NORTH YORKSHIRE COUNCIL

AUDIT COMMITTEE

18 MARCH 2024

COUNTER FRAUD FRAMEWORK REPORT

1.0 PURPOSE OF THE REPORT

1.1 To note the results of the annual fraud risk assessment.

1.2 To seek Member approval for the 2024/25 counter fraud strategy action plan and the counter fraud workplan.

1.3 To seek Member approval for the updated Anti-Money Laundering & Terrorist Financing Policy.

2.0 BACKGROUND

2.1 Fraud remains a serious risk to the public sector in the UK. When fraud is committed against the public sector, funds are diverted from essential public services into the hands of criminals. Fraud has become the most common offence in the UK, accounting for 41% of all crime[1].

2.2 Veritau provides a counter fraud service to the Council. This includes the maintenance of the counter fraud framework which includes policies and processes designed to help prevent, detect and deter fraud. The framework is reviewed annually.

3.0 COUNTER FRAUD FRAMEWORK

3.1 An updated counter fraud framework is contained in **appendix 1**. The updated framework reflects a number of national developments which affect local government, including the establishment of the Public Sector Fraud Authority and the potential for new legislation which will create a corporate offence of failing to act to prevent fraud.

3.2 The counter fraud framework sets out the Council's approach to minimising the risk of fraud. It includes an updated fraud risk assessment. The Identification of fraud threats is key to assessing the Council's current exposure to risk. The assessment is designed to identify the areas of fraud that present the greatest risk to the Council and is informed by national and regional reports of fraud affecting local authorities. The results of the assessment will be used to focus future audit and counter fraud work and to help develop or strengthen fraud prevention measures.

3.3 The assessment identifies the following as key areas of focus for counter fraud work

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

in 2024/25:

- Adult social care fraud
- Creditor fraud
- Cybercrime

3.4 The fraud risk assessment will be kept under review so that any significant new or emerging risks are identified and addressed.

3.5 The framework update also includes a new strategy action plan for 2024/25 and provides details of the actions completed from last year's plan.

3.6 In addition, a number of limited changes have been made to the Council's Anti-Money Laundering & Terrorist Financing Policy. The changes include the identification of a deputy Money Laundering Reporting Officer (in paragraph 1.5 of the policy).

4.0 COUNTER FRAUD WORKPLAN

4.1 The Counter Fraud workplan is attached as **appendix 2**. The plan sets out the areas of counter fraud work to be undertaken in 2024/25. The time allocation for each area is not known at this stage because it will depend on the levels of suspected fraud reported to the Corporate Fraud Team (CFT). 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 strategy action plan and fraud risk assessment.

4.2 A total of 1,100 days has been allocated to counter-fraud work in 2024/25.

5.0 IMPLICATIONS

5.1 There are no local member, financial, human resources, legal, equalities or climate change implications.

6.0 RECOMMENDATIONS

Members are asked to:

- note the results of the annual fraud risk assessment
- approve the 2024/25 counter fraud strategy action plan
- approve the updated Anti-Money Laundering & Terrorist Financing Policy

MAX THOMAS
Head of Internal Audit

29 February 2024

BACKGROUND DOCUMENTS

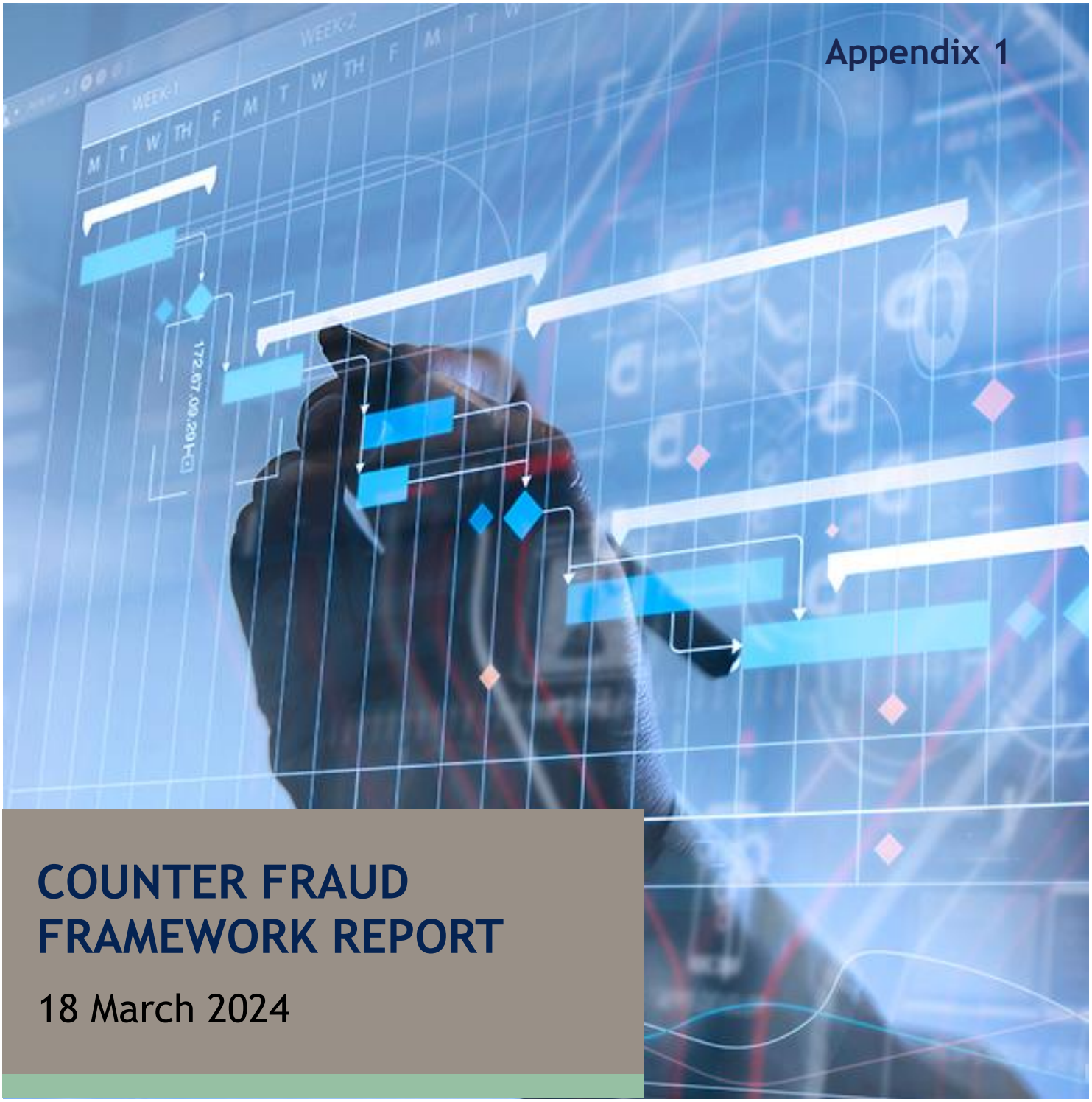
None

Report prepared and presented by Daniel Clubb, Assistant Director – Counter Fraud

Veritau - Assurance Services for the Public Sector
County Hall
Northallerton

Appendix 1 - Counter Fraud Framework Report
Appendix 2 - Counter Fraud Plan 2024/25

Appendix 1



COUNTER FRAUD FRAMEWORK REPORT

18 March 2024

Head of Internal Audit: Max Thomas

Assistant Director - Corporate Fraud:
Daniel Clubb

Veritau

INTRODUCTION

1 Fraud has become the most common offence in the UK, accounting for 41% of all crime[1]. It is a significant risk to the public sector. Fraud threats continue to evolve with new tools and techniques being used. It is also increasingly originating from national and international actors, as opposed to being a locally occurring issue.

2 The government estimated that between £33.2 and £58.8 billion of public expenditure was lost to fraud in 2020/21[2]. At a local level, fraud can impact the ability of local authorities to support public services and it can cause reputational damage.

3 To provide an effective response to fraud the Council needs to have a robust counter fraud framework in place that helps prevent, detect, and deter fraud. Fraudsters continually develop their approach to exploit systems and obtain funds. Counter fraud work therefore needs to develop at least as quickly as the techniques used by criminals seeking to defraud the Council.

NATIONAL PICTURE

4 The Public Sector Fraud Authority (PSFA) was launched in August 2022. The formation of the PSFA represents a potentially significant step in the government's efforts to modernise its counter fraud response. The PSFA will agree counter fraud plans with, and provide support to, central government departments and other public bodies to help combat fraud. The PSFA will focus on ministerial bodies but will share best practice and standards with local government[3]. The PSFA will also seek input from Councils on how they can support local government counter fraud functions.

5 The PSFA has taken on responsibility for the National Fraud Initiative (NFI). This is the exercise that matches data within and between public and private sector bodies to prevent and detect fraud. All local authorities are required to take part. Sitting within the National Counter Fraud Data Analytics Service, the NFI is likely to benefit from the use of new technology, including artificial intelligence.

6 Following the Covid-19 pandemic, there has been an increased emphasis on managing fraud risks in government funded grant schemes. Local authorities must consider the local arrangements in place to mitigate and address fraud when distributing central government funds through the creation of fraud management plans. Post assurance reviews and audits continue to provide opportunities to identify fraud and error.

---

[1] Progress combatting fraud (Forty-Third Report of Session 2022-23), Public Accounts Committee, House of Commons
[2] Tackling fraud and corruption against Government, HM Treasury / Cabinet Office
[3] Public Sector Fraud Authority Mandate, HM Government, September 2022

7 The government is also seeking to introduce new legislation that aims to hold organisations to account where they profit from employees committing fraud. The Economic Crime and Corporate Transparency Bill proposes a new offence of failing to prevent fraud. To mitigate fraud committed by employees, private sector and many public sector organisations will be required to have procedures in place to prevent fraud. Failure to do so could result in unlimited fines.

LOCAL PICTURE

8 Veritau provided counter fraud services to 5 of the former North Yorkshire district and borough councils. Since Local Government Reorganisation (LGR) in April 2023, Veritau has continued to provide counter fraud services to the new authority. The counter fraud team has continued to develop relationships with staff across the Council and to provide support. Veritau maintains fraud reporting mechanisms for Council employees and the public to report suspicions. Contact can be made by telephone on 0800 9179 247, or by email to counter.fraud@veritau.co.uk.

9 Raising the awareness of officers to the risks of fraud is essential to help to prevent fraud. Veritau continues to provide awareness training for council officers in services at higher risk of fraud as well as delivering wider fraud awareness information. The team has highlighted the whistleblowing policy, anti-money laundering and anti-bribery policies in campaigns this year. In addition, the dangers of cybercrime were raised as part of international cyber awareness month in October 2023.

10 The team are active members of regional counter fraud groups. The North East Counter Fraud Group recently received a presentation from the Competition and Markets Authority (CMA) on procurement fraud. They are developing a new tool to help organisations identify and prevent activity by procurement cartels. Veritau will monitor opportunities to work with external agencies, like the CMA, to enhance the Council's response to fraud.

11 Veritau represents the Council at regional and national counter fraud groups and chairs a national Fighting Fraud and Corruption Locally group that focusses on adult social care fraud. We have presented to counter fraud practitioners at national conferences to disseminate findings and share best practice.

FRAUD RISK ASSESSMENT

12 Veritau completes an annual Fraud Risk Assessment, designed to identify the areas of fraud that present the greatest risk to the Council. The risk assessment is informed by national and regional reports of fraud affecting local authorities as well as the fraud reported to and investigated by the counter fraud team. 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.

13 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.

14 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.

15 The updated risk assessment now includes the addition of grant schemes. Government departments are increasingly requiring local authorities develop a fraud management plan for grant schemes they are asked to administer. The plans set out measures in place to prevent, detect, and investigate fraud. Failure to document and implement these measures could result in Council requests for grant funding being denied, loss of public funds if fraudulent applications succeed, and the potential for the Council to become liable for irrecoverable payments made incorrectly.

16 The fraud risk assessment will be kept under review so that any significant new or emerging risks are addressed.

COUNTER FRAUD FRAMEWORK

17 The Council's counter fraud framework is reviewed annually. The framework contains a counter fraud strategy and associated action plan, a counter fraud policy, a fraud risk assessment, and a number of related policies (e.g. whistleblowing).

18 In March 2023, the Council adopted its current counter fraud and corruption strategy. The strategy takes into account the latest national guidance for tackling fraud in local government. The Council's strategy action plan is updated annually, and the latest version is included in **annex 2**, below. It details the progress made against last year's plan and introduces new priorities for the counter fraud team in 2024/25. New objectives this year include:

- exploring local data matching opportunities
- engaging with the public sector fraud authority.

19 A number of limited changes have been made to the Council's Anti-Money Laundering & Terrorist Financing Policy. The changes include the identification of a deputy Money Laundering Reporting Officer (in paragraph 1.5 of the policy). The revised policy is included at **annex 3.**

ANNEX 1: Fraud Risk Assessment (March 2024)

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
Adult Social Care Fraud	For adult social care, losses can occur through deprivation or non-declaration of capital. For example, the transfer or disguise of property and assets 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). Misuse of the Direct Payment scheme can occur for both adult and children's social care. For example, money allocated to meet a customer's assessed needs may not be used to procure appropriate services. In cases where fraud or error is identified, the average loss is £15k (based on the outcomes of investigations nationally over the last 11 years). Losses in individual cases can be much higher,	High	The Council's assessment team review applications for care funding 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 service. 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.	High	Counter Fraud Team (CFT) to deliver a rolling programme of fraud awareness training with staff in safeguarding, financial assessments and with relevant legal services team members. Regular work by internal audit reviews the control environment. Concerns of fraud should be reported to the CFT who can determine if criminal investigation would be effective.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	especially if they are not detected at an early stage. A recent case in the national press reported a £700k direct payment fraud.				
Creditor Fraud	The volume and sophistication of fraud against creditor payment systems has increased in recent years. 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	High	The Council has put strong controls in place to identify fraudulent attempts to divert payments from genuine suppliers and to validate any requests to change supplier details. Many employees who joined the authority from former district and borough councils will be familiar with these practices which were previously implemented locally as a response to emerging threats. 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, the frequency of attacks on public	High	Veritau will regularly provide support and advice to finance officers responsible for the payment of suppliers. Key financial systems and processes are subject to regular audit review, including creditors, debtors, and general ledger systems in 2023/24. Periodic work to identify duplicate payments also take place. An e-learning module developed prior to LGR that highlights threats to financial systems remains available to all employees. CFT delivered fraud awareness training to relevant teams ahead of the formation of the new authority. Increased awareness provides a greater chance to stop fraudulent attempts before losses occur.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	include whaling, where senior members of the Council are targeted and impersonated in order to obtain fraudulent payments. The Council must maintain awareness of increased risk from impersonation-based attacks. Staff members joining new teams may be deceived by fraudsters posing as council officers or suppliers with whom they are not yet familiar, and may work in different locations, in attempts to set up payments and release funds to non-supplier accounts. In recent years 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.		organisations, and potential employee adjustment to new teams and working practices as the authority continues to become established. The Council's reliance on employees working for both the Council and its suppliers to follow processes, and human error are factors in many successful mandate fraud attacks.		All instances of whaling fraud reported to CFT will be reported to the relevant agencies, such as the National Cyber Security Centre, as well as directly to the email provider from which false emails originated. The counter fraud team will share 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.
Cybercrime	Methods used by those perpetrating cybercrime	High	The Council has skilled ICT employees whose expertise	High	Raising awareness with employees can be crucial in

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	continue to evolve. Fraudsters 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. Some Council systems continue to be locally accessed until the can be integrated (eg Revenues and Benefits		can be 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 National Crime Agency report that cybercrime can now be committed by less technically proficient criminals. Human error was found to be a factor in 82% of cyber breaches according to a recent		helping to prevent successful cyberattacks. The CFT works with ICT to support activities on raising awareness. A campaign to mark cybersecurity awareness month is undertaken annually. Council employees are also required to complete regular cybersecurity training. Audits of ICT access controls, and ICT governance are in progress. ICT can access free resources from the National Cyber Security Centre to help develop and maintain their cyber defence strategy.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	records). Ensuring consistent security measures across the Council's infrastructure is key in protecting the wider system. There have been a number of high profile cyber-attacks on public and private sector organisations. Attacks stemming from the hacking of software or IT 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.		study[4]. 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 the regular review of controls.		
Council Tax and Business Rates Frauds (discounts and exemptions)	Council Tax discount fraud is a common occurrence. In 2022, CIFAS found that 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	High	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 (where necessary), to verify information.	Medium	CFT will deliver periodic fraud awareness training to employees in revenues and customer services teams about frauds affecting Council Tax and Business Rates. IA will routinely review the administration of Council Tax and Business Rates as one of

[4] 2022 Data Breach Investigations Report, Verizon

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	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. Business Rate fraud is less prevalent than Council Tax fraud but can lead to higher losses in individual cases. The Council has brought together employees that previously operated separately across North Yorkshire. During the phase of restructuring, fraudsters may try to take advantage of changes to working practice and levels of local knowledge to exploit opportunities to obtain discounts and exemptions.		The Council will routinely take part in the National Fraud Initiative (NFI). An exercise to review Single Person Discount entitlement is in progress. The Council undertakes rolling reviews of single person discounts to ensure that those receiving a discount remain eligible to do so.		the Council's key financial systems. CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution. CFT will also seek opportunities to raise awareness with the public about mechanisms for reporting fraud and publicise any successful prosecutions to act as a deterrent. CFT will be exploring opportunities to proactively identify fraud through data matching in this area.
Council Tax Support Fraud	Council Tax Support (CTS) is a Council funded reduction in liability introduced in 2013 to	High	The Council undertakes eligibility checks on those who apply for support. Officers with	Medium	CFT will routinely raise awareness of fraud with teams

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	replace Council Tax Benefit. It is resourced through Council funds. Fraud and error in this area is often of a 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 declare their total assets, correct household composition or household 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. Many CTS claims are linked to state benefits (eg Universal Credit) which are administered by the Department for Work and Pensions (DWP). The Council has limited influence on DWP decision making which makes it harder to address fraud in this area.		suitable training in benefits will 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). Further matching will take place in 2024/25 which will help identify incorrect claims for CTS. The DWP use data from HMRC to confirm claimants' income. This information is passed through to council systems. This mitigates the risk of claimant's 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 will report suspected fraud to the DWP, but this does not always give		involved in processing claims for CTS. 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 CFT by Council employees. CFT also seek opportunities to raise awareness with the public about mechanisms for reporting fraud. If fraud cannot be addressed by the Council directly it will be reported to the DWP. CFT engage with the DWP at a senior level to foster collaborative working wherever possible. The team now undertake joint investigations with DWP counterparts in suitable cases.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
			the Council control over resolving false claims for CTR.		
Housing related fraud	Council properties represent a significant asset to the Council. Individuals may attempt to gain council housing by providing false information to meet eligibility criteria or misrepresent their circumstances to increase their priority for a property. Tenants may sublet their property when they no longer need it in order to make a financial gain. Tenants who sublet or falsely obtain council properties remove a property from a person or family in true need of housing. It can also cost the Council directly if people are being housed in temporary accommodation and are waiting for a suitable property to become available.		The Council has strong controls to prevent false applications for housing. The housing department will engage with tenants regularly to ensure properties are not being misused. They also conduct identity and money laundering checks on applicants during the Right to Buy process.		CFT will 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 can face criminal prosecution and repossession of their council properties. The team will also support the Council in seeking Unlawful Profit Orders where council properties have been sublet for financial gain. CFT will develop an offer of support through verification exercises on Right to Buy applications that are likely to proceed. CFT will also seek opportunities to raise awareness with the public about mechanisms for reporting fraud, including through tenant newsletters. We also provide awareness training to staff on signs of fraud and

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	Housing fraud can also deprive the Council of these assets through false applications for Right to Buy.				actions Veritau can take to investigate concerns.
Procurement Fraud	Procurement fraud, by its nature, is difficult to detect but can result in large scale loss of public funds over long periods of time. The Competition and Markets Authority (CMA) estimates that having a cartel within a supply chain can raise prices by 30% or more. 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'. Contracts and supplier arrangements may have been subject to renewal and changes during the transfer of services under LGR. Increased procurement activity may present additional opportunities for fraud to enter the system.	High	The Council has established Contract Procedure Rules which ensure a competitive process is carried out (where required) through an e-tender system. The Procedure Rules will also be reviewed regularly. A team of procurement professionals provides guidance and advice to ensure procurement processes are carried out correctly. Contract monitoring will help detect and deter potential fraud.	Medium	Continued vigilance by relevant employees is key to identifying and tackling procurement fraud. CFT will provide training to raise awareness of fraud risks and investigate any suspicions of fraud referred. CFT will continue to develop links with the Competition and Markets Authority and other relevant bodies that can provide support to the Council. We will monitor the development of the CMA's cartel detection tool, and its potential relevance to the Council. There is regular procurement and contract management work undertaken by internal audit to help ensure processes are effective and being followed correctly.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
Theft of Assets	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 owns a large amount of portable, desirable physical assets such as IT equipment, vehicles, and tools that are at higher risk of theft. North Yorkshire Council took ownership of assets that were previously logged on separate asset registers. As services continue to restructure, it may be more difficult to identify instances of theft or loss during this period of change.	High	Specific registers of physical assets (eg capital items, property, and ICT equipment) will be consolidated and maintained. Asset tagging methods are also used to deter theft and aid recovery. The Council operates CCTV systems covering key premises and locations where high value items are stored. Entrance to council buildings is regulated and controlled via different access methods which helps manage access to areas where equipment is stored. The Council's whistleblowing arrangements provide an outlet for reporting concerns of theft.	Medium	Thefts will be reported to the police and Veritau. Instances of theft will be investigated by CFT where appropriate.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
Internal Frauds	Fraud committed by employees is a risk to all organisations. 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 related 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.	Medium	The Council has robust whistleblowing and anti-bribery policies in place. Campaigns are undertaken annually to promote these 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, eg 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 will include checks on payroll records for potential issues.	Medium	Veritau will liaise with senior management on internal fraud issues. Where internal fraud arises, IA and CFT will review the circumstances to determine if there are underlying control weaknesses that can be addressed. CFT provides training to HR officers on internal fraud issues. It will also provide training to all employees on whistleblowing and how to report concerns. An e-learning module on whistleblowing will be made available to all employees through the Council's learning platform. CFT will 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 will support any disciplinary action taken by the Council

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
					relating to internal fraud issues. Regular liaison meetings are held with HR to discuss ongoing investigations and arising concerns.
Recruitment Fraud	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 a risk 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.	Medium	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 will be taken from previous employers and there are processes to ensure qualifications provided are genuine.	Medium	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.
Treasury Management	Treasury Management involves the management and safeguarding of the Council's cash flow, its banking, and money market and capital market transactions. The	High	Treasury Management systems are subject to a range of internal controls, legislation, and codes of practice which protect council funds.	Low	IA will conduct periodic reviews of finance systems to ensure controls are strong and fit for purpose.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	impact of fraud in this area could be significant.		Only pre-approved employees can undertake transactions in this area, and they work within pre-set limits.		
Fraudulent Insurance Claims	The Council may receive exaggerated or fabricated insurance claims. If false claims progress unchecked this would negatively affect the Council in terms of the annual premiums it pays. Zurich previously reported a rise in false claims due to the "cost of living crisis". The Council carries a £5 million excess on all policies.	Medium	Claims against the Council are passed to insurers to investigate and decide on liability. The Council must be proven negligent before claims are paid.	Low	CFT continue to explore opportunities to help the Council defend illegitimate claims.
Grant Schemes	The Council takes on the responsibility for distributing 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	Medium	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.	Low	CFT and internal audit will support the development of fraud management plans, and associated controls, as appropriate. CFT can undertake investigation into cases of suspected fraud.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	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.				
Blue Badge & Parking Fraud	Blue Badge fraud carries low financial risk to the Council 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. People using a Blue Badge that does not belong to them and without the badge holder present are acting contrary to the law. They may also incorrectly be exempted from parking charges or pay reduced fees, in addition to being able to park in restricted	Low	Measures are in place to control the issue 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. The Council has a dedicated team that enforce parking regulations.	Low	CFT will deliver fraud awareness training to enforcement officers, and those involved in issuing permits. CFT has engaged with the service to plan proactive days of action with the Council's enforcement team. This will help 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.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation
	areas including on many double yellow lines. Other low level parking fraud is relatively common. For example, misuse of residential permits to avoid commercial parking charges.				
Cash handling	The use of cash has diminished with the majority of transactions now taking place online or by card payment. However, some services will continue to accept cash, although this tends to be of low value (e.g. leisure services, libraries, etc). A risk of theft is present, but the values of cash held are generally low, reducing any potential loss. There are also very few reported instances of cash loss/theft. The Council recognises the need to streamline cash handling/income processes, and to implement a consistent approach.	Low	Services have established cash handling and banking procedures in place, although they can be variable in nature. The Council's insurer provides a level of protection in cases of theft.	Low	Instances of loss/suspected theft can be reported to IA and CFT. Support will be provided to services, and cases may be referred to the police. Veritau will support services as required with advice on robust cash handling controls. Cash handling and income process will remain an area of interest as the Council reviews its income management systems.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Risk Mitigation

ANNEX 2: COUNTER FRAUD STRATEGY ACTION 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 counter fraud activity to the Audit Committee.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
1	Monitor developments to ensure the counter fraud framework remains compliant with best practice and relevant legislation and regulations.	Governing	Ongoing	Veritau	Policies and practices will be updated to reflect any changes, as necessary.
2	Develop links with services administering government funded grants to residents and local business to provide support with fraud management processes.	Acknowledging	March 2025	Veritau / relevant service areas	Veritau can support services to develop fraud management plans where they are a requirement of central government grant funding.
3	Collate and submit data to the Public Sector Fraud Authority for the 2024/25 National Fraud Initiative the exercise.	Preventing	January 2025	Veritau / relevant service areas	Veritau will work with services to ensure that suitable privacy notices are in place, and to collect relevant

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
					data required for the mandatory exercise. Results from the exercise will be released in 2025.
4	Establish a framework to undertake data analysis and matching projects to detect fraud using council data.	Preventing	July 2024	Veritau	Veritau has developed expertise in preparing for and conducting data matching projects. Relevant privacy notices will continue to be reviewed as necessary during the development of specific projects.
5	Explore local data matching using council tax data to detect fraud and error.	Pursuing	December 2024	Veritau / relevant service areas	New opportunities to undertake data matching have become available as a result of former district and borough council services being transferred to the new Council.
6	Complete the review of 2022/23 National Fraud Initiative (NFI) outcomes for all the former North Yorkshire councils.	Pursuing	July 2024	Veritau	The collection and submission of data to NFI took place pre-LGR, however, additional matches have continued to be released as late as January 2024. These new matches incorporate new external data sets.

Ref	Action Required	Theme	Target Date	Responsibility	Notes / Further Action Required
7	Conduct a review of Council arrangements to prevent and detect fraud in high-risk areas, as identified in the fraud risk assessment.	Protecting	December 2024	Veritau / Relevant Service Areas	This is an ongoing project with relevant services to ensure robust counter fraud measures are in place. Veritau will work with teams as they restructure to build in best practice.
8	Engage with the Public Sector Fraud Authority (PSFA); identify recommended actions and implement as required.	Protecting	March 2025	Veritau	The PSFA will reach out to local government counter fraud teams to discuss how it can provide support.

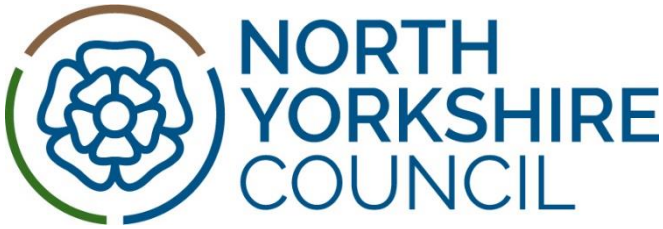
Completed activities:

Ref	Action Required	Theme	Responsibility	Update
1	Prepare a counter fraud strategy which acknowledges fraud risks facing the Council and sets overall counter fraud aims. The strategy should set out actions required for developing counter fraud arrangements.	Governing	Director of Resources / Veritau	A counter fraud strategy was presented to the audit committee in March 2023. It is subject to annual review and updated to provide continual development of counter fraud processes.
2	Develop the Council's counter fraud policy framework and	Governing	Audit Committee / Veritau	The Council approved the counter fraud framework in February 2023. These are

Ref	Action Required	Theme	Responsibility	Update
	ensure that robust policies are in place.			reviewed annually as part of the annual counter fraud framework refresh.
3	Create and review a new Fraud Risk Assessment which evaluates the threat of fraud to the new authority within specific service areas.	Acknowledging	Audit Committee / Veritau	A fraud risk assessment was presented to the Audit Committee in March 2023. It is subject to annual review.
4	Approve an annual counter fraud workplan with sufficient resources to enable counter fraud work to be undertaken.	Acknowledging	Audit Committee / Veritau	A counter fraud workplan was approved by the Audit Committee in March 2023. It detailed areas of work to be undertaken by the counter fraud team.
5	Raise awareness of the counter fraud policy framework amongst all council employees. Counter fraud guidance will be disseminated to employees throughout the year as part of targeted campaigns.	Preventing	Veritau / Communications Department	Campaigns to raise awareness of fraud risks took place throughout 2023/24. The team also continued to develop relationship with service areas and staff joining the new authority. An e-learning package on whistleblowing is still in development.
6	Develop processes with the Legal Department to ensure that when fraud against the Council is detected that legal and recovery action can be taken swiftly.	Pursuing	Veritau / Legal Department	Contacts in the Legal Department have been established to enable suitable cases to be pursued through legal action.
7	Raise awareness of the threat of fraud to employees and the public. Publicise routes to report	Protecting	Veritau / Communications Department	The Council's intranet and website have been updated to ensure that methods for reporting concerns are available to offices and the public.

Ref	Action Required	Theme	Responsibility	Update
	fraud for employees and the public.			Future awareness campaigns will further promote the counter fraud team's contact details.

ANNEX 3: Anti-Money Laundering & Terrorist Financing Policy



ANTI-MONEY LAUNDERING & TERRORIST FINANCING POLICY

Index

1 Introduction

1.1 Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes illegally obtained money and converts it into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' or ‘launders’ them. Money or assets gained as a result of crime can ultimately be used to fund terrorism.

1.2 The Council undertakes transactions and delivers services which can fall under UK anti-money laundering legislation, which includes, but is not limited to:

- the Terrorism Act 2000
- the Proceeds of Crime Act 2002
- the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on Payer) Regulations 2017
- the Criminal Finance Act 2017
- the Money Laundering Regulations.

1.3 Anti-money laundering legislation has been updated regularly by the Government in recent years. While the legislation does not specifically target local authorities, some types of council activity can fall under the requirements of the law. It is therefore important for councils to assess money laundering risks and put sufficient controls in place to prevent their organisation from being used for money laundering.

1.4 All employees should be aware of the threat of money laundering, the need to report suspicions of money laundering, and the consequences of not following the principles and processes set out in this Policy. A list of key risk factors for employees to be aware of is included in **Appendix A**.

1.5 The Council has a Money Laundering Reporting Officer (MLRO) who is responsible for raising awareness of the issue within the Council and reporting appropriate concerns to the National Crime Agency (NCA) when they arise. The MLRO is the Head of Internal Audit and they can be contacted on 01904 552940. If the MLRO is unavailable the Council has a Deputy MLRO. The Deputy MLRO is the Deputy Head of Internal and they can be contacted on 01904 552936.

1.6 Some types of work undertaken by the Council may fall under the definition of regulated activity in the legislation (see paragraph 2.3). There are more specific detailed requirements for employees working in these areas and guidance is set out in **Appendix B**. The Council has a Chief Money Laundering Compliance Officer (CMLCO) who has oversight of all Council

anti-money laundering arrangements and is specifically responsible for overseeing regulated activity. The CMLCO is the Council's Assistant Chief Executive (Legal and Governance) and can be contacted on 01609-532173.

1.7 This Policy contains a form that should be submitted to the MLRO when money laundering concerns arise (**Appendix D**). This form may be used by any employee to report a suspected issue.

2 Scope of the Policy

2.1 This Policy applies to all employees of the Council. It aims to maintain the high standards of conduct expected by the Council by preventing criminal activity through money laundering.

2.2 To ensure the Council complies with its legal obligations, all employees must be aware of the content of this Policy. Failure by an employee to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them and could constitute a criminal offence. Any disciplinary action will be dealt with in accordance with the Council's disciplinary policies and procedures.

2.3 Money laundering legislation sets out some activities that are subject to specific requirements. These are areas that are at greater risk of being targeted by criminals for money laundering (for example certain financial and legal services, and those dealing in property sales and acquisitions). These areas, amongst others, are known as regulated activities. Some work undertaken by the Council may fall under the definition of regulated activity. This is generally in higher risk areas, where the Council carries out work on behalf of other organisations such as:

- accounting and treasury management services
- legal and company related work
- property services
- payroll services.

2.4 Employees undertaking work that could be considered regulated activity need to be aware of the more detailed requirements set out in **Appendix B**. If anyone is unsure of whether their work falls into this category, further advice can be sought from the CMLCO, the MLRO, or the Deputy MLRO.

3 What is money laundering?

3.1 Money laundering is a general term for any method of disguising the origin of assets obtained through crime. Assets including money and property are

described as “criminal property” in legislation. Criminal property may be the proceeds of any criminal activity including terrorism, drugs trafficking, corruption, tax evasion and theft. The purpose of money laundering is to hide the origin of the criminal property so that it appears to have come from a legitimate source. Unfortunately, no organisation is safe from the threat of money laundering, particularly where it is receiving funds from sources where the identity of the payer is unclear. There is therefore a real risk that the Council may be targeted by criminals seeking to launder the proceeds of crime.

3.2 It is possible that the proceeds of crime may be received from individuals or organisations who do not know that the assets involved originated from criminal activity. However, this could still be an offence under the legislation. It is no defence for a payer or recipient of funds to claim that they did not know that they were committing an offence if they should have been aware of the origin of assets. All employees dealing with the receipt of money or having contact with third parties from whom money may be received need to be aware of the possibility of money laundering taking place. This includes a wide range of service areas. As an example, an area where money laundering may need to be considered includes cases where the Council takes possession of money belonging to a customer, for safekeeping, under its statutory care duties.

3.3 Money laundering offences include:

- concealing, disguising, converting, transferring criminal property or removing it from the UK;

- entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;

- acquiring, using or possessing criminal property;

  - an attempt, conspiracy or incitement to commit such an offence; or
  - aiding, abetting, counselling or procuring such an offence

- becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property.

3.4 The broad definition of money laundering means that the legislation applies to a very wide range of everyday activities within the Council. This means that any employee (irrespective of what sort of work they do at the Council) could encounter money laundering and be required to report it.

3.5 Whilst the risk to the Council of contravening the legislation is relatively low, **it is important that all employees are familiar with their responsibilities. Serious criminal sanctions may be imposed for breaches of the legislation**. Any person found guilty of a money laundering offence is liable to imprisonment (maximum sentence of 14 years), a fine or both. However, an offence is not committed if any suspected money laundering activity is reported to the Council's MLRO and, where necessary, official permission is obtained to continue with a transaction[1].

Potential signs of money laundering

3.6 It is impossible to give a definitive list of how to spot potential money laundering or how to decide whether to make a report to the MLRO. The following are examples of major risk factors which may, either alone or cumulatively with other factors, suggest the possibility of money laundering activity. A more exhaustive list is contained in **Appendix A**.

<u>General factors</u>

- Payment of a substantial sum in cash (over £10,000).
- A secretive client or customer: for example, they refuse to provide requested information without a reasonable explanation, don't want to provide identification, or they supply unsatisfactory identification.
- Concerns about the honesty, integrity, identity, or location of a client or customer.
- The cancellation or reversal of an earlier transaction (where the client or customer is likely to request the return of previously deposited monies).
- Any other activity which by its nature is likely to be related to money laundering, tax evasion, or terrorist financing.

<u>Property transactions</u>

- A cash buyer.
- Funds received for deposits or prior to completion from an unexpected source, or where instructions are given for settlement funds to be paid to an unexpected destination.
- No clear explanation as to the source of funds along with a lack of clarity as to how the client would be in a position to finance the purchase.

3.7 Property transactions are a higher risk for the Council. Tenants have the ability to purchase their council property under the Right to Buy scheme and the Council may choose to sell land to a developer or other third party. In

[1] Where money laundering is suspected the MLRO will report this to the National Crime Agency (NCA). The NCA may give permission to proceed with a suspect transaction – for example to avoid those involved becoming alert to suspicions having been raised.

any sale of property or land, checks need to be made to establish the source of funding and ensure that money laundering offences are not occurring. In addition, if a buyer has no legal representation, then client identification must be sought before business is conducted. If a buyer has legal representation, then that representative is responsible for undertaking the required identification.

3.8 Facts which tend to suggest that something odd is happening may be sufficient for a reasonable suspicion of money laundering to arise. Be on the look-out for anything out of the ordinary. If something seems unusual, stop and question it. If anyone is unsure of any transaction then further advice should be sought from the MLRO.

4 How to report concerns

4.1 Where an employee knows or suspects that money laundering activity is taking place (or has already) they must disclose this as soon as possible to the MLRO.

4.2 The disclosure should be made to the MLRO using the form attached in **Appendix D**. The report must include as much detail as possible. It should contain all available information to help the MLRO decide whether there are reasonable grounds to show knowledge or suspicion of money laundering. The MLRO will use this information to prepare a report to the National Crime Agency (NCA) if needed. Copies of any relevant supporting documentation should be sent to the MLRO along with the form.

4.3 Once an issue has been reported to the MLRO employees must follow any directions they may give. Employees must not make any further enquiries into issues themselves. If an investigation is needed it will be carried out by the NCA. All employees are required to cooperate with the MLRO and the NCA (or other external authorities such as the police) during any subsequent money laundering investigation.

4.4 Employees must at no time and under no circumstances voice any suspicions to people who they suspect of money laundering (or to anyone other than a line manager (unless possibly implicated) or the MLRO). Doing so could result in a criminal offence (“tipping off”) being committed.

4.5 No references should be made on any Council files or systems that a report has been made to the MLRO. If a client exercised their right to see a file (for example through a subject access request under data protection legislation) then a note could tip them off to a report having been made. The MLRO will keep appropriate records in a confidential manner.

4.6 The MLRO will advise the employee of the timescales in which they will respond to the report. They may wish to discuss the report with the employee and gather further information.

5 Responsibilities

5.1 The Council has a responsibility to prevent money laundering from occurring within the organisation whether that be in the course of day-to-day business or in work that is considered to be regulated activity. It is the responsibility of every employee to be vigilant and report any concerns of money laundering.

5.2 The Chief Money Laundering Compliance Officer has overall responsibility for monitoring anti-money laundering policy, regulations and procedures. The CMLCO will appoint a MLRO and deputy MLRO. The CMLCO will ensure appropriate procedures for regulated activity are in place and obtain approval of the policy from the Audit Committee. The CMLCO will also ensure that directorate departments undertaking regulated activity have appropriate training and risk assessments in place.

5.3 The Money Laundering Reporting Officer (and deputy) have responsibility for receiving reports of suspicions of money laundering, considering those reports and, where appropriate, submitting reports to the National Crime Agency (see **Appendix C**). The MLRO will convey instructions from the NCA eg, to halt or proceed with a transaction. They will also maintain records of all reports on behalf of the Council.

5.4 The Head of Internal Audit will ensure there is an independent audit function to evaluate and make recommendations about the policies, controls, and compliance in relation to anti-money laundering. Veritau will regularly promote awareness of the Anti-Money Laundering Policy to all employees.

6 Policy review

6.1 This Policy will be reviewed every three years or as soon as any significant changes to anti-money laundering legislation, regulations, or guidance occurs.

POLICY APPROVED 22 02 2023

Appendix A

Signs of potential money laundering

It is not possible to give a definitive list of ways in which to identify money laundering or how to decide whether to make a report to the Money Laundering Reporting Officer. However, the following are types of risk factors which may, either alone or cumulatively, suggest possible money laundering activity.

Concerns about transactions

- Payment of a substantial sum in cash (over £10,000).
- Complex or unusually large transactions or systems.
- The source or destination of funds differs from the original details given by the client.
- Movement of funds overseas, particularly to a higher risk country or a tax haven[2].
- Where, without reasonable explanation, the size, nature and frequency of transactions or instructions (or the size, location, or type of a client) is out of line with normal expectations. For example, the use of cash where other means of payment are normal.
- Unusual patterns of transactions which have no apparent economic, efficient, or visible lawful purpose.
- Transactions at substantially above or below fair market rates.

Other activity of concern

- Transactions that don't seem logical from a third party's perspective. For example, receipt of unexpected funds, or unnecessary routing of transactions through another party's accounts.
- Overpayments by a client (or money given on account). Care needs to be taken, especially with requests for refunds. For example, if a significant overpayment is made which results in repayment being needed – this should be properly investigated and authorised before payment.
- Helping to set up trusts or company structures, which could be used to obscure ownership of property.
- The cancellation or reversal of an earlier transaction (where the client is likely to request the return of previously deposited monies).

[2] See Financial Action Task Force list of high risk countries, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

- Requests for release of client account details other than in the normal course of business.
- Companies and trusts:
  - Bodies with a complicated ownership structure, which could conceal underlying beneficiaries.
  - Extensive use of corporate structures and trusts in circumstances where the client's needs are inconsistent with the use of such structures.
- Any other activity which by its nature is likely to be related to money laundering, tax evasion, or terrorist financing.

<u>Concerns about a client</u>

- A secretive client: for example, they refuse to provide requested information without a reasonable explanation, don't want to provide identification, or they supply unsatisfactory identification.
- A client you have not met.
- Difficulties in establishing the identity of the client.
- Concerns about the honesty, integrity, identity, or location of a client. For example, a client who is not present in the area and where there is no good reason why they would have dealings with the Council; or information reveals that a client is linked with criminality.
- Involvement of an unconnected third party without logical reason or explanation.
- Absence of an obvious legitimate source of the funds.
- Poor business records or internal accounting controls.
- Individuals or companies that are insolvent yet have funds.
- A previous transaction for the same client which has been, or should have been, reported to the MLRO.

<u>Concerns about property transactions</u>

- A cash buyer.
- Sudden change of buyer.
- The client's financial profile does not fit.
- Unusual property investment transactions if there is no apparent investment purpose or rationale.
- Instructions to receive and pay out money where there is no linked substantive property transaction involved (surrogate banking).

- Funds received for deposits or prior to completion from an unexpected source, or where instructions are given for settlement funds to be paid to an unexpected destination.
- No clear explanation as to the source of funds along with a lack of clarity as to how the client would be in a position to finance the purchase.
- Money comes from an unexpected source.

Appendix B

Guidance for officers undertaking Regulated Activity

1 Introduction

1.1 Money laundering legislation and guidance defines a number of commercial activities that are subject to specific anti-money laundering requirements. These are areas that are at greater risk of being targeted by criminals for laundering money (for example financial services, and those dealing in property sales and acquisitions). These areas are known as regulated activities. Further details on regulated activities are set out in paragraph 2.1 below.

1.2 It is clear from the money laundering regulations and guidance from supervisory bodies, that councils and their in-house lawyers and accountants are not intended to be caught within the definition of regulated activities when carrying out normal council business. For example, because they are not acting as external or independent advisors for their council.

1.3 However, with the growth in external commercial work being undertaken by councils in recent years, there are a growing number of circumstances where lawyers, accountants and others working for councils could be caught within the scope of the legislation. For example, where employees undertake work for organisations other than the Council under contract. Such external work may be classed as being undertaken “by way of business” and could bring those activities within the regulated sector. Guidance issued by supervisory bodies states that where there is uncertainty over the application of the regulations, the broadest possible approach to compliance with the regulations should be undertaken.

2 Definition of regulated activity

2.1 Regulated activity is defined as:

- material aid or assistance or advice in connection with the tax affairs of another person by a practice or sole practitioner (whether provided directly or through a third party);
- the provision to other persons of accountancy services by a firm or sole practitioner who by way of business provides such services to other persons;
- legal or notarial services involving the participation in financial or real property transactions concerning:
  - the buying and selling of real property or business entities;
  - the managing of client money, securities, or other assets;

- the opening or management of bank, savings, or securities accounts;
- the organisation of contributions necessary for the creation, operation, or management of companies;
- the creation, operation or management of trusts, companies, or similar structures;

by a firm or sole practitioner who by way of business provides legal or notarial services to other persons (a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for a client in relation to it);

- forming companies or other legal persons;
- acting, or arranging for another person to act:
  - as a director or secretary of a company;
  - as a partner of a partnership;
  - in a similar position in relation to other legal persons;
- providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;
- acting, or arranging for another person to act, as:
  - a trustee of an express trust or similar legal arrangement;
  - a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

2.2 In general, the areas where the Council is carrying out activities that may fall within the definition of regulated activities relate to accounting services, treasury management, payroll services and legal services in relation to financial, company or property transactions. However, this will only be the case if the work is carried out for external clients. Work undertaken on behalf of Council services (including traded services where there is no separate legal entity involved) would not fall under the scope of regulated activity.

3 Responsibilities

3.1 All officers undertaking regulated activity within the Council should be aware of the potential to become involved in money laundering and terrorist financing. Members of staff may be liable to criminal charges if they fail to report their concerns. These criminal charges relate to someone's actions (or lack of them) where money laundering activity is suspected. A criminal offence could be committed if an employee:

- knows or suspects (or has reasonable grounds to do so) that another person is engaged in money laundering;

- can identify a money launderer or the whereabouts of laundered property (or they believe, or it is reasonable to expect them to believe, that information held would assist in identifying a money launderer or the whereabouts of laundered property); and
- does not disclose information held to the MLRO as soon as practicable.

3.2 As set out in paragraph 1.7 of the Policy, the Council's Assistant Chief Executive (Legal and Governance) is the senior officer within the Council responsible for ensuring compliance with anti-money laundering requirements (the Chief Money Laundering Compliance Officer – CMLCO). The CMLCO is responsible for ensuring that the Council has appropriate policy, procedures, and controls in place to manage money laundering risks.

3.2 In relation to regulated activities, the CMLCO will:

- ensure there are arrangements in place within the Council for conducting money laundering and terrorist financing, and tax evasion risk assessments;
- establish appropriate systems, policies, controls and procedures to address identified risks of money laundering – and ensure that the arrangements have been approved by the relevant body or bodies;
- ensure arrangements are in place to screen relevant employees, including an assessment of their skills, knowledge, and expertise to carry out their functions effectively and of their conduct and integrity;
- support and facilitate independent internal audit of money laundering arrangements;
- ensure training on anti-money laundering is provided to relevant employees.

4 Due diligence

4.1 Where the Council is carrying out regulated activities (see 2.1 above), and any of the following apply, then customer due diligence measures must be applied.

- The Council forms a business relationship with a client (which is expected to have an element of duration) – this includes the formation of a company;
- The Council undertakes an occasional transaction amounting to 15,000 Euros (approximately £13,000) or more whether carried out in a single operation or several linked ones;
- The Council suspects money laundering or terrorist financing;
- The Council suspects tax evasion from the UK or a foreign country;

- The Council doubts the veracity or adequacy of information previously obtained for the purposes of client identification or verification.

4.2 Information on customer due diligence procedures is set out in 4.5 below. If due diligence is needed, it must reflect the corporate regulated activity AML risk assessment, and the assessed level of risk in the individual case – taking account of factors such as:

- the purpose of an account, transaction, or business relationship;
- the level of assets to be deposited/size of the transactions undertaken by the client;
- the regularity and duration of the business relationship.

4.3 The customer due diligence procedure set out below must be followed before the establishment of the relationship or carrying out of the transaction (or during, provided that verification is completed as soon as practicable after contact is first established and this is necessary not to interrupt the conduct of business and there is little risk of money laundering).

4.4 The Council is not required to undertake the customer due diligence checks set out below if its customer is another public authority, unless it suspects money laundering or terrorist funding.

4.5 Applying customer due diligence means:

- identifying the client (unless their identity is already known and has been verified) and verifying the client's identity (unless already verified) on the basis of documents or information obtained from a reliable and independent source and assessing (and where appropriate obtaining information on) the purpose and intended nature of the business relationship/occasional transaction:
    - Where the client is acting or appears to be acting for someone else, reasonable steps must also be taken to establish the identity of that other person (although this is unlikely to be relevant to the Council).

- where the client is beneficially owned by another person, identifying the beneficial owner and taking reasonable steps to verify their identity so that the Council can be satisfied that it knows who the beneficial owner is. In the case of a beneficial owner being a legal person, trust, company, foundation or similar legal arrangement, officers must take reasonable measures to understand the ownership and control structure of it. Reliance cannot solely be placed on the statutory register of people with significant control:
    - In terms of clients for whom the Council provides regulated services, "beneficial owner" would include bodies corporate (eg our public

authority clients) and any individual who exercises control over the management of the body (eg Chief Executive Officer).

UNLESS the client is a company which is listed on a regulated market, in which case the above steps are not required.

- where the client is a body corporate:
  - obtaining and verifying its name, company/registration number, registered office address (and if different, its principal place of business address);
  - taking reasonable measures to determine and verify (UNLESS the client is a company which is listed on a regulated market, in which case the steps below are not required):
    - the law to which it is subject;
    - its constitution (whether set out in its articles of association or other governing documents);
    - the full names of the board of directors (or if there is no board, the members of the equivalent management body) and the senior persons responsible for the body's operations;
  - where the client is a body corporate and the beneficial owner cannot be identified or where the individual identified as the beneficial owner cannot be verified as such, despite exhausting all possible means, officers must take reasonable measures to identify and verify the identity of the senior person responsible for managing the body. In these circumstances officers must keep written records of all steps taken to identify the beneficial owner, all action taken, and difficulties encountered.

- where another person purports to act on the client's behalf, officers must verify that they are authorised to so act, identify them and verify their identity from a reliable source, independent of both parties;

- assessing and where appropriate obtaining information on the purpose and intended nature of the business relationship or occasional transaction.

4.6 Where customer due diligence is required, employees in the relevant team must obtain and verify satisfactory evidence of the identity of the prospective client, and full details of the purpose and intended nature of the relationship/transaction, as soon as practicable after instructions are received and before the establishment of the business relationship or carrying out of the occasional transaction. However, the legislation does allow organisations to vary customer due diligence and monitoring according to the risk of money laundering or terrorist financing which

depends on the type of customer, business relationship, product or transaction. This recognises that not all clients present the same risk. Satisfactory evidence of identity is that which:

- is capable of establishing, to the satisfaction of the person receiving it, that the client is who they claim to be, and
- does in fact do so.

4.7 In the Council, details of proposed transactions are usually, as a matter of good case management practice, recorded in writing in any event and proposed ongoing business relationships are usually the subject of Terms of Business Letters, Service Level Agreements or other written record which will record the necessary details.

4.8 Customer due diligence measures must also be applied at other times to existing clients on a risk-based approach and when the Council becomes aware that such existing clients' circumstances have changed, relevant to the risk assessment, taking into account:

- any indication that the identity of the client/its beneficial owner, has changed;
- any transactions which are not reasonably consistent with knowledge of the client;
- any change in the purpose or intended nature of the Council's relationship with the client;
- any other matter which might affect officers' assessment of the money laundering or terrorist financing risk in relation to the client.

Opportunities to do this will differ, however one option is to review these matters as part of the ongoing monitoring of the business arrangements, as is usually provided for in the Terms of Business Letter, Service Level Agreement or other written record.

4.9 Council staff conducting regulated business need to be able to demonstrate that they know their clients and the rationale behind particular instructions and transactions.

4.10 Once instructions to provide regulated business have been received, and it has been established that any of the conditions in paragraph 4.1 above apply, or it is otherwise an appropriate time to apply due diligence measures to an existing client, evidence of identity and its verification and information about the nature of the particular work should be obtained or checked.

4.11 Most of the external clients to whom the Council provides potentially regulated business services are UK public authorities and consequently, as above, proportionate, simplified customer due diligence measures should

be undertaken. Full details about the nature of the proposed transaction should be recorded on the client file or suitable central record (kept by the relevant team), and the identity of such external clients should continue to be checked, along with other external clients (eg designated public bodies). Officers should also then obtain the appropriate additional evidence: appropriate additional evidence of identity will be written instructions on the organisation's official letterhead at the outset of the matter or an email from the organisation's e-communication system. Such correspondence should then be placed on the relevant client file or central record along with a prominent note explaining which correspondence constitutes the evidence and where it is located.

4.12 In some circumstances, however, **enhanced due diligence** (eg obtaining additional evidence of identity or source of funds to be used in the relationship/transaction) and enhanced ongoing monitoring must be carried out, for example where:

- there is an identified high risk of money laundering. Risk factors to be considered include:
  - the type and nature of customers;
  - the countries or geographic areas in which a business operates;
  - where customers are based;
  - customers' behaviour;
  - how customers come to do business with the Council;
  - the products or services to be provided;
  - the nature of transactions;
  - delivery channels and payment processes (eg cash over the counter, cheques, electronic transfers or wire transfers);
  - where customers' funds come from or go to.

- the client is a "politically exposed person" (an individual who at any time in the preceding year has held a prominent public function in the UK, and EU or international institution/body, a family member or known close associate). This is unlikely to ever be relevant to the Council but the provision must be included in local procedures;

- the business relationship or transaction is with a person established in a high-risk third country;

- the client has provided false/stolen identification evidence and the Council wishes to continue to deal with them;

- the transaction is complex or unusually large, or there is an unusual pattern of transactions, or it has no apparent economic or legal purpose;

- the nature of the situation presents a higher risk of money laundering or terrorist financing.

4.13 Enhanced due diligence measures *must* include

- examining the background and purpose of the transaction;
- increasing the degree and nature of the monitoring of the business relationship to determine whether the transaction appears suspicious.

4.14 With instructions from new clients, or further instructions from a client not well known to the Council, officers may wish to seek additional evidence of the identity of key individuals in the organisation and of the organisation itself, for example:

- checking the organisation's website to confirm the identity of key personnel, its business address and any other details;
- conducting an on-line search via Companies House to confirm the nature and business of the client (including any registered office and registration number) and to confirm the identities of any directors;
- where the client is a company, appropriate evidence might be company formation documents or a business rate bill;
- attending the client at their business address
- asking the key contact officer and/ or any individual who exercises control over the management of the body (eg the Chief Executive Officer) to provide evidence of their personal identity and position within the organisation, for example:
  - passport;
  - photocard driving licence;
  - birth certificate;
  - medical card;
  - utility bill;
  - bank/building society statement (but not if used to prove address and no older than 3 months);
  - National Insurance number;
  - signed, written confirmation from their Head of Service or Chair of the relevant organisation that such person works for the organisation.

If such additional evidence is obtained, then copies should be retained on the relevant client file or a suitable central record.

4.15 Relevant persons are still able to rely on the customer due diligence carried out by a third party if that third party is either subject to the Money Laundering Regulations 2017 or an equivalent regime. However, the conditions for doing so are prescriptive. The third party must effectively provide the customer due diligence information it has obtained and enter into a written agreement under which it agrees to immediately provide copies of all customer due diligence documentation in respect of the customer and/or its beneficial owner.

4.16 In all cases, the due diligence evidence should be retained for at least five years from the end of the business relationship or transaction(s). This could be used in any future money laundering investigation. Such personal data should be recorded and stored carefully and in compliance with the Council's information governance requirements.

4.17 If satisfactory evidence of identity is not obtained and verified at the outset of the matter then generally the business relationship or one off transaction(s) cannot proceed any further and any existing business relationship with that client must be terminated (however there are some exceptions).

5 Ongoing monitoring and record keeping

5.1 Each team conducting potentially regulated business must monitor, on an ongoing basis, their business relationships in terms of scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with their knowledge of the client, its business and risk profile; and reviewing existing records and keeping due diligence information up-to-date. Particular scrutiny should be given to:

- complex or unusually large transactions;
- unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- any other activity particularly likely by its nature to be related to money laundering, terrorist financing, or tax evasion.

5.2 Teams should also maintain records of:

- client identification/verification evidence obtained (or references to it), and
- details of all regulated business transactions carried out for clients

for at least five years from the end of the transaction/relationship. This is so that they may be used as evidence in any subsequent investigation by the authorities into money laundering.

5.3 The precise nature of the records is not prescribed by law however they must be capable of providing an audit trail during any subsequent investigation, for example distinguishing the client and the relevant transaction and recording the source of, and in what form, any funds were received or paid. In practice, Council teams will be routinely making records of work carried out for clients in the course of normal business and these should suffice in this regard.

Appendix C

Money Laundering Report Officer Disclosure Process

1.1 It is important that the appointed MLRO (and deputy) are aware of the National Crime Agency's (NCA) processes for submitting suspicious activity reports (SARs). SARs should be submitted via the SAR Online platform. On appointment the MLRO (and deputy) should create an account on SAR Online promptly[1].

1.2 Upon receipt of a disclosure report, the MLRO must note the date of receipt on their section of the AML Reporting Form (**Appendix D**) and acknowledge receipt of it.

1.3 The MLRO should consider the report and any other available internal information they think relevant, for example:

- reviewing other transaction patterns and volumes;
- the length of any business relationship involved;
- the number of any one-off transactions and linked one-off transactions;
- any due diligence information held;

and undertake such other reasonable enquiries they think appropriate in order to ensure that all available information is taken into account in deciding whether a report to NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved).

1.4 The MLRO should consider NCA guidance on how and when to submit a SAR[2] in evaluating the AML Reporting Form and any other relevant information. The MLRO should make a timely determination as to whether:

- there is actual or suspected money laundering taking place;
- there are reasonable grounds to know or suspect that is the case;
- the identity of the money launderer or the whereabouts of the property involved is known, or they could be identified, or the information may assist in such identification;
- whether they should seek consent from NCA for a particular transaction to proceed.

1.5 The MLRO should also consider whether the report indicates suspicions of other crimes that should be reported to the Police, eg a vulnerable person

[1] See NCA SAR Online User Guidance.
[2] See NCA Guidance on submitting better quality Suspicious Activity Reports.

or child at immediate risk of harm, supply of firearms, or modern slavery/human trafficking.

1.6 If the MLRO concludes that the matter should be reported then they should do that as soon as practicable via NCA's Online SAR Portal, unless there is a reasonable excuse for non-disclosure to NCA (for example, if the form has been completed by a lawyer and they wish to claim legal professional privilege[3] for not disclosing the information).

1.7 Where the MLRO suspects money laundering but has a reasonable excuse for non-disclosure, then they must note this on the AML Reporting Form; they can then immediately give their consent for any ongoing or imminent transactions to proceed.

1.8 Where consent is required from NCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from NCA.

1.9 If the MLRO concludes that there are no reasonable grounds to suspect money laundering then they should record this on the AML Reporting Form and give their consent for any ongoing or imminent transaction(s) to proceed.

1.10 All disclosure reports referred to the MLRO, reports made to NCA, and any subsequent communications from the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

[3] In cases where legal professional privilege may apply, the MLRO must liaise with the legal adviser to decide whether there is a reasonable excuse for not reporting the matter to NCA.

Appendix D

Money Laundering Reporting Officer
Suspicious Activity Reporting (SAR) Form
Confidential

To: Money Laundering Reporting Officer, North Yorkshire Council

From: Email:
Job Title: Department:

Note – if no response to a required field, put 'Unknown'.

Main Subject

Is the main subject a person or a legal entity eg a Company?	

Surname		Forename(s)	
Title		Gender	
Date of Birth		Occupation	
Address			
Address Type	Accommodation Address, Foreign Address, Home Address, Other, Previous, Registered Office, Trading Address, UK Address, Unknown		

Current Address?	Yes, No, Unknown

Company Name		Companies House Number	
Company Type		Name of Officer(s) representing Company	
Address			
Address Type	Accommodation Address, Foreign Address, Home Address, Other, Previous, Registered Office, Trading Address, UK Address, Unknown		
Current Address?	Yes, No, Unknown		

Additional Information - fill in any of these, if known

Email address	
Website address	
Car registration	
Mobile number (home or work)	
NHS number	
National Insurance number	
Passport No	
Phone number (home or work)	
Tax Ref number	

Associated Subject – any joint account holders, on the account to be used for the transaction

Subject Status	Victim, Suspect, Unknown		
Surname		Forename(s)	
Title		Gender	
Date of Birth		Occupation	
Address			
Address Type	Accommodation Address, Foreign Address, Home Address, Other, Previous, Registered Office, Trading Address, UK Address, Unknown		
Current Address?	Yes, No, Unknown		

Details of Transaction

Date		Amount	
Credit/Debit		Currency	
Property			
Type	Cash, Property Transaction, Cash/Cheque, Cheque, Credit Card, Currency, Draft, Electronic Transfer, Loan, Mixed, Mortgage, On-Line, Other, Policy, Purchase, Share Transfer, Smart Card, Travellers Cheques, Unknown, Wire Transfer		

Details of the subject's account

Account Holder		Account Number	
Institution Name		Sort Code	
Date Opened		Date Closed	
Account Balance		Balance Date	
Turnover Credit		Turnover Debit	
Turnover Period			

Reason for Suspicion

Please provide as much information as possible, including,

(i) the information or other matter which gives the grounds for your knowledge, suspicion or belief;

(ii) a description of the property that you know, suspect or believe is criminal property; and

(iii) a description of the prohibited act for which you seek a defence (by prohibited act, we mean the proposed activity that you are seeking a defence to undertake).

Enquiries already undertaken

Please answer the questions below and provide as much information as possible, including,

(i) Is the report about an ongoing transaction? What is the current state of the transaction?

(ii) Has the matter been investigated? By whom and what were the findings?

(iii) Have you discussed your suspicions with anyone else? If yes then to whom and why was this necessary?

(iv) Have you consulted any supervisory body guidance eg the Law Society?

(v) Do you feel you have a reasonable explanation for not disclosing this matter to NCA (eg you are a lawyer and wish to claim legal professional privilege?)

To be completed by MLRO

Date report received	Click or tap to enter a date.			
Date receipt of report acknowledged	Click or tap to enter a date.			
Are there reasonable grounds for suspecting money laundering activity?	Yes	☐	No	☐

Do you know the identity of the alleged money launderer, or whereabouts of the property concerned?	Yes	☐	No	☐
Do the circumstances described above meet the NCA's threshold to submit a Suspicious Activity Report (SAR) to obtain a Defence Against Money Laundering (DAML)?	Yes	☐	No	☐
If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to NCA, or it would not meet their threshold, please set out the reasons for non-disclosure				
Date SAR is sent to the NCA (if applicable)	Click or tap to enter a date.			

Signed ……..…… Date: Click or tap to enter a date.

Signed (MLRO)…….. Date: Click or tap to enter a date.

THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS

Appendix 2

COUNTER FRAUD PLAN 2024/25

Date: 18 March 2024

Daniel Clubb
Assistant Director – Counter Fraud

Max Thomas
Head of Internal Audit

INTRODUCTION

1 Veritau undertakes counter fraud work on behalf of North Yorkshire Council. This document summarises the agreed areas of counter fraud work for 2024/25.

2 A total of 1,100 days has been allocated to counter fraud work in 2024/25. 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 Strategy Action Plan.

3 A high-level summary of the areas for counter fraud work in 2024/25 is shown in the table below.

2024/25 COUNTER FRAUD SUMMARY

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: • 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 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.