

2026/27 Counter Fraud Plan

Date: 16 April 2026

APPENDIX 1

CONTENTS

3	Background
3	National Counter Fraud Strategy
5	Fraud Risk Assessment
6	Development and Work Plans
6	Policy Framework Review
7	Annex A: Fraud Risk Assessment
18	Annex B: Counter Fraud Development Plan
20	Annex C: Counter Fraud Work Plan

BACKGROUND

- 1 Fraud continues to be a significant and growing risk to the public sector. Fraud offences account for 41% of all crime reported in the UK¹. 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 was detected and recovered². These losses directly reduce councils' ability to fund essential 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 fraud. It is important to promote a strong anti-fraud culture at all levels of the organisation as well as amongst the public.
- 3 Criminals are constantly improving their techniques and using new tools to defraud local authorities and other public sector bodies. 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 Middlesbrough 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 2026/27.

NATIONAL COUNTER FRAUD STRATEGY

- 5 CIPFA sets out the responsibilities of Local Authority leaders to counter fraud and corruption within their organisations in its code of practice on managing the risk of fraud and corruption³. The code says that organisations should:
 - acknowledge their responsibility 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 cases of fraud and corruption.
- 6 Fighting Fraud and Corruption Locally (FFCL) published the most recent counter fraud and corruption strategy for local government⁴ in 2020. Over the past six years Middlesbrough Council has followed the principles set out by CIPFA and FFCL to guide and develop its response to fraud.
- 7 The strategy recommends that councils consider the effectiveness of their counter fraud framework by considering performance against the five key themes set out below.

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

- **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 maintains a robust and regularly reviewed anti-fraud policy framework, supported by ongoing communication and reminders to staff. Counter-fraud activity is reported to both members and senior officers throughout the year. Middlesbrough Council sets clear expectations of honesty and integrity for all employees. The Council maintains an up to date whistleblowing policy. Veritau provides whistleblowing support to employees and managers, logs all referrals, operates a whistleblowing hotline, publicises the policy, and delivers training. The anti-fraud, bribery and corruption policy guide how fraud is investigated at the Council and how cases are concluded when fraud is proven to have occurred.

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

Middlesbrough Council is aware that it is regularly targeted by fraudsters across different service areas. An annual fraud risk assessment is produced and presented to members. The assessment draws on national fraud trends, intelligence from cases reported to and investigated by the counter fraud team, and the insights of senior officers who understand the risks within their service areas. Each year, targeted development activity is planned in response to the assessed risks, emerging issues, and ongoing evaluation of the Council's arrangements against recognised good practice guidance. As a result of increased workload and positive results from counter fraud activity the Council increased the level of resource for counter fraud work in 2025/26 and it has increased again for 2026/27.

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

Fraud prevention is embedded in the work of both the counter fraud and internal audit teams. When investigations highlight opportunities to strengthen controls, these findings are shared with senior officers, and follow-up checks ensure that agreed improvements are implemented. Ongoing investment in specialist training helps counter fraud officers stay current with emerging technologies and techniques. In addition, collaboration with the Communications Team supports the development of a proactive anti-fraud culture across the organisation and within the wider community the Council serves.

- **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.*

The Council takes strong action to hold offenders to account and to recover public funds lost to fraud. All allegations are investigated to

criminal standards, and prosecution is considered where appropriate, alongside a range of alternative sanctions. The Council has a constructive partnership with Cleveland Police and raises concerns with them where appropriate. The counter fraud team has built bonds with the Department for Work and Pensions (DWP) to tackle council tax reduction scheme fraud, with joint investigations often providing a more efficient and effective response to fraud affecting both agencies. The Council explores every available avenue for financial recovery, including the use of civil remedies. Counter fraud activity has resulted in £371k in savings in 2025/26 (up to the end of February), demonstrating the impact of this work.

- **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 the North East and residents are as likely to be targeted as the Council is. The Council regularly issues alerts to warn residents about emerging scams and fraudulent activity. National data matching helps identify where residents may be the victims of identity theft. Regular liaison with other councils in the region can identify fraud that is occurring cross boundary.



FRAUD RISK ASSESSMENT

- 8 Fraud risks are assessed annually to identify priorities for counter fraud work. The 2026/27 fraud risk assessment, included in annex A, draws on national and regional intelligence affecting local authorities, as well as cases reported directly to the counter fraud team. Each area is assigned an inherent risk rating, reflecting the level of exposure to fraud if no controls existed, and the residual risk rating indicates the remaining risk when current controls are considered.

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. 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.
- 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. However, it is separate from the wider Council risk management framework.

- 11 The updated risk assessment factors in upcoming work by internal audit and the counter fraud team, eg introduction and revision of e-learning modules providing training on social care fraud and whistleblowing, support to the Council to prevent fraud within the new Crisis and Resilience Fund and help protecting the Council from fraud associated with the new Failure to Prevent Fraud offence.
- 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 2026/27 counter fraud development plan is attached in annex B. It sets out development activity for the counter fraud team and Middlesbrough Council for the year. Actions are organised into the five key themes set out by the FFCL counter fraud strategy for local government and any findings from the Fraud Risk Assessment.
- 14 The counter fraud work plan is attached in annex C. The plan sets out the areas of counter fraud work to be undertaken in 2026/27. 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 400 days has been allocated to counter fraud work in 2026/27, an increase of 150 days.



POLICY FRAMEWORK REVIEW

- 15 The Council's counter fraud policy framework is reviewed annually. The review considers counter fraud related policies (including the anti-fraud and corruption, prosecution, anti-bribery, and whistleblowing policies).
- 16 The review identified that the Council's whistleblowing policy requires updating to reflect upcoming changes to whistleblowing legislation due to the Employment Rights Act 2025 as well as a recent employment tribunal decision. No other changes or updates to policies are required currently.

ANNEX A: 2026/27 FRAUD RISK ASSESSMENT

Risk area #1	Social care fraud	Inherent risk	High	Residual risk	High
Risk description	<p>Adult social care customers complete a financial assessment with the Council to determine any financial contribution they must make towards their care. Losses can occur through deprivation or non-declaration of capital which can involve the transfer or disguise of property 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.</p>				
Risk controls	<p>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. 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.</p>				
Priorities for internal audit / counter fraud	<p>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. The CFT delivers a rolling programme of fraud awareness to employees with responsibilities for assessment and payments. 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.</p>				

Risk area #2	Creditor fraud	Inherent risk	High	Residual risk	High
Risk description	<p>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 email accounts of suppliers and using these to attempt to commit mandate fraud. These attempts can be much more difficult to detect and prevent.</p>				
Risk controls	<p>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. Organisations' reliance on its own employees, and those of its suppliers, to follow processes, and the inevitable element of human error, are factors in many successful mandate fraud attacks.</p>				
Priorities for internal audit / counter fraud	<p>Veritau regularly provide support and advice to finance officers responsible for the payment of suppliers. The IA work programme includes audits of key financial systems and processes. This includes ordering and creditor payment processes, eg segregation of duties and controls to prevent mandate fraud. IA also undertake duplicate payment checks on a regular basis. The CFT delivers fraud awareness training to relevant officers. 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, as well as directly to the email provider from which false emails originated. The CFT regularly shares intelligence alerts relating to attempted fraud occurring</p>				

nationally with relevant council officers to help prevent losses. As part of any investigation of attempted fraud in this area, the CFT will advise on improvements to help strengthen controls.

Risk area #3	Cybercrime	Inherent risk	High	Residual risk	High
Risk description	<p>Cybercrime is a continually evolving area where criminals refine their techniques in order to overcome controls, obtain unauthorised access and information, and frustrate systems. In 2025, the government reported that approximately 612,000 UK business and 61,000 charities identified cyber breaches or attacks over a 12 month period. The potential for cybercrime is heightened by the availability of online tools and AI-driven attacks. 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. There have been several 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.</p>				
Risk controls	<p>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. Council systems could be exposed by yet unknown weaknesses in software. Suppliers of software or IT services could also be compromised which might allow criminals access to council systems believed to be secure. The residual risk</p>				

	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 and is overseen and delivered by CISA (Certified Information System Auditor) accredited auditors. Planned audits in 2026/27 cover disaster recovery, third party risk, and cloud management. 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 is 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 can also involve falsely claiming discounts that a business is not entitled to, eg small business rate relief. Reports of business rate fraud are less prevalent 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 visits to properties are undertaken 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 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	The CFT delivers fraud awareness training to employees in the revenues team about frauds affecting Council Tax and Business Rates. IA routinely review the administration of Council Tax and Business Rates as one of the Council's key financial systems.
--	--

Risk area #5	Council tax reduction fraud	Inherent risk	High	Residual risk	Medium
Risk description	Council Tax Reduction (CTR) 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. CTR fraud can involve applicants failing to declare their total assets or income. 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 CTR 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 CTR to identify potential issues. The Council will routinely take part in the National Fraud Initiative (NFI) which highlights potentially fraudulent claims. The DWP use data from HMRC on claimants' incomes which is then passed through to council systems. This 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 jointly works with the DWP to investigate fraud that affects both organisations, this can help achieve better results for the Council where state benefits are involved. The CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution.				
Priorities for internal audit / counter fraud	The CFT will continue to raise awareness of fraud with teams involved in processing claims for CTR and highlight reporting lines for suspected fraud. CFT will also seek opportunities to raise awareness with the public about the mechanisms for reporting fraud. If fraud cannot be addressed by the Council directly it will be reported to the DWP. CFT will continue to promote joint working with the DWP.				

Risk area #6	Procurement fraud	Inherent risk	High	Residual risk	Medium
Risk description	<p>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'.</p>				
Risk controls	<p>The Council has established Contract Procedure Rules. The rules are reviewed regularly and ensure the requirement for a competitive process (where required) through an e-tender system. A team of procurement professionals provide guidance and advice to ensure procurement processes are carried out correctly. The Middlesbrough Manager Framework includes contract management expectations for managers. The Contract Procedure Rules also set out the requirements for declarations of interest to be made. Contract monitoring helps to detect and deter potential fraud.</p>				
Priorities for internal audit / counter fraud	<p>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 have a planned audit within Procurement in 2026/27.</p>				

Risk area #7	Theft of assets	Inherent risk	High	Residual risk	Medium
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's whistleblowing arrangements provide an outlet for reporting concerns of theft.				
Priorities for internal audit / counter fraud	Thefts are reported to the police and Veritau. Instances of theft are investigated by CFT where appropriate.				
Risk area #8	Internal fraud	Inherent risk	Medium	Residual risk	Medium
Risk description	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 to obtain salary payments. A new criminal offence came into force in 2025, Failure to Prevent Fraud, which holds large				

	organisations like the Council accountable for fraud committed by employees, contractors, suppliers that is designed to benefit it.
Risk controls	The Council has up to date whistleblowing, counter fraud policies, and anti-bribery policies. Campaigns are held annually to promote the policies and to remind staff how to report any concerns. Veritau provide e-learning training on whistleblowing to council employees and managers. 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.
Priorities for internal audit / counter fraud	Veritau regularly liaises with senior management on internal fraud issues. Where internal fraud arises, IA and the CFT will review the circumstances to determine if there are underlying control weaknesses that can be addressed. CFT provide training to HR officers on internal fraud and whistleblowing issues. CFT investigate any suspicions of fraud or corruption. Serious cases of fraud will be reported to the police. In some instances, it may be necessary to report individuals to their professional bodies. CFT support any disciplinary action taken by the Council relating to internal fraud issues.

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 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. Polygamous working is an emerging fraud risk; this occurs when an employee, usually in a temporary position, works for several different organisations at the same time. There have been growing numbers of cases identified in the UK and a number of prosecutions have been publicised.				

Risk controls	The Council has controls in place to mitigate the risk of fraud in this area. DBS checks are undertaken where 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. The National Fraud Initiative undertakes payroll data matches to help 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, the 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.

Risk area #10	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 #11	Grant schemes	Inherent risk	Medium	Residual risk	Low
Risk description	<p>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.</p>				
Risk controls	<p>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.</p>				
Priorities for internal audit / counter fraud	<p>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. A new scheme, the Crisis and Resilience Fund, will be introduced in April 2026. Veritau will support the Council to prevent fraud against the scheme and protect funds meant for vulnerable people.</p>				
Risk area #12	Blue badge fraud	Inherent risk	Low	Residual risk	Low
Risk description	<p>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 low level parking fraud is relatively common, for example, misuse of residential permits to avoid commercial parking charges.</p>				

Risk controls	Measures are in place to control the issuing of blue badges, to ensure that only eligible applicants receive badges. 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.
Priorities for internal audit / counter fraud	The CFT undertake periodic proactive days of action with the Council's enforcement team. This helps raise awareness and act as a deterrent to blue badge misuse. Warnings will be issued to people who misuse parking permits and blue badges. Serious cases will be considered for prosecution.

ANNEX 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 Committee.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
1	Update the Council's whistleblowing policy	Governing	May 2026	Veritau / Human Resources	The Council's whistleblowing policy will be revised to reflect changes in the law. E-learning material will also be updated to reflect this.
2	Review and maintain the Council's fraud risk assessment	Acknowledging	Ongoing	Veritau	Ensure the Council is made aware of new threats and respond to emerging risk like polygamous working and the new Failure to Prevent Fraud offence.
3	Increase levels of counter fraud work undertaken in 2026/27.	Acknowledging	Ongoing	Veritau	Manage the increase in resource for counter fraud work (150 days) to obtain good outcomes for the Council.
4	Raising awareness of adult social care fraud amongst employees	Preventing	Ongoing	Veritau	In 2026/27 Veritau will introduce an e-learning module on adult social care and make it available to employees working in the area.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
5	Support service areas in collation and submission of data for the 2026/27 National Fraud Initiative	Pursuing	November 2026	Veritau / Council Departments	Veritau will receive data from a range of council departments, cleanse data to meet NFI specifications, and securely upload it. Privacy notices will also be reviewed to ensure compliance with data sharing regulations.
6	Support the Council to introduce the new Crisis and Resilience Fund	Protect	Ongoing	Veritau	Helping prevent fraud in this new scheme will protect funds meant to support the public in times of crisis.
7	Continue active engagement with neighbouring bodies and local authorities.	Protect	Ongoing	Veritau	Fraud can occur across council boundaries. CFT are active members of regional professional networks in Yorkshire and the North East. These forums bring together fraud officers, internal auditors, and housing associations. Identifying opportunities to share information and joint working can help to detect and deter fraud.

ANNEX C: COUNTER FRAUD WORK PLAN

A total of 400 days has been allocated to counter fraud work in 2026/27, an increase of 150 days. A large proportion of this work will comprise reactive investigations which are determined 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 the areas for counter fraud work is shown in the table below.

Area	Scope
Counter Fraud General	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 Committee during the year.
Proactive Work	This includes: <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 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 the submission of data and investigation of matches produced by the National Fraud Initiative (NFI).

Area	Scope
Fraud Liaison	Joint Work with the Department for Work and Pensions where appropriate and provide data to support housing benefit investigations. Liaise with neighbouring local authorities to address cross boundary fraud.