crime experienced by adults in England and Wales in the year ending September 2022. Fraud is now the most common offence in the UK and local authorities continue to face significant fraud challenge, exacerbated by the Covid-19 pandemic and the ongoing cost-of-living crisis. Economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. This poses a threat to the UK's economy and its institutions and causes serious harm to society and individuals. It includes activity which:

- Allows criminals to benefit from the proceeds of their crimes or fund further criminality,
- Damages our financial systems and harms the interests of legitimate business,
- Undermines the integrity of the UK's position as an international finance centre, and
- Poses a risk to the UK's prosperity, national security, and reputation.

1.3 This strategy recognises that the terms "fraud" and "corruption" form part of a much wider agenda, but the strategy has not been re-titled "economic crime"; however, acknowledging this enables us to have an awareness and provide a holistic response to the following types of criminality:

- Fraud against the individual, private sector, and public sector,
- Terrorist financing,
- Sanctions contravention,
- Market abuse,
- Corruption and bribery,
- The laundering of proceeds of all crimes.

1.4 This strategy along with the policies in place detail the Council's arrangements for managing the risk of fraud and corruption. We are committed to reducing losses from fraud by using an integrated approach which encompasses the Fighting Fraud and Corruption Locally (FFCL) 2020's standards of:

- Governance (accountability, leadership, awareness, strategy, resources, authority, and independence),
- Operations (capability & competency, risk assessment, intelligence & data, collaboration, prevention, investigation, and redress), and
- Reporting (measurement, transparency, and monitoring).

1.5 The threat and risks of fraud and corruption are ever evolving and can quickly develop into new and complex fraud attacks and as such our response to countering fraud needs to be dynamic as developments in technology, social change and other factors create new challenges.

2. OVERVIEW

2.1 This strategy outlines the approach to combat fraud, corruption, and money laundering within the Council. The aim is to create efficient, self-sustainable, and cost-effective systems and processes which enhance organisational value and serves as a deterrent to fraudulent activities. This strategy includes the current legislative and regulatory framework that the Council should consider within it:

- **Core Fraud and Corruption Legislation**

  a) Fraud Act 2006 – Establishes offences of fraud by false representation, failure to disclose, and abuse of position.

  b) The Bribery Act 2010 – Covers bribing, being bribed, bribery of foreign public officials, and failure to prevent bribery.

  c) Theft Acts 1968 and 1978 – Cover theft, false accounting, and dishonesty offences.

  d) Proceeds of Crime Act 2002 (POCA) – Allows recovery of criminal proceeds and introduces offences of money laundering.

- **Local Authority-Specific and Sector-Specific Legislation**

  a) Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013 – Provides councils with powers to investigate and prosecute fraud related to council tax reduction schemes.

  b) Prevention of Social Housing Fraud Act 2013 – Criminalises tenancy fraud and gives local authorities powers to investigate and recover social housing.

  c) Local Government Act 1972 (Section 151) – Requires councils to ensure proper financial administration and protect public funds.

  d) Local Government Act 2000 – Establishes ethical frameworks, codes of conduct for members, and promotes governance standards.

- <u>**Criminal Procedure and Investigation Framework**</u>

  a) **Police and Criminal Evidence Act 1984 (PACE)** – Sets out powers and safeguards for the collection of evidence in criminal investigations, ensuring legality and proportionality.

  b) **Criminal Procedure and Investigations Act 1996 (CPIA)** – Governs disclosure obligations and requires councils to manage investigation material systematically.

- <u>**Surveillance and Investigation Powers**</u>

  a) **Regulation of Investigatory Powers Act 2000 (RIPA)** – Regulates covert surveillance and the use of covert human intelligence sources (CHIS) by councils.

  b) **Investigatory Powers Act 2016** – Extends surveillance powers and data retention obligations for law enforcement and certain public bodies.

- <u>**Economic Crime and Corporate Governance**</u>

  a) **Economic Crime and Corporate Transparency Act 2023** – Introduces new powers for tackling economic crime, enhanced corporate transparency obligations, and strengthens authorities' ability to act against financial crime.

  b) **Criminal Finances Act 2017** – Introduces corporate offences for failing to prevent the facilitation of tax evasion.

- <u>**Data, Privacy, and Transparency**</u>

  a) **Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)** – Sets standards for processing and storing personal data, relevant to investigation and fraud detection activities.

  b) **Freedom of Information Act 2000** – Requires councils to disclose information unless exempt, balancing transparency with confidentiality needs during investigations.

  c) **Local Government Transparency Code 2015** – Mandates the publication of information on counter-fraud work and enforcement action.

- <u>**Human Rights and Ethical Standards**</u>

  a) **Human Rights Act 1998 and European Convention on Human Rights (ECHR)** – Ensures fraud and corruption investigations are lawful, proportionate, and respect individuals' rights under the ECHR.

  b) **Equality Act 2010** – Ensures equality and non-discrimination principles in all actions, including investigation and enforcement.

- **Governance and Best Practice Standards**

  a) **Accounts and Audit Regulations 2015** – Requires councils to maintain effective internal controls, risk management, and arrangements for preventing and detecting fraud.

  b) **CIPFA Code of Practice on Managing the Risk of Fraud and Corruption (2014)** – Industry-standard guidance on managing fraud risk within public sector bodies.

  c) **CIPFA/SOLACE Delivering Good Governance Framework (2016)** – Establishes best practice for good governance, including counter-fraud principles.

  d) **Government Counter Fraud Functional Standard (GovS 013)** – Sets out required standards for public sector organisations in countering fraud.

  e) **National Fraud Initiative (NFI) and Norfolk FraudHub** – Data-matching exercises run by the Cabinet Office to identify fraud and error in public sector spending.

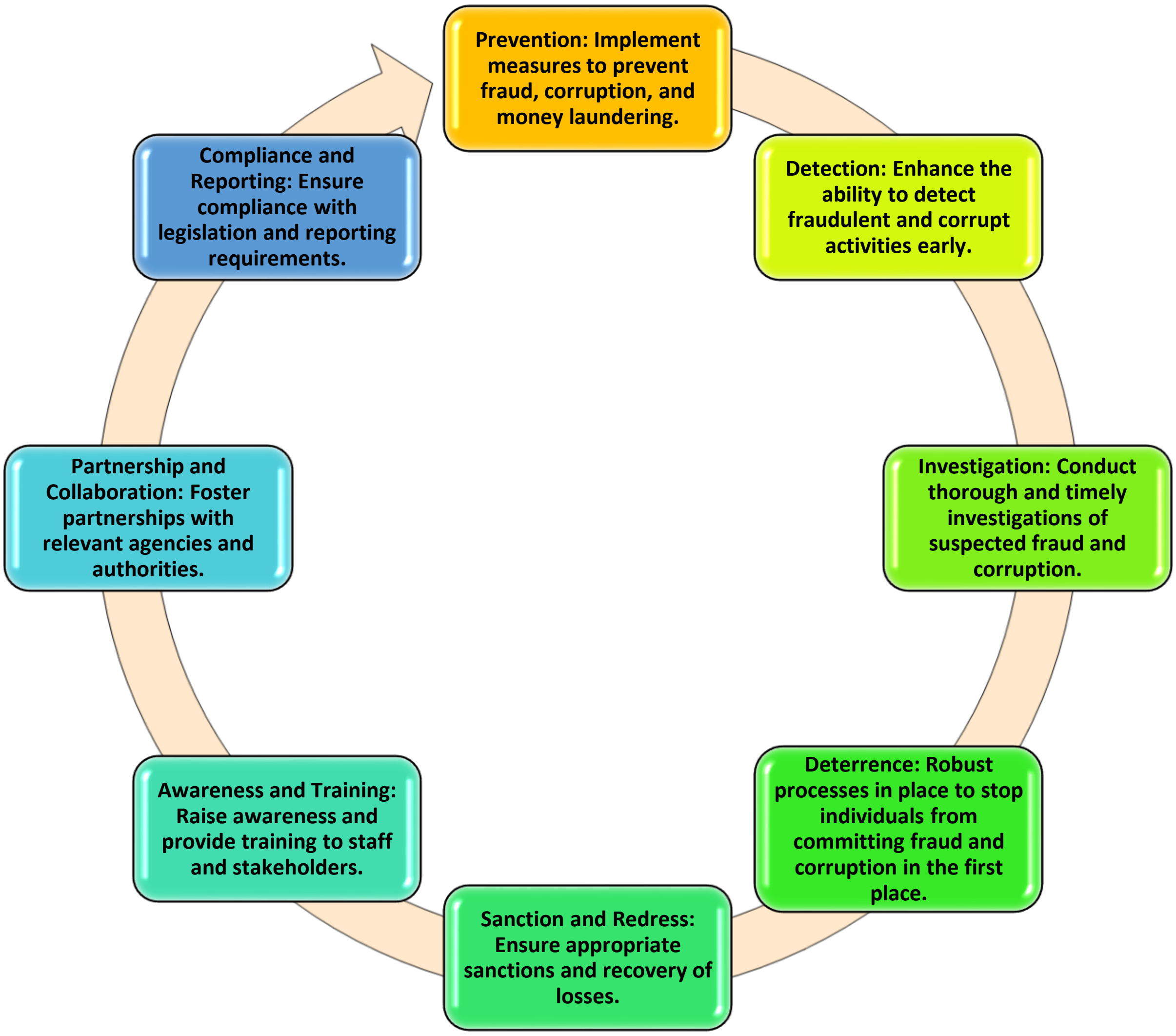
  f) **Fighting Fraud and Corruption Locally 2020s** – The counter fraud and corruption strategy for local government. It provides a blueprint for a coordinated response to fraud and corruption perpetrated against local authorities.

2.2 The Council is committed to embedding its anti-fraud and anti-corruption policies and procedures within all areas of governance, service delivery, financial management, and procurement processes, as such this strategy takes into account the following:

- ✓ Anti-Fraud & Anti-Corruption Policy
- ✓ Whistleblowing Policy
- ✓ Anti-Money Laundering Policy
- ✓ Financial Regulations

A further policy is being developed alongside this strategy “Anti-Bribery Policy”.

3. STRATEGIC AIMS



4. FRAUD RISK ASSESSMENT (CONCLUDED NOVEMBER 2024)

Service Area	Fraud Awareness	Asset Misappropria-tion	Financial Reporting	Non-Financial Reporting	Regulatory Compliance	Illegal Acts	Bribery & Corruption	Fraud Prevention Procedures	Pre-employment Screening	Other Controls	Money Laundering & POCA
Planning / CIL	Adequate	Adequate	N/A	Excellent	Strong	Adequate	Basic	Basic	N/A	Excellent	Adequate
Environmental Quality	Adequate	Adequate	N/A	Strong	Strong	Adequate	Adequate	Strong	N/A	Excellent	Adequate
Environment & Planning Support	Adequate	Adequate	N/A	Strong	Strong	Adequate	Basic	Basic	N/A	Excellent	Adequate
Planning Policy	Adequate	Basic	N/A	Strong	Strong	Adequate	Basic	Adequate	N/A	Adequate	N/A
Democratic Services	Adequate	Strong	N/A	Adequate	Strong	Adequate	Adequate	Poor	N/A	Adequate	N/A
CIC	Strong	Strong	N/A	Strong	Strong	Adequate	Basic	Adequate	N/A	Strong	Adequate
Personnel Services	Adequate	Adequate	N/A	Strong	Strong	Adequate	Adequate	Strong	Strong	Excellent	Adequate
Corporate Policy	Adequate	Adequate	N/A	Adequate	Adequate	N/A	Poor	Basic	N/A	Adequate	N/A
Communications	Adequate	Adequate	N/A	Adequate	Adequate	Adequate	Adequate	Adequate	N/A	Adequate	N/A
Legal Services	Strong	Strong	N/A	Adequate	Strong	Adequate	Adequate	Adequate	N/A	Basic	Basic
Licensing	Adequate	Strong	N/A	Adequate	Adequate	Adequate	Adequate	Adequate	N/A	Strong	N/A
Corporate Governance	Adequate	Adequate	N/A	Strong	Strong	Adequate	Adequate	Basic	N/A	Adequate	N/A
Climate Change	Strong	Adequate	N/A	Strong	Strong	Adequate	Strong	Adequate	N/A	Adequate	N/A
Corporate Projects	Strong	Strong	N/A	Strong	Basic	Adequate	Basic	Strong	N/A	Strong	N/A
Procurement	Strong	Strong	N/A	Adequate	Adequate	Adequate	Adequate	Strong	N/A	Basic	Adequate
Housing Needs & Allocations	Strong	Strong	N/A	Strong	Adequate	Adequate	Adequate	Strong	N/A	Strong	Adequate
Strategic Housing	Adequate	Adequate	N/A	Strong	Strong	Adequate	Adequate	Adequate	N/A	Strong	Adequate
Food and Health & Safety	Strong	Strong	N/A	Adequate	Basic	Strong	Adequate	Adequate	N/A	Strong	N/A
Careline Community Service	Adequate	Strong	N/A	Adequate	Adequate	Adequate	Strong	Adequate	N/A	Strong	Strong
Repairs and Adaptations (including Handyperson Service)	Adequate	Strong	N/A	Strong	Adequate	Basic	Basic	Adequate	N/A	Adequate	Adequate
Housing Standards	Adequate	Strong	N/A	Strong	Strong	Basic	Basic	Adequate	N/A	Strong	Adequate
CSNN / Enviro Crime / ASB / Help Hub	Adequate	Strong	N/A	Adequate	Adequate	Basic	Adequate	Adequate	N/A	Strong	Adequate
Public Open Space	Adequate	Adequate	N/A	Poor	Adequate	Basic	Adequate	Adequate	N/A	Adequate	N/A
Waste Management	Adequate	Adequate	N/A	Adequate	Adequate	Basic	Basic	Basic	N/A	Adequate	Adequate
Crematorium & Cemeteries	Poor	Adequate	N/A	Strong	Strong	Basic	Adequate	Adequate	N/A	Strong	N/A
CCTV	Strong	Adequate	N/A	Adequate	Strong	Adequate	Basic	Adequate	N/A	Adequate	N/A
Resort Services & Parking Operations (inc. Civil Enforcement)	Strong	Adequate	N/A	Strong	Strong	Adequate	Adequate	Adequate	N/A	Strong	N/A
Property and Projects	Excellent	Adequate	N/A	Adequate	Excellent	Strong	Adequate	Adequate	N/A	Adequate	Strong
Finance	Excellent	Adequate	Strong	Basic	Adequate	Adequate	Adequate	Adequate	N/A	Strong	Adequate
ICT	Strong	Adequate	N/A	Basic	Basic	Poor	Poor	Poor	N/A	Adequate	N/A
Revenues	Excellent	Strong	N/A	Strong	Excellent	Strong	Strong	Adequate	N/A	Excellent	Adequate
Benefits	Excellent	Adequate	N/A	Strong	Excellent	Strong	Strong	Adequate	N/A	Excellent	Adequate
Internal Audit & Fraud	Strong	Adequate	N/A	Strong	Strong	Strong	Strong	Strong	N/A	Excellent	Adequate
Alive West Norfolk	Adequate	Adequate	N/A	Excellent	Strong	Basic	Strong	Basic	N/A	Excellent	Strong

4.1 During 2024, a corporate wide fraud risk assessment was undertaken of which the results are shown above. Fraud risk and compliance elements have been assessed based upon the responses returned from all services and functions (34 responses were returned out of 36 across the council – 94.44%).

4.2 The Bribery Act 2010 and the Economic Crime and Corporate Transparency Act 2023 introduced specific standards and requirements in respect of anti-bribery measures and “reasonable fraud prevention procedures”. The standards require “adequate” (in terms of anti-bribery) and “reasonable” (in terms of fraud prevention procedures) controls to be in place. For the purposes of the assessment undertaken these terms are one and the same.

4.3 Therefore, the overall assessment of the organisation is that there are many adequate/reasonable controls in place; however, there are some suggested best practices to consider. Specifically, these are as follows:

- Staff are encouraged to undertake the available e-learning fraud awareness training at regular intervals.
- Service areas are encouraged to effectively communicate fraud risks to raise awareness.
- Where assets are held within service areas, it is encouraged to introduce inventory tracking and periodic inventory checks.
- Where non-financial reporting is in place, ensure a consistent validation process to improve reliability and outputs are produced by trained staff to ensure accurate reporting.
- Raising awareness of illegal acts specific to service areas through policies, procedures with line managers promoting ethical culture aligned to the “*Seven Principles of Public Life*” and internal Codes of Conduct.
- Regular risk assessments within service areas for illegal activities, with mitigation strategies in place.
- Raising awareness of the whistleblowing reporting mechanisms across the council.
- The introduction of an Anti-Bribery Policy (a draft has now been produced).
- Introduce “Declaration of Interests” and “land ownership” declarations.
- The introduction of anti-bribery e-learning training across the organisation.
- Monitoring and compliance checks in respect of gifts, gratuities and hospitality.
- Maintaining separation of duties, financial oversight, and refreshing fraud awareness and whistleblowing training for staff.
- Conducting corporate wide fraud risk assessments on a frequent basis.
- Leadership actively promoting fraud awareness and ensuring the policies and procedures are maintained and integrated into the corporate governance framework.
- Networking and professional membership subscriptions to maintain working knowledge of relevant changes in legislation, regulations and emerging risks.

4.4 The Fraud Risk Assessment has furthermore highlighted services and functions where there is a need to consider Anti-Money Laundering preventative procedures and processes. A total of 19 of the 34 areas that responded were involved in activities that could be susceptible to money laundering activities. The key areas where the council could be affected by money laundering activities are:

- Paying out any recoverable loans or grants,
- Receiving cash payments of £1,000 or more,
- Having the potential to pay out refunds of £1,000 or more.

The areas highlighted within the Fraud Risk Assessment should therefore receive Anti-Money Laundering training and regular refresher training, alongside this effective procedures should be maintained when dealing with such transactions across the organisation. The Council has an Anti-Money Laundering Policy and Procedures in place and relevant staff should familiarise themselves with these. Additional controls can be introduced to reduce risks around refund processes (a recent procedure has been produced for the Revenues Department that can be considered good practice).

4.5 In addition to these controls, maintaining the annual subscription to the National Anti-Fraud-Network provides valuable resource across the organisation to various intelligence checks. New checks are being made available as enhancements in digital and technology occur, such as the new bank account verification service available to check both consumers and suppliers bank details and verify that they relate to the consumer/supplier being presented.

Failing to Prevent Fraud: Avoiding Corporate Criminal Liability

4.6 The Economic Crime and Corporate Transparency Act 2023 (the Act) received Royal Assent on 26 October 2023. While the Act is now law, not all changes will take effect immediately and are to be rolled out gradually under a government implementation timetable. The offence will come into effect on 1 September 2025. Central government guidance was published in November 2024, which can be found on the following webpage - https://www.gov.uk/government/news/new-failure-to-prevent-fraud-guidance-published, that outlined the following reasonable fraud prevention procedures need to be in place:

i. Top level commitment
ii. Risk Assessment
iii. Proportionate risk-based fraud prevention procedures
iv. Due Diligence
v. Communication
vi. Monitoring and Review

i. Top level commitment

Responsibility for the prevention and detection of fraud rests with those charged with the governance of the organisation. The board of directors, partners and senior management of a relevant body should be committed to preventing associated persons from committing fraud. They should foster a culture within the organisation in which fraud is never acceptable and should reject profit based on, or assisted by, fraud.

Senior management have a leadership role in relation to fraud prevention. The level and nature of their involvement will vary depending on the size and structure of the relevant body, but their role is likely to include:

- Communication and endorsement of the organisation’s stance on preventing fraud, including mission statements.
- Ensuring that there is clear governance across the organisation in respect of the fraud prevention framework.
- Commitment to training and resourcing.
- Leading by example and fostering an open culture, where staff feel empowered to speak up if they encounter fraudulent practices.

ii. Risk Assessment

The organisation assesses the nature and extent of its exposure to the risk of employees, agents and other associated persons committing fraud in scope of the offence. The risk assessment is dynamic, documented and kept under regular review.

Relevant organisations may already undertake a range of risk assessments relating to fraud and other economic crime. In this case, organisations may find it most effective to extend their existing risk assessments to include the risk of frauds in scope of this offence.

Since the definition of an associated person is wide, organisations may wish to start by identifying typologies of associated persons. For example: agents, contractors providing a particular service for or on behalf of the organisation, or staff in specific sensitive roles.

iii. Proportionate risk-based fraud prevention procedures

An organisation’s procedures to prevent fraud by persons associated with it are proportionate to the fraud risks it faces and to the nature, scale and complexity of the organisation’s activities. They are also clear, practical, accessible, effectively implemented and enforced.

The relevant body should draw up a fraud prevention plan, with procedures to prevent fraud being proportionate to the risk identified in the risk assessment.

It is a key principle that the fraud prevention plan should be proportionate to the risk and the potential impact. The level of prevention procedures considered to be reasonable should take account of the level of control and supervision the organisation is able to exercise over a particular person acting on its behalf and the relevant body's proximity to that person. For example, a relevant body is likely to have greater control over the conduct of an employee than that of an outsourced worker performing services on its behalf. Nonetheless, appropriate controls should be implemented via the relevant contract.

In some limited circumstances, it may be deemed reasonable not to introduce measures in response to a particular risk. Any decision made not to implement procedures to prevent a specific risk should be documented, together with the name and position of the person who authorised that decision and reviewed as appropriate.

Since the offence extends across organisations in all sectors of the economy, many of these businesses will also be subject to other regulations, for example, regulations concerning financial reporting, environmental, health and safety or competition matters. Processes for compliance with these regulations may address certain potential frauds (for example, robust processes for compliance with specific environmental regulations might reasonably be expected to prevent fraud by misrepresentation on the relevant environmental statements).

It is not necessary or desirable for organisations to duplicate existing work. Equally, it would not be a suitable defence to state that because the organisation is regulated its compliance processes under existing regulations would automatically qualify as "reasonable procedures" under the Economic Crime and Corporate Transparency Act.

To avoid duplication of work, organisations are advised to assess whether their existing regulatory compliance mechanisms, financial reporting controls and fraud prevention measures would be sufficient to prevent each of the fraud risks identified in the risk assessment. Where existing mechanisms appear to be insufficient, organisations should develop appropriate measures to prevent fraud.

iv. Due Diligence

The organisation 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, in order to mitigate identified fraud risks.

Relevant organisations in the sectors facing the greatest fraud risks may already undertake a wide variety of due diligence procedures, both mandatory and in response to risks associated with specific transactions or customers.

However, it should be noted that merely applying existing procedures tailored to a different type of risk will not necessarily be an adequate response to tackle the risk of fraud. Those with exposure to the greatest risk may choose to clearly articulate their due diligence procedures specifically in relation to the corporate offence.

Relevant organisations should conduct due diligence on associated persons (including new partners). Examples of best practice include:

- ✓ Using appropriate technology, for example, third-party risk management tools, screening tools, internet searches, checking trading history or professional or regulated status if relevant, or vetting checks if appropriate.
- ✓ Reviewing contracts with those providing services, to include appropriate obligations requiring compliance and ability to terminate in the event of a breach where appropriate.
- ✓ Reviewing contracts for agents.
- ✓ Monitoring of well-being of staff and agents to identify persons who may be more likely to commit fraud because of stress, targets or workload.

Relevant organisations should conduct due diligence in relation to mergers or acquisitions. Examples of best practice include:

- ✓ Using third party merger and acquisition tools.
- ✓ Assessment of any relevant criminal or regulatory charges.
- ✓ Assessment of tax documentation.
- ✓ Assessment of the firm’s exposure to risk.
- ✓ Assessment of the firm’s fraud detection and prevention measures (bearing in mind that if the firm being acquired does not qualify as a “large organisation” as set out in section 201, it may not have any procedures that directly address the offence of failure to prevent fraud).
- ✓ Integration of fraud prevention measures post-acquisition.

Relevant organisations may choose to conduct their due diligence internally, or externally, for example by consultants. The due diligence procedures put in place should be proportionate to the identified risk and kept under review as necessary.

v. Communication

The organisation seeks to ensure that its prevention policies and procedures are communicated, embedded and understood throughout the organisation, through internal and external communication. Training and maintaining training are key.

A clear articulation and endorsement of an organisation's policy against fraud deters those providing services for or on behalf of the relevant body from engaging in such activities. Communication should be from all levels within an organisation. It is not enough for the senior management to say that staff should not commit fraud, if middle management then actively ignore this and encourage junior members to circumvent the relevant body's fraud prevention procedures.

It is important that the relevant body ensures awareness and understanding of its policies amongst those who provide services for or on its behalf. The organisation may feel that it is necessary to require its representatives to undertake fraud-specific training, depending on the risks it is exposed to. This would be to ensure that they have the skills needed to identify when they and those around them might be at risk of engaging in an illegal act and what whistle-blowing procedures should be followed if this occurs.

It may be helpful to integrate fraud messaging into existing policies and procedures. For instance, policies related to sales targets or customer interactions could include a brief statement addressing fraud rationalisation and the potential consequences of committing fraud.

Organisations may also choose to publicise within the organisation the outcome of investigations, particularly the sanctions imposed.

vi. Monitoring and Review

The organisation monitors and reviews its fraud detection and prevention procedures and makes improvements where necessary. This includes learning from investigations and whistleblowing incidents and reviewing information from its own sector.

Full details of the government guidance can be found at:
https://assets.publishing.service.gov.uk/media/67868e29c6428e013188179c/Failure+to+Prevent+Fraud+Guidance+-+English+Language+v1.6.pdf

5. IMPLEMENTATION PLAN

5.1 Below is an outline of controls and oversight / governance arrangements that are in place or those that can be introduced to assist in the prevention, detection and deterrence of fraud, corruption and money laundering across the Council:

Prevention

Target Areas	Measures	Processes
Procurement & Contract Management	✓ Robust Policies: Maintain and enforce comprehensive procurement policies. ✓ Supplier Due Diligence: Conduct thorough vetting of suppliers to ensure legitimacy. ✓ Contract Management: Implement protocols for contract management with clear performance metrics and penalties for non-compliance.	✓ Regularly review procurement policies to ensure they are up-to-date. ✓ Perform due diligence checks on new suppliers before contracts are awarded. ✓ Monitor supplier performance through regular reviews and audits.
Payroll & Human Resources	✓ Audit Payroll Records: Conduct periodic audits to identify discrepancies. ✓ Controls Over Payroll: Maintain controls to ensure segregation of duties and authorisation protocols. ✓ Recruitment Procedures: Ensure hiring processes prevent false employee records	✓ Schedule regular payroll audits. ✓ Ensure payroll changes are authorised by multiple parties. ✓ Verify employee credentials during the hiring process.
Grant and Benefit Administration	✓ Verification Processes: Introduce stringent processes for verifying eligibility. ✓ Review and Audit: Regularly audit grant and benefit disbursements. ✓ Approval Guidelines: Establish clear guidelines for grant approvals	✓ Implement automated verification systems for grant and benefit applications. ✓ Schedule periodic audits of disbursement records. ✓ Train staff on approval processes and guidelines.
Financial Transactions and Accounting	✓ Internal Controls: Ensure strong controls over transactions and accounting records. ✓ Regular Reconciliations: Perform regular reconciliations and independent reviews. ✓ Secure Systems: Maintain secure electronic payment systems.	✓ Conduct monthly reconciliations of financial accounts. ✓ Perform independent reviews of financial statements periodically. ✓ Regularly update security protocols for payment systems.

Information Technology	✓ Cybersecurity: Maintain strong cybersecurity measures to protect data. ✓ Access Controls: Ensure strict access controls and audit IT systems regularly. ✓ Staff Training: Conduct regular training on cyber fraud prevention.	✓ Update and test cybersecurity measures periodically. ✓ Audit access logs and user activities regularly. ✓ Provide annual cybersecurity training for all staff.

Detection

Target Areas	Measures	Processes
Procurement & Contract Management	✓ Data Analytics: Use data analytics to monitor for anomalies. ✓ Compliance Audits: Conduct regular compliance audits. ✓ Supplier Performance Monitoring: Regularly review supplier performance.	✓ Implement analytics tools to detect irregular patterns. ✓ Schedule compliance audits periodically. ✓ Review supplier performance reports frequently.
Payroll & Human Resources	✓ Irregularity Detection: Use data analytics to identify payroll irregularities. ✓ Periodic Checks: Conduct periodic checks for ghost employees. ✓ Timesheet Monitoring: Monitor timesheets for discrepancies.	✓ Implement payroll analytics software. ✓ Conduct surprise checks on payroll records. ✓ Review timesheets frequently.
Grant and Benefit Administration	✓ Automated Flagging: Use systems to flag unusual claims. ✓ Programme Audits: Regularly audit grant and benefit programmes. ✓ Data Matching: Use data matching to verify claimant information.	✓ Implement automated fraud detection systems. ✓ Schedule audits of grant programmes periodically. ✓ Use data matching tools to cross-check claimant information.
Financial Transactions and Accounting	✓ Continuous Monitoring: Monitor transactions continuously using analytics. ✓ Surprise Audits: Conduct surprise audits of financial records. ✓ Unusual Transaction Monitoring: Monitor for unusual banking transactions.	✓ Set up real-time transaction monitoring systems. ✓ Conduct surprise financial audits periodically. ✓ Review banking transactions frequently.
Information Technology	✓ Intrusion Detection: Employ intrusion detection systems. ✓ Security Audits: Conduct regular IT security audits. ✓ User Activity Monitoring: Monitor user activity for unusual behaviour.	✓ Implement and regularly update intrusion detection systems. ✓ Schedule IT security audits periodically. ✓ Monitor and review user activity logs frequently.

Deterrence

Target Areas	Measures	Processes
Procurement & Contract Management	✓ Publicise Successes: Publicise successful fraud prevention cases. ✓ Strict Penalties: Enforce strict penalties for procurement fraud. ✓ Transparency: Promote transparency in procurement processes.	✓ Issue regular reports on successful fraud prevention cases. ✓ Apply penalties consistently and visibly. ✓ Ensure procurement processes are open and transparent.
Payroll & Human Resources	✓ Zero-Tolerance Policy: Communicate zero-tolerance policies for fraud. ✓ Training: Provide regular training on ethical behaviour. ✓ Disciplinary Actions: Enforce disciplinary actions for fraud.	✓ Issue regular reminders about zero-tolerance policies. ✓ Conduct periodical ethics training sessions. ✓ Apply disciplinary actions consistently and fairly.
Grant and Benefit Administration	✓ Public Awareness: Run public awareness campaigns on fraud consequences. ✓ Strict Penalties: Enforce penalties for fraudulent claims. ✓ Transparency: Promote transparency in grant and benefit administration.	✓ Launch periodical public awareness campaigns. ✓ Consistently apply penalties for fraudulent claims. ✓ Ensure transparency in the administration process.
Financial Transactions and Accounting	✓ Visible Controls: Implement visible internal controls. ✓ Communication: Communicate the consequences of financial fraud. ✓ Code of Conduct: Regularly update and enforce the code of conduct.	✓ Conduct regular reviews of internal controls. ✓ Issue regular communications on fraud consequences. ✓ Update and distribute the financial regulations and code of conduct annually.
Information Technology	✓ Publicise Measures: Publicise cybersecurity measures. ✓ Strict Penalties: Enforce strict penalties for IT security breaches. ✓ Cyber Vigilance: Promote a culture of cyber vigilance.	✓ Regularly communicate about cybersecurity measures. ✓ Consistently apply penalties for IT breaches. ✓ Conduct regular cybersecurity awareness campaigns.

6. ANTI-FRAUD AND ANTI-CORRUPTION CULTURE AND AWARENESS

6.1 Building a Strong Culture:

1. Leadership Commitment: Senior management must lead by example, demonstrating zero tolerance for fraud and corruption.
2. Ethical Standards: Promote and enforce high ethical standards and integrity throughout the council.
3. Open Communication: Foster an environment where employees feel safe to report suspicious activities without fear of retaliation.

6.2 Awareness Initiatives:

1. Regular Training: Conduct regular training sessions for all staff on recognising and preventing fraud and corruption.
2. Communication Campaigns: Use internal newsletters, emails, and intranet updates to keep staff informed about anti-fraud measures.
3. Workshops and Seminars: Organise workshops and seminars to discuss real-life cases and best practices.

7. COMMUNICATION STRATEGY FOR STAKEHOLDERS

Internal Stakeholders	Communication Strategy
Staff	✓ Regular Updates: Provide regular updates on anti-fraud policies and procedures through emails and intranet. ✓ Training Programs: Implement mandatory training programs on fraud awareness and prevention. ✓ Feedback Mechanism: Establish a feedback mechanism for staff to voice concerns or suggestions regarding anti-fraud measures.
Senior Management & Members	✓ Reports and Briefings: Deliver regular reports and briefings on the status of anti-fraud measures and incidents. ✓ Strategic Involvement: Involve senior management in strategic decisions related to fraud prevention and response.

External Stakeholders	Communication Strategy
Partners and Contractors	✓ Clear Communication: Communicate anti-fraud policies and expectations to all partners and contractors. ✓ Due Diligence: Conduct thorough due diligence on all partners and contractors to ensure compliance with anti-fraud policies. ✓ Contractual Obligations: Include anti-fraud clauses in contracts with partners and contractors, outlining expectations and consequences of non-compliance.
Suppliers	✓ Regular Communications: Provide suppliers with information on the authority's anti-fraud measures and expectations. ✓ Training and Workshops: Offer training sessions and workshops to suppliers on detecting and preventing fraud. ✓ Audits and Reviews: Conduct regular audits and reviews of supplier performance and adherence to anti-fraud policies.
Public and Beneficiaries	✓ Public Awareness Campaigns: Run campaigns to educate the public about the consequences of fraud and the importance of reporting suspicious activities. ✓ Accessible Reporting Channels: Ensure there are accessible and confidential channels for the public to report fraud. ✓ Transparency: Maintain transparency about the authority's efforts to combat fraud, including publishing statistics and outcomes of anti-fraud activities.
Regulatory Bodies	✓ Regular Reporting: Ensure timely and accurate reporting to regulatory bodies as required by law. ✓ Collaboration and Information Sharing: Foster partnerships with external agencies and participate in information-sharing networks to enhance fraud detection and prevention efforts. ✓ Compliance Audits: Engage in regular compliance audits to ensure adherence to all relevant legislation and regulations.

8. CONCLUSION

8.1 Implementing this comprehensive strategy will create a robust framework for combating fraud, corruption, and money laundering within the Council that will ensure compliance with legislation and regulations. By targeting specific areas with tailored prevention, detection, and deterrence measures, the authority can significantly reduce risks, protect public funds, maintain public trust, and enhance organisational value. The involvement of technology and collaboration with external agencies will further ensure a focused and effective anti-fraud and anti-corruption strategy.

The strategy’s success depends on building a strong anti-fraud culture, raising awareness among all stakeholders, and maintaining clear and open communication channels. This holistic approach will not only safeguard the council’s assets but also reinforce its reputation for integrity and accountability.