

2025/26 Counter Fraud Plan

Date: 13 March 2025

ANNEX 1

CONTENTS

3	Background
3	National Counter Fraud Strategy
5	Fraud Risk Assessment
6	Development and Work Plans
6	Policy Framework Review
7	Appendix A: Fraud risk assessment
19	Appendix B: Counter Fraud Development Plan
21	Appendix C: Counter Fraud Work Plan



BACKGROUND

- 1 Fraud is a significant risk to the public sector. Fraud is the most common offence in the UK, accounting for 41% of all crime¹. The National Audit Office estimates that fraud and error cost the taxpayer between £55 and £81 billion in 2023/24 and that only a fraction of this is detected². Financial loss due to fraud can reduce a council's ability to support public services and can cause reputational damage.
- 2 When fraud is committed against the public sector, money is diverted from vital public services into the hands of criminals. Local authorities must ensure that they have the right policies and procedures in place to prevent it from happening. They should also promote a strong anti-fraud culture at all levels of the organisation as well as amongst the general public.
- 3 The methods employed by criminals are constantly evolving as they explore new ways to defraud local authorities. To respond effectively, councils need to monitor the fraud landscape to ensure that their counter fraud measures offer protection from these evolving threats.
- 4 This report sets out the council's approach to addressing fraud, reviews its counter fraud policy framework, updates the annual fraud risk assessment, details new and ongoing developmental activity, and sets out how counter fraud resources will be used in 2025/26.



NATIONAL COUNTER FRAUD STRATEGY

- 5 In 2014, CIPFA set out the responsibilities of Local Authority leaders to counter fraud and corruption within their organisations in their Code of practice on managing the risk of fraud and corruption³. The code says that organisations should:
 - acknowledge the responsibility of the governing body for countering fraud and corruption
 - identify the fraud and corruption risks
 - develop an appropriate counter fraud and corruption strategy
 - provide resources to implement the strategy
 - take action in response to fraud and corruption.
- 6 In 2020, Fighting Fraud and Corruption Locally (FFCL) published the most recent counter fraud and corruption strategy for local government⁴. Over the past five years City of York Council has followed the principles set out by CIPFA and FFCL to guide and develop its response to fraud.

¹ [Progress combatting fraud \(Forty-Third Report of Session 2022-23\)](#), Public Accounts Committee, House of Commons

² [An overview of the impact of fraud and error on public funds](#), National Audit Office

³ [Code of practice on managing the risk of fraud and corruption](#), CIPFA

⁴ [A strategy for the 2020s](#), Fighting Fraud and Corruption Locally

- 7 The FFCL strategy recommends that councils consider the effectiveness of their counter fraud framework by considering performance against the five key themes set out below.

- **Govern** – *Having robust arrangements and executive support to ensure anti-fraud, bribery and corruption measures are embedded throughout the organisation. Having a holistic approach to tackling fraud is part of good governance.*

The council has a strong anti-fraud policy framework that is reviewed annually and regular reminders are issued to employees. Counter fraud work is regularly reported to members and officers in the course of the year. The council has up to date whistleblowing policy supported by Veritau who log all reports and provide an external whistleblowing hotline. Training has been provided to managers across the organisation. Employees and managers will be encouraged to complete new e-learning packages which will be available in 2025/26.

- **Acknowledge** – *Acknowledging and understanding fraud risks and committing support and resource to tackling fraud in order to maintain a robust anti-fraud response.*

An annual risk assessment of fraud is published and presented to members. The risk assessment is informed by national fraud trends, fraud reported to and investigated by the counter fraud team as well as the views of senior council officers who have in depth knowledge of their service areas. Development activity is planned each year, based on the risk assessment, emerging trends, and evaluation of arrangements against good practice guidance.

- **Prevent** – *Preventing and detecting more fraud by making better use of information and technology, enhancing fraud controls and processes and developing a more effective anti-fraud culture.*

Prevention of fraud is considered as a matter of course in the work of both the counter fraud and internal audit teams. Where investigations identify changes to controls that could help prevent fraud these are discussed with senior council officers and checks are made to ensure any agreed action is implemented. The counter fraud team invests in training for its officers to ensure they remain up to date in the use of technology. Work with the Communications Team helps to develop an anti-fraud culture within the council and the residents it serves. In 2025 a new offence will come into law, Failure to Prevent Fraud, which makes large organisations corporately liable for fraud committed by its employees. The implications of the new law for the council need to be examined.

- **Pursue** – *Punishing fraudsters and recovering losses by prioritising the use of civil sanctions, developing capability and capacity to investigate fraudsters and developing a more collaborative and supportive local enforcement response.*

Strong action is taken to punish criminals and recover funds lost to fraud. All cases of fraud are investigated to criminal standards and the council

considers prosecution of suspected offenders where appropriate, or can apply a range of other potential sanctions. The council has a good relationship with North Yorkshire Police and will raise concerns with them when appropriate. The counter fraud team work with the Department for Work and Pensions (DWP) to address council tax support fraud. Conducting joint investigations into criminals defrauding both the council and the DWP is often more effective and efficient. All avenues are considered to recover loss, including civil recovery. As a result of counter fraud work the council has achieved £245k in counter fraud savings⁵ in 2024/25 (up to the mid-January).

- **Protect** – *Protecting against serious and organised crime, protecting individuals from becoming victims of crime and protecting against the harm that fraud can do to the community.*

Fraud affects communities across Yorkshire and residents are as likely to be targeted as the council is. The council's public protection team regularly alerts residents to emerging frauds and scams perpetrated against the public. The counter fraud team shares information about fraud affecting the public with council colleagues, for example national data matching may identify where residents are the victims of identity theft. Regular liaison with other councils in the region can identify fraud that is occurring cross boundary. The counter fraud team will explore data matching projects with surrounding councils in 2025/26.

FRAUD RISK ASSESSMENT

- 8 Fraud risks are assessed annually to identify priorities for counter fraud work. The 2025/26 fraud risk assessment, contained in appendix A, is informed by national and regional reports of fraud affecting local authorities as well as fraud reported directly to the counter fraud team (CFT). Inherent risk ratings show the risk to the council if no controls are in place to prevent fraud. The residual risk rating indicates the potential risk level after current controls are taken into account.

The results of the assessment are used to:

- develop or strengthen existing fraud prevention and detection measures
 - revise the counter fraud policy framework
 - focus future audit and counter fraud work.
- 9 By their nature, fraud risks are hard to quantify. For example, there are no established methodologies for determining estimated losses due to fraud in most areas. The terms high, medium, and low are therefore used in the risk assessment to provide a general indication of both the likelihood and impact of fraud in each area. However, we have intentionally avoided defining what high, medium, and low risk mean given the inherent uncertainty.

⁵ Counter fraud savings consist of money recovered during the course of the year (debts may have been calculated in previous years as well as the current financial year) and 12 months of savings where an ongoing fraud has been stopped through the work of the counter fraud team.

- 10 The risk assessment has been carried out by Veritau, based on our understanding of fraud risks in the sector and our knowledge of controls in place within the council to prevent, identify and deter fraud. It is used to inform priorities for counter fraud and internal audit work by Veritau. It is separate from the wider council risk management framework, however the views of senior officers within affected service areas are sought.
- 11 The updated risk assessment includes additional work planned by the internal audit and counter fraud teams, eg further audit testing of direct payments, training on detecting procurement fraud under new procurement legislation, and addressing emerging fraud risks like diverting parking payments with false QR codes.
- 12 The fraud risk assessment will be kept under review so that any significant new or emerging risks are addressed.



COUNTER FRAUD DEVELOPMENT AND WORK PLANS

- 13 The 2025/26 counter fraud development plan is included in appendix B. It sets out development activity for the council and the counter fraud team for the year. These priorities are informed by the fraud risk assessment, policy framework review, and seek to develop counter fraud work in each of the five themes set out in the FFCL national counter fraud strategy.
- 14 The counter fraud work plan is included in appendix C. The plan sets out the areas of counter fraud work to be undertaken in 2025/26. The time allocation for each area is not defined because it will depend on the levels of suspected fraud reported to the counter fraud team. Reactive investigations (determined by allegations of fraud received) will however account for the largest proportion of work. Priorities for work in the remaining areas will be determined in accordance with the counter fraud development plan and fraud risk assessment. A total of 983 days has been allocated to counter fraud work in new financial year.



POLICY FRAMEWORK REVIEW

- 15 The council's counter fraud policy framework is reviewed annually. The review considers a number of counter fraud related policies (including the anti-fraud, corruption, and bribery policy, the whistleblowing policy, and other associated policies).
- 16 The review found no urgent requirement to change or update policies at the present time. However, the council's whistleblowing policy requires refreshing as it was last updated in 2019. The need was identified in 2024/25 but it is likely that this work will be completed in 2025/26. In addition, a new policy may need to be created (or an existing policy expanded) to reflect the Economic Crime and Corporate Transparency Act 2023. This created a new Failure to Prevent Fraud offence which comes into effect in September 2025.

APPENDIX A: 2025/26 FRAUD RISK ASSESSMENT

Risk area #1	Social care fraud	Inherent risk	High	Residual risk	High
Risk description	For adult social care, losses can occur through deprivation or non-declaration of capital which can involve the transfer or disguise of property in order to avoid paying for residential or domestic care provision. Residential homes could also continue to claim for customers who are no longer in residence (eg after they pass away). In both adult and children’s social care, fraud can occur through the misuse of the Direct Payment scheme. For example, where monies allocated to meet a customer’s assessed needs are not used to procure support services. Losses in social care fraud cases can be substantial, especially if they are not detected at an early stage.				
Risk controls	Applications for care funding are carefully assessed to ensure that recipients meet the eligibility criteria and that any financial contribution for care by the customer is correctly calculated. A range of monitoring and verification controls are operated by the council. This includes requiring customers in receipt of Direct Payments to have a separate bank account for managing these funds and complying with monitoring procedures to verify spending. In instances of misused Direct Payments, customers are moved to a commissioned service. If concerns are raised about the wellbeing of customers, then the council has a multi-agency safeguarding process which can highlight fraud. The residual risk of adult and children’s social care fraud is still considered to be high. This is due to the level of spend in this area, the scale of losses, and the speed at which they can be accrued. It is also a reflection of the difficulty all councils have in detecting assets when people are determined to keep them hidden.				
Priorities for internal audit / counter fraud	Veritau has established relationships with senior management and officers responsible for the provision of social care; concerns of fraud are regularly reported to the counter fraud team (CFT) for investigation. Internal audit (IA) periodically conducts audits in higher risk areas. Investigation of fraud in this area provides a deterrent to those considering committing it and can assist the council to recover losses through the court system. Delivering more fraud awareness training for employees working in social care is a priority for 2025/26.				

Risk area #2	Creditor fraud	Inherent risk	High	Residual risk	High
Risk description	Over the course of a number of years attempts to commit fraud against the creditor payment systems of public and private sector organisations has increased in terms of volume and sophistication. The mandatory publication of payment data makes councils particularly vulnerable to attack. Attacks are often the work of organised criminal groups who operate from abroad. Individual losses due to fraud can be extremely large (in excess of £1 million). The likelihood of recovery is low once a fraud has been successfully committed. The most common issue is mandate fraud (payment diversion fraud) where fraudsters impersonate legitimate suppliers and attempt to divert payments by requesting changes in bank details. Other types of fraud include whaling, where senior members of the council are targeted and impersonated in order to obtain fraudulent payments. There have been increased instances nationally and regionally of hackers gaining direct access to the email accounts of suppliers and using them to attempt to commit mandate fraud. These attempts can be very difficult to detect and prevent.				
Risk controls	The council has strong controls in place to identify fraudulent attempts to divert payments from genuine suppliers and to validate any requests to change supplier details. Segregation of duties exist between the ordering, invoicing and payments processes. The residual risk of creditor fraud is still considered to be high due to potentially high levels of loss and the frequency of attacks. The council relies on its own employees, and those of its suppliers, to follow processes which prevent this type of fraud from occurring. However good processes can be undermined by human error which is a factor in many successful mandate fraud attacks.				
Priorities for internal audit / counter fraud	Veritau provide support and advice to finance officers responsible for the payment of suppliers. IA regularly perform audits of ordering and creditor payment processes, eg segregation of duties and controls to prevent mandate fraud. IA also undertake duplicate payment checks on a quarterly basis. Increased awareness provides a greater chance to stop fraudulent attempts before losses occur. All instances of attempted creditor related fraud are reported to the CFT who then report to relevant agencies, such as the National Cyber Security Centre. The CFT regularly shares intelligence alerts relating to attempted fraud occurring nationally with relevant council officers to help prevent losses. As part of any investigation of fraud in this				

area, the CFT will advise on improvements that can help strengthen controls. Training to officers involved in the management of payments to creditors has been arranged for the new financial year.

Risk area #3	Cybercrime	Inherent risk	High	Residual risk	High
Risk description	Cybercrime is an evolving area where criminals are continually refining their techniques in order to overcome controls, obtain unauthorised access and information, and frustrate systems. As cybercrime can be perpetrated remotely, attacks can come from within the UK or overseas. Some cybercrime is motivated by profit however some is designed purely to disrupt services. Types of cybercrime experienced by local authorities include ransomware, phishing, whaling, hacking, and denial of service attacks. Attacks can lead to loss of funds or systems access/data which could impact service delivery to residents. Security breaches and infractions can put the council’s accreditations at risk, eg Public Sector Network compliance, which could have a negative effect on the council’s relationships with third parties. There have been a number of high-profile cyber-attacks on public and private sector organisations in recent years. Attacks stemming from the hacking of software or ICT service providers have become more prevalent. These are known as supply chain attacks and are used by hackers to target the end users of the software created by the organisations targeted.				
Risk controls	The council employs highly skilled ICT employees whose expertise is used to help mitigate the threat of cybercrime. The ICT department has processes to review threat levels and controls (eg password requirements for employees) on a routine basis. It carries out weekly automated vulnerability scanning, as well as annual penetration testing performed by an accredited third-party organisation. The ICT department also uses filters to block communications from known fraudulent servers and will encourage employees to raise concerns about any communications they do receive that may be part of an attempt to circumvent cybersecurity controls. Despite strong controls being in place, cybercrime remains a high residual risk for the council. The potential for cybercrime is heightened by the availability of online tools. The UK government reported that 50% of businesses and 32% of charities had experienced some form of cyber security breach or attack in 2023/24. Council systems could be exposed by as yet unknown weaknesses in software.				

	Suppliers of software or IT services could also be compromised which may allow criminals access to council systems believed to be secure. The residual risk of cybercrime remains high due to the constantly evolving methods employed by fraudsters which requires regular review of controls.
Priorities for internal audit / counter fraud	Cybersecurity is an ongoing priority for IA work, the annual work programme consistently includes ICT audit work overseen and delivered by CISA (Certified Information System Auditor) accredited auditors. Raising awareness with employees can be crucial in helping to prevent successful cyberattacks. The CFT work with ICT to support activities that raise awareness amongst employees. A campaign to mark cybersecurity awareness month is undertaken annually.

Risk area #4	Council tax and business rate frauds	Inherent risk	High	Residual risk	Medium
Risk description	Council tax discount fraud can be a common occurrence. CIFAS conducted a survey in 2022 in which 10% of UK adults said they knew someone who had recently committed single person discount fraud. In addition, 8% of people thought falsely claiming a single person discount was a reasonable thing to do. Individual cases of fraud in this area are of relatively low value but cumulatively can represent a large loss to the council. Business rates fraud involves people falsely claiming discounts that a business is not entitled to, eg small business rate relief. Reports of business rate fraud are less common than council tax fraud but can lead to higher losses in individual cases.				
Risk controls	The council employs a number of methods to help ensure only valid applications are accepted. This includes requiring relevant information be provided on application forms and undertaking visits to properties where needed to verify information. The council routinely takes part in the National Fraud Initiative (NFI). The exercise allows councils to cross check for potential instances of fraud in multiple locations (eg multiple claims for single person discount by one individual). The council regularly undertakes additional data matching exercises designed to identify where multiple people are living in a property, but a single person discount is being claimed. The CFT provide a deterrent to fraud in this area through the investigation of potential offences which can, in serious cases, lead to prosecution.				

Priorities for internal audit / counter fraud	Council tax and business rates are considered to be one of the council's key financial systems and as such are routinely examined by IA – an audit is planned in 2025/26. A compliance scheme is currently being piloted which encourages residents who claim single person discount to report relevant changes to their circumstances. The results of the pilot will be reviewed in the new financial year.
--	--

Risk area #5	Council tax support fraud	Inherent risk	High	Residual risk	Medium
Risk description	Council Tax Support (CTS) is a council funded reduction in liability for council tax. It is resourced through council funds. Fraud and error in this area is of relatively low value on a case-by-case basis but cumulatively fraud in this area could amount to a substantial loss. CTS fraud can involve applicants failing to correctly declare their assets, income, or household composition. Those receiving support are also required to notify relevant authorities when they have a change in circumstances that may affect their entitlement to support. Most CTS claims are linked to state benefits (eg Universal Credit) which are administered by the Department for Work and Pensions (DWP).				
Risk controls	The council undertakes eligibility checks on those who apply for support. Officers manage the assessment of new and ongoing claims for CTS to identify potential issues. The DWP use data from HMRC on claimants' incomes which is then passed through to council systems which mitigates the risk of claimants not updating the council with income details. There are established lines of communication with the DWP where claims for support are linked to externally funded benefits. The council routinely takes part in the National Fraud Initiative (NFI) which highlights potentially fraudulent claims. The CFT provide a deterrent to fraud in this area through the investigation of potential offences which can, in serious cases, lead to prosecution. The CFT jointly works with the DWP to investigate fraud when it affects both organisations. This can help achieve better results for the council where state benefits are involved. If fraud cannot be addressed by the council directly it will be reported to the DWP.				
Priorities for internal audit	The CFT will continue to raise awareness of fraud with teams involved in processing claims for CTS as well as seeking opportunities to raise awareness with the public about the mechanisms for reporting fraud. Training				

/ counter fraud	for council officers working in customer services is scheduled for the new financial year. The results of a pilot compliance scheme in relation to CTS will also be reviewed.
-----------------	---

Risk area #6	Housing fraud	Inherent risk	High	Residual risk	Medium
Risk description	Council properties represent a significant asset to the council. Housing fraud can deprive the council of these assets through false applications for Right to Buy. Tenants who sublet or falsely obtain council properties remove a property from a person or family in true need of housing and can negatively affect the council financially when people are in temporary accommodation and are waiting for a suitable property to become available.				
Risk controls	The council has strong controls in place to prevent false applications for housing. The housing department engages with tenants regularly to ensure properties are not being misused. Eligibility checks are made before council owned properties are let. The CFT work with council colleagues to conduct checks, eg identity and money laundering, on all applications for Right to Buy. The CFT provide a deterrent to fraud in this area through the investigation of any suspected subletting of council properties using powers under the Prevention of Social Housing Fraud Act. Offenders face criminal prosecution and repossession of their council properties.				
Priorities for internal audit / counter fraud	The CFT will continue to raise awareness of fraud with teams involved in applications for council housing and the management of housing stock. The investigation of reports of the subletting of council properties are treated as a priority.				

Risk area #7	Procurement fraud	Inherent risk	High	Residual risk	Medium
Risk description	Procurement fraud, by its nature, is difficult to detect but can result in large scale loss of public funds over long periods of time. Businesses that collude to stifle competition and fix or inflate prices are referred to as a cartel. The Competition and Markets Authority (CMA) estimates that having a cartel within a supply chain can raise prices by 30% or more. Procurement fraud can also take the form of mischarging, undertaking substandard work, and diverting goods or services. In 2020 CIPFA reported losses of £1.5m for local authorities, due to procurement fraud. It found that 8% of fraud detected in this area involved 'insider fraud'.				
Risk controls	The council has established Contract Procedure Rules. The rules are reviewed regularly and require a competitive process for significant procurements through an e-tender system. A team of procurement professionals provide guidance and advice to ensure procurement processes are carried out correctly. The Contract Procedure Rules also set out the requirements for declarations of interests to be made. Contract monitoring helps to detect and deter potential fraud. The Procurement Act 2023 has recently come into force. The Act contains new processes which should help prevent and detect fraud in this area.				
Priorities for internal audit / counter fraud	Continued vigilance by relevant employees is key to identifying and tackling procurement fraud. IA and the CFT monitor and share guidance on fraud detection issued by the Competition and Markets Authority and other relevant bodies. IA reviewed the council's preparedness for the new procurement legislation and gave it substantial assurance. Further IA work is planned for 2025/26 to measure compliance with the new Act. The CFT will provide updated training for the procurement team as a result of the legislation.				

Risk area #8	Internal fraud	Inherent risk	Medium	Residual risk	Medium
Risk description	<p>Fraud committed by employees is a risk to all organisations. Internal fraud within councils occurs infrequently and usually results in low levels of loss. However, if fraud or corruption occurred at a senior level there is the potential for a greater level of financial loss and reputational damage to the council. There are a range of potential employee frauds including theft, corruption, falsifying timesheets and expense claims, abusing flexitime or annual leave systems, undertaking alternative work while sick, or working for a third party on council time. Some employees have access to equipment and material that may be misused for private purposes. Payroll related fraud can involve the setting up of 'ghost' employees in order to obtain salary payments.</p>				
Risk controls	<p>In the past two years the council has introduced new whistleblowing and anti-bribery policies. Campaigns are held annually to promote the policies and to remind staff how to report any concerns. The council has checks and balances in place to prevent individual members of staff being able to circumvent financial controls, eg deviation reports are produced and checked for expense claims that can highlight potential issues with claims, segregation of duties are applied in council processes. Management controls are also in place surrounding flexitime, annual leave and sickness absence.</p>				
Priorities for internal audit / counter fraud	<p>Veritau regularly liaises with senior management on internal fraud issues. Instance of internal fraud are analysed by both IA and CFT to determine if control weaknesses exist and can be addressed. The CFT provides training to all staff on whistleblowing and how to report concerns. Any suspicion of fraud or corruption is treated as a priority investigation. Serious cases of fraud will be reported to the police. Disciplinary action taken by the council relating to internal fraud issues is often supported by the CFT. IA undertake work to ensure that appropriate checks and balances are in place to help prevent and detect internal fraud and corruption. In 2025/26 new e-learning training on whistleblowing will be released for employees and managers across the council and fraud awareness training for HR employees has also been scheduled.</p>				

Risk area #9	Recruitment fraud	Inherent risk	Medium	Residual risk	Medium
Risk description	Recruitment fraud can affect all organisations. Applicants can provide false or misleading information in order to gain employment such as bogus employment history and qualifications or providing false identification documents to demonstrate the right to work in the UK. There is danger for the council if recruitment fraud leads to the wrong people occupying positions of trust and responsibility, or not having the appropriate professional accreditation for their post. In addition, there have been reports nationally of 'polygamous working' fraud, where an employee, usually in a temporary position, works for a number of different organisations at the same time.				
Risk controls	The council has controls in place to mitigate the risk of fraud in this area. DBS checks are undertaken for certain roles as necessary. Additional checks are made on applications for roles involving children and vulnerable adults. References are taken from previous employers and there are processes to ensure qualifications provided are genuine. Right to work checks are completed in line with statutory guidance. The National Fraud Initiative undertakes payroll data matches to identify employees who are working for multiple organisations at the same time.				
Priorities for internal audit / counter fraud	Where there is a suspicion that someone has provided false information to gain employment, CFT will be consulted on possible criminal action in tandem with any disciplinary action that may be taken. Applicants making false claims about their right to work in the UK or holding professional accreditations will be reported to the relevant agency or professional body, where appropriate. The CFT routinely share details of identities found to be used in polygamous working with HR to prevent and detect potential issues. IA plan to review council recruitment and selection processes in 2025/26.				

Risk area #10	Theft of assets	Inherent risk	Medium	Residual risk	Low
Risk description	The theft of assets can cause financial loss and reputational damage. It can also negatively impact on employee morale and disrupt the delivery of services. The council own a large amount of portable, desirable physical assets such as ICT equipment, vehicles, and tools that are at higher risk of theft.				
Risk controls	Specific registers of physical assets (eg capital items, property, and ICT equipment) are maintained. The council operates CCTV systems covering key premises and locations where high value items are stored. Entrances to council buildings are regulated and controlled via different access methods. The council employs a specialist security team to safeguard its premises, employees, and assets. The security team respond to incidents of theft through increased patrols and recommending improvements to processes. The council's whistleblowing arrangements provide an outlet for reporting concerns of theft. Thefts are reported to the police and Veritau.				
Priorities for internal audit / counter fraud	Instances of theft will be investigated by CFT where appropriate.				

Risk area #11	Treasury management	Inherent risk	Medium	Residual risk	Low
Risk description	Treasury Management involves the management and safeguarding of the council's cash flow, its banking, and money market and capital market transactions. The impact of fraud in this area could be significant.				

Risk controls	Treasury Management systems are subject to a range of internal controls, legislation, and codes of practice which protect council funds. Only pre-approved employees can undertake transactions in this area and they work within pre-set limits.
Priorities for internal audit / counter fraud	IA conduct periodic work in this area to ensure controls are strong and fit for purpose.

Risk area #12	Grant schemes	Inherent risk	Medium	Residual risk	Low
Risk description	The council takes on the responsibility for disbursing government funded grant schemes to local residents, businesses, and other organisations. Fraud in this area can include applicants supplying incorrect information to obtain grant payments or grant funded works (for example where grant funds are paid to a third-party supplier). Suppliers undertaking work may overcharge or not complete work to agreed standards. The council can become liable for recovery of any incorrectly paid government funding. This can create a loss to the council and may affect access to future grant schemes.				
Risk controls	The council will complete any required fraud management plan which will consider fraud risks, and mechanisms for preventing and detecting fraud. When awarding payments or agreeing works, the council (or their contractor) will complete checks to confirm applicants' eligibility.				
Priorities for internal audit / counter fraud	The CFT and IA support the development of fraud management plans, and associated controls, where required. CFT will undertake investigation in cases of suspected fraud. IA regularly undertake certification work on grant funded schemes.				

Risk area #13	Blue badge & parking fraud	Inherent risk	Low	Residual risk	Low
Risk description	Blue Badge fraud carries low financial risk to the authority but can affect the quality of life for disabled residents and visitors. There is a risk of reputational damage to the council if abuse of this scheme is not addressed. Other types of parking fraud also occur, including the misuse of residential parking permits by the owners of short term holiday lets to avoid commercial parking charges. Electronic payments by members of the public for use of council car parks can be diverted by criminals using false QR codes.				
Risk controls	Measures are in place to control the issue of blue badges, to ensure that only eligible applicants receive badges. Checks are made to ensure that commercial businesses don't inappropriately access residential parking permits. The council participates in the National Fraud Initiative which flags badges issued to deceased users, and badge holders who have obtained a blue badge from more than one authority, enabling their recovery to prevent misuse. The CFT and Parking Enforcement work closely together to identify, deter and investigate parking fraud. Proactive days of action are undertaken by both teams to raise awareness and act as a deterrent to blue badge misuse. Warnings are issued to people who misuse parking permits and blue badges. Serious cases of both types of fraud are considered for prosecution. Council car parks are monitored to detect and deter efforts to divert electronic payments.				
Priorities for internal audit / counter fraud	The CFT will continue to investigate fraud in this area as well as undertaking days of action to combat blue badge fraud in the course of the year. The team will work with the parking department to investigate an emerging risk, the use of false QR codes in council car parks to divert payments.				

APPENDIX B: COUNTER FRAUD DEVELOPMENT PLAN

Veritau is responsible for maintaining, reviewing, and strengthening counter fraud arrangements at the council. An annual review of priorities for the future development of counter fraud arrangements is therefore undertaken. Actions to be taken over the next year are set out below.

In addition to the specific areas set out in the table below, ongoing activity will continue in other areas that contribute to the council's arrangements for countering the risk of fraud, including:

- a rolling programme of fraud awareness training for officers based on priorities identified through the fraud risk assessment and any other emerging issues
- regular reporting of internal audit and counter fraud activity to the Audit and Governance Committee.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
1	Update the council's whistleblowing policy and deliver training	Governing	October 2025	Veritau / Human Resources	The council's whistleblowing policy will be reviewed and updated. E-learning packages will also be rolled out to employees and managers in support of the new policy.
2	Evaluate results of compliance pilots	Governing	September 2025	Veritau	Compliance pilots for council tax support and council tax discounts are ongoing. If proven effective they could become normal counter fraud work.
3	Review and maintain the council's fraud risk assessment	Acknowledging	Ongoing	Veritau	Ensure the council are made aware of new threats and respond to emerging threats like polygamous working and use of false QR codes.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
4	Provide training to staff involved in procurement	Preventing	December 2025	Veritau / Procurement Team	The new Procurement Act 2023 'goes live' in February 2025. Updated training will be delivered to employees working in this area.
4	Evaluate the impact of the new Economic Crime and Corporate Transparency Act.	Preventing	September 2025	Veritau / Legal Department	The council may require policy change to reflect the new legislation as well as training for relevant employees.
5	Review and investigate results of the 2024/25 National Fraud Initiative (NFI).	Pursuing	December 2025	Veritau	Data was submitted to the Public Sector Fraud Authority in October 2024 and results have been sporadically released since December. There are currently 52k matches to review.
6	Explore data matching exercises with neighbouring local authorities to identify fraud.	Protect	April 2026	Veritau	Fraud can occur across council boundaries. Regional data matching exercises can identify fraud that otherwise might not be detected.

APPENDIX C: COUNTER FRAUD WORK PLAN

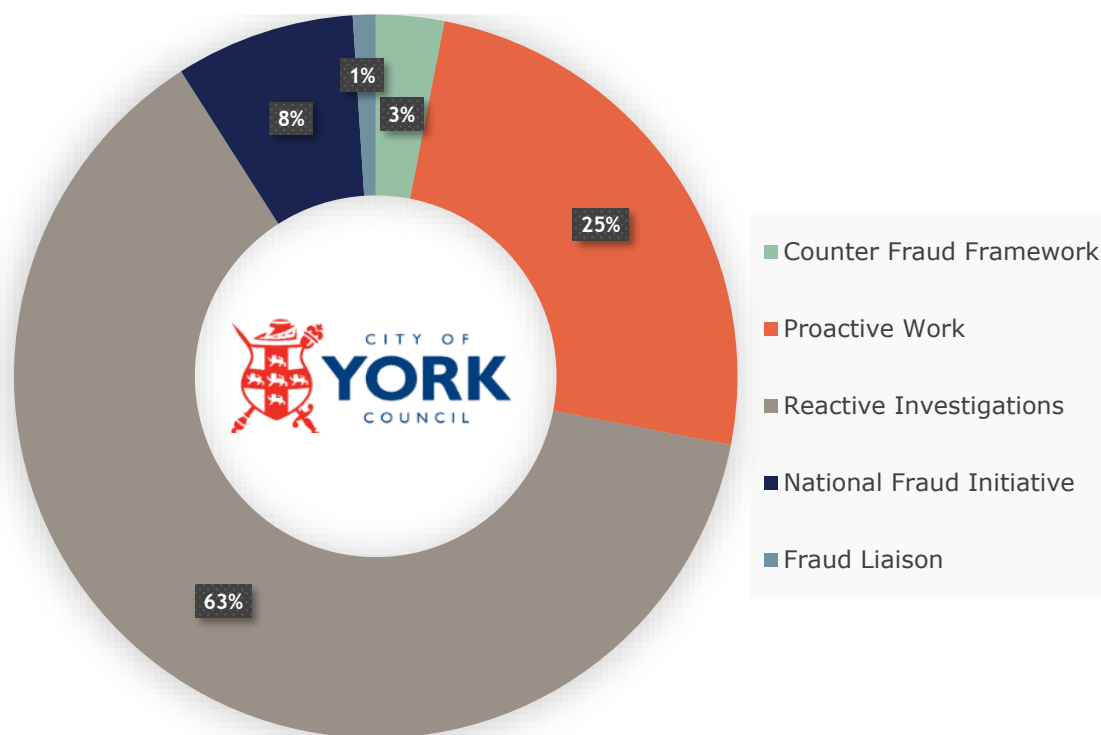
- 1 Veritau undertakes counter fraud work on behalf of City of York Council. This document summarises expected counter fraud activity for 2025/26.
- 2 A large part of the work of the team involves undertaking reactive investigations. The level of investigations is driven by referrals received from officers and the public about suspected fraud. Other work will be undertaken in accordance with priorities determined by the Fraud Risk Assessment and Counter Fraud Development Plan. A high-level summary of areas of counter fraud work are shown in table 1 below.

Table 1: Counter fraud work programme

Programme area	Purpose
▲ Counter Fraud Framework	Monitoring changes to regulations and guidance, reviewing counter fraud risks, and support to the council with maintenance of the counter fraud framework. Updates on significant fraud trends and counter fraud activities will be provided to the Audit and Governance Committee during the year.
▲ Proactive Work	<p>This includes:</p> <ul style="list-style-type: none"> • raising awareness of counter fraud issues and procedures for reporting suspected fraud - for example through training and provision of updates on fraud related issues • targeted proactive counter fraud work - for example through local and regional data matching exercises • support and advice on cases which may be appropriate for investigation and advice on appropriate measures to deter and prevent fraud.
▲ Reactive Investigations	Investigation of suspected fraud affecting the council. This includes feedback on any changes needed to procedures to prevent fraud reoccurring.
▲ National Fraud Initiative	Coordinating submission of data to the Public Sector Fraud Authority for the National Fraud Initiative (NFI) data matching programme and investigation of subsequent matches.
▲ Fraud Liaison	Acting as a single point of contact for the Department for Work and Pensions, to provide data to support housing benefit investigations.

- 3 The overall level of service is based on an indicative number of days for planning purposes (983 for 2025/26). Figure 1 below shows the proportion of time we expect to deliver across each area during the year.

Figure 1: Indicative spilt of counter fraud work



- 4 The split of activities shown in the figure above are not fixed. Actual work will depend on the level of suspected fraud referred to the team. We will also keep priorities for proactive and other counter fraud work under review, to ensure counter fraud resources continue to be used in the areas of greatest value to the council.