Cherwell
DISTRICT COUNCIL
NORTH OXFORDSHIRE

2025/26
Counter Fraud Plan

Date: 19 March 2025

APPENDIX 1

Veritau
Assurance for the public sector

CONTENTS

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 crime[1]. The government estimated that up to £81 billion of public spending was lost to fraud in 2023-24[2]. 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 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 corruption[3]. 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 government[4].

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] The impact of fraud and error on public funds 2023-24, National Audit Office, published November 2024.
[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 has a strong anti-fraud policy framework that is reviewed annually. Counter fraud work is regularly reported to members and officers in the course of the year. The Council introduced an updated whistleblowing policy in 2024/25.

- **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 used alongside good practice guidance and information on emerging trends to prioritise counter fraud development activity and investigative work.

- **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. Joint working arrangements are in place with the Department for Work and Pensions. All avenues are considered to recover loss, including civil recovery.

- **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 Oxfordshire and residents are as likely to be targeted as the Council is. 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. The counter fraud team intend to develop information sharing protocols with more stakeholders 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 annex 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.

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. We will be seeking to further develop the risk assessment in the coming year by working with officers responsible for management of risks in key areas.

11 The updated risk assessment factors in upcoming work by internal audit and the counter fraud team. 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

12 The 2025/26 counter fraud development plan is included in annex B. It sets out development activity for the counter fraud team and Cherwell District Council 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.

13 The counter fraud work plan is included in annex 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.

POLICY FRAMEWORK REVIEW

14 The Council's counter fraud policy framework is reviewed annually. The review considers a number of counter fraud related policies (including the Counter Fraud and Corruption Policy, the Anti-Money Laundering Policy, the whistleblowing policy, and other associated policies).

15 The review found no requirement to change or update policies at the present time. However, 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.

ANNEX A: 2025/26 FRAUD RISK ASSESSMENT

Risk area #1	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 email accounts of suppliers and using these to attempt to commit mandate fraud. These attempts can be much more 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's 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. Nevertheless, the team act with vigilance and experience, and are able to identify problems which may not be picked up through techniques such as Artificial Intelligence.				
Priorities for internal audit / counter fraud	Veritau regularly provide support and advice to finance officers responsible for the payment of suppliers. The Internal Audit 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. Internal Audit (IA) also undertake duplicate payment checks on a regular basis. The Counter Fraud Team				

	(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 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 that will strengthen controls.

Risk area #2	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. 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. The ICT department 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	IA routinely include ICT audits in the annual work programme. Cybersecurity is an ongoing priority for IA work. Raising awareness with employees can be crucial in helping to prevent successful cyberattacks. The CFT works with ICT to support activities on raising awareness amongst employees. ICT can access free resources from the National Cyber Security Centre to help develop and maintain their cyber defence strategy.

Risk area #3	**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 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).				

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. The CFT provide a deterrent to fraud in this area through the investigation of potential offences which can, in serious cases, lead to prosecution.

Risk area #4	**Council Tax Reduction and Discretionary Housing Payment 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. CTR fraud can involve applicants failing to declare their total assets or income. Most CTR claims are linked to state benefits (eg Universal Credit) which are administered by the Department for Work and Pensions (DWP). Discretionary Housing Payment (DHP) is government-funded scheme which supports the housing costs of residents who also receive Housing Benefit or Universal Credit (UC). It is a limited pot of funding, and applications are evaluated on a case-by-case basis in line with the Council's policy. Fraud and error in these schemes are of relatively low value on an individual basis but cumulatively fraud in this area could amount to a substantial loss.				
Risk controls	The Council undertakes eligibility checks on CTR applicants who are not already in receipt of UC, and on DHP applications. The Council will routinely take part in the National Fraud Initiative (NFI) which highlights potentially fraudulent CTR claims. The DWP use data from HMRC on claimants' incomes which is then passed through to Council systems. There are established lines of communication with the DWP where claims for support are linked to externally funded benefits. The Council can undertake joint investigations with the DWP to investigate fraud that affects both organisations. This can help achieve better results for the Council where state benefits are involved.				
Priorities for internal audit / counter fraud	The CFT regularly raises awareness of fraud with teams involved in processing claims for CTR. The CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution. Concerns of fraud can be reported to the CFT by employees. The 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. The CFT intends to undertake				

	more proactive work to identify any application and identity frauds affecting DHP applications in the next financial year.

Risk area #5	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 interest 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 regularly undertake procurement related work to help ensure processes are effective and being followed correctly. The CFT can provide updated fraud training for the procurement team as a result of the legislation.				

Risk area #6	Housing related fraud	Inherent risk	High	Residual risk	Medium
Risk description	The Council has a statutory duty to provide a homelessness and housing options service to Cherwell residents. The Council also has a small housing stock of its own. Housing fraud can deprive local residents, the Council and Housing Associations of social housing provision through false applications.				
Risk controls	The Council has strong controls in place to prevent false applications for housing. The CFT can provide a deterrent to fraud in this area through the investigation of any suspected fraudulent housing application using powers under the Housing Act. Offenders can face criminal prosecution and repossession of their Council or social housing properties.				
Priorities for internal audit / counter fraud	The CFT will continue to raise awareness of fraud with teams involved in applications for housing and the management of housing stock. The investigation of reports alleging subletting of Council properties are treated as a priority.				

Risk area #7	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 occurs 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. It can also include theft of council assets, and 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.
Risk controls	The Council has up to date whistleblowing and anti-bribery policies. Campaigns are held annually to promote the policies and to remind employees how to report any concerns. The Council has checks and balances to prevent individual employees being able to circumvent financial controls, e.g. segregation of duties. Controls are in place surrounding flexitime, annual leave and sickness absence. The Council regularly participates in the National Fraud Initiative. Data matches include checks on payroll records for potential issues.
Priorities for internal audit / counter fraud	Veritau 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. The CFT support any disciplinary action taken by the Council relating to internal fraud issues.

Risk area #8	**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 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 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 #9	**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.				

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 Accounts, Audit and Risk Committee (AARC).

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
1	Provide fraud awareness training to staff involved in procurement	Governing	December 2025	Veritau / Procurement Team	The new Procurement Act 2023 'goes live' in February 2025.
2	Continue providing fraud awareness to staff in emerging areas, including recruitment and polygamous working frauds, and grant schemes	Governing	Ongoing	Veritau	
	Provide fraud awareness training to Council Members	Governing	December 2025	Veritau	
3	Review and maintain the Council's fraud risk assessment	Acknowledging	Ongoing	Veritau / AARC	The fraud risk assessment is subject to annual review. Emerging threats will be considered as required during the course of the year to make sure

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
					the risk assessment remains up to date.
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	Undertake proactive work in the Discretionary Housing Payment scheme to assess for any attempted identity and application frauds	Preventing	September 2025	Veritau / Benefits	
6	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 late December. There are currently 980 matches to review.
7	Explore further opportunities to engage with neighbouring bodies and local authorities.	Protect	April 2026	Veritau	Fraud can occur across Council boundaries. Information sharing and joint working could help detect and deter fraud.

ANNEX C: COUNTER FRAUD WORK PLAN

A high-level summary of the areas for counter fraud work in 2025/26 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 Accounts, Audit and Risk Committee (AARC) during the year.
Proactive Work	This includes: • 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 investigation of data matches produced by the National Fraud Initiative (NFI).
Fraud Liaison	Joint work with the Department for Work and Pensions where appropriate and provide data to support housing benefit investigations. Liaise with regional local authorities to address cross-boundary fraud.