NORTH YORKSHIRE COUNCIL

AUDIT COMMITTEE

12 DECEMBER 2022

COUNTER FRAUD POLICY FRAMEWORK

Report of the Head of Internal Audit

1.0 PURPOSE OF THE REPORT

1.1 To seek member approval for the counter fraud policy framework for the new North Yorkshire Council.

.

2.0 BACKGROUND

2.1 Fraud is a serious risk to the public sector in the UK. When fraud is committed against the public sector, money is diverted from important services into the hands of criminals. Fraudsters are constantly refining their tactics and techniques in order to circumvent the checks and controls put in place to prevent fraud from occurring. In order to protect resources, public sector bodies must therefore continuously review and develop their counter fraud arrangements to meet these evolving threats.

3.0 THE COUNTER FRAUD POLICY FRAMEWORK

3.1 As a unitary authority, North Yorkshire Council will be responsible for counter fraud arrangements across a number of new service areas, including business rates, council tax, benefits and housing. The total value of fraud risk facing the Council will therefore be significantly higher than for the County Council. It is therefore important that the Council has a policy framework in place on vesting day in order to effectively address the risks of fraud.

3.2 The draft Counter Fraud and Corruption Policy is attached at **appendix 1**. The policy sets out how suspected fraud should be reported, investigated, and what sanctions can be applied when fraud is found, including prosecution. The policy also contains an Anti-Bribery policy to protect the Council from fraud occurring within the organisation.

3.3 The draft Whistleblowing Policy is attached at **appendix 2**. The policy sets out a process for people working for the Council to report concerns that are in the public interest. It is important that employees and contractors feel comfortable to report concerns and are aware of the protections in law which apply to people who ‘blow the whistle’. It is equally important that managers are aware of what to do when a member of staff reports a concern. The policy therefore contains an appendix which provides a procedure for managers to follow in such circumstances.

3.4 The draft Anti-Money Laundering and Terrorist Financing Policy is attached at

appendix 3. The purpose of the policy is to protect the Council from criminals who try to 'launder' assets obtained through crime and make them appear legitimate. The Council has a legal obligation to report suspicions of money laundering to the National Crime Agency and when undertaking certain types of activity to follow the money laundering regulations.

3.5 The policies contain references to certain posts, other related policies, and service areas which are yet to be determined. The references have been highlighted and will be confirmed ahead of vesting date.

3.6 Further fraud related work is required ahead of vesting day. A draft Counter Fraud Strategy and Fraud Risk Assessment will be presented to the Committee in March 2023, along with the annual counter fraud work programme. Awareness raising and training for staff in all the North Yorkshire councils will also continue up to vesting day to help ensure fraud risks are mitigated.

4.0 RECOMMENDATION

4.1 Members are asked to approve the Counter Fraud and Corruption Policy, the Whistleblowing Policy, and the Anti-Money Laundering and Terrorist Financing Policy.

M A THOMAS
Head of Internal Audit

12 December 2022

BACKGROUND DOCUMENTS

None

Report prepared by Jonathan Dodsworth (Veritau – Counter Fraud) and presented by Max Thomas (Head of Internal Audit).

Veritau - Assurance Services for the Public Sector
County Hall
Northallerton

COUNTER FRAUD AND CORRUPTION POLICY

Incorporating the Fraud and Corruption Prosecution Policy and the Anti-Bribery Policy

1 Introduction

1.1 Fraud committed against the Council represents the theft of taxpayer's money. It is unlawful and deprives the Council of resources which should be available to provide services to the public. The Council must have effective measures in place to counter risks of fraud and corruption, to help reduce losses and to minimise the impact on services.

1.2 This document sets out the Council's policy on countering fraud and corruption risks. It includes overall arrangements and responsibilities for preventing, detecting and deterring fraud. It includes the Fraud and Corruption Prosecution Policy at annex A and the Anti-Bribery Policy at annex B. It forms part of the Council's overall policy framework for combating fraud and corruption and should be read in conjunction with other relevant guidance and policies including the following.

- The Constitution
- Financial Procedure Rules
- Procurement and Contract Procedure Rules
- Counter Fraud and Corruption Strategy
- Whistleblowing Policy
- Anti-Money Laundering policy
- Disciplinary Procedures

2 Definitions and Scope

2.1 For the purpose of this policy, the term fraud is used broadly to encompass:

- acts which would fall under the definition in the Fraud Act (2006)
- anything which may be deemed fraudulent in accordance with the generally held view of fraud as causing loss or making a gain at the expense of someone by deception and dishonest means
- any offences which fall under the Council Tax Reduction Schemes Regulations (2013) and the Prevention of Social Housing Fraud Act (2013)
- any act of bribery or corruption including specific offences covered by the Bribery Act (2010)
- acts of theft
- any other irregularity which is to the detriment of the Council whether financially or otherwise, or by which someone gains a benefit they are not entitled to.

2.2 This policy does not cover fraud or corruption against third parties, except in circumstances where there may also be a detriment to the Council. It does not cover other acts – for example offences involving violence –

which may affect the Council, which in most cases should be reported directly to the police.

3 Principles

3.1 The Council will not tolerate fraud or corruption in the administration of its responsibilities, whoever commits it. This includes, for example:

- councillors
- officers
- customers receiving services
- third party organisations contracting with the Council
- organisations or individuals receiving funding from the Council
- any other agencies the Council has business dealings with

3.2 There is a basic expectation that councillors, employees, and contractors' staff will act with integrity and with due regard to matters of probity and propriety. All representatives of the Council are required to act lawfully and comply with all rules, procedures and practices set out in legislation, the Constitution, the Council's policy framework, and all relevant professional and other codes of practice.

3.3 The Council will seek to assess its exposure to risks of fraud and corruption. It will prioritise resources available to prevent and deter fraud to help minimise this risk.

3.4 The Council will take all allegations and suspicions of fraud seriously, regardless of the source. It will consider any issues raised and if appropriate will undertake an investigation to confirm whether fraud has occurred and determine appropriate outcomes. Investigations undertaken will be proportionate to the circumstances of the issues raised. The Council may refer any incident of suspected fraud to the police or other agencies for investigation, where appropriate.

3.5 To act as a deterrent, the Council will take action in all cases where fraud (or an attempt to commit fraud) is proven, in proportion to the act committed and through any appropriate route. This may include prosecution, application of internal disciplinary procedures, referral under relevant codes of conduct or to a professional body, or any other action appropriate to the offence. Prosecution decisions will be made in accordance with the Fraud and Corruption Prosecution Policy which is contained in annex A.

3.6 As a further deterrent, and to minimise losses, the Council will attempt to recover any losses incurred through civil or legal action. In addition, the

Council will seek to apply any appropriate fines or penalties, and recover any costs incurred in investigating and prosecuting cases.

3.7 The Council will not tolerate any form of bribery. This includes bribes offered to or by employees, councillors, or suppliers. Any act of bribery puts the Council at risk of committing a criminal offence. Further details about the Council's measures to prevent and detect bribery are contained in the Anti-Bribery Policy which is attached at annex B.

4 Responsibilities

4.1 Overall responsibility for counter fraud arrangements rests with the [CFO / s151 officer] on behalf of the Council. The [CFO / s151 officer] has a responsibility for ensuring the Council has appropriate measures for the prevention and detection of fraud and corruption.

4.2 The Audit Committee has a responsibility to consider the effectiveness of counter fraud and anti-corruption arrangements at the Council. This includes monitoring of Council policies on raising concerns at work and countering the risks of fraud and corruption.

4.3 [Management board / CMT] are collectively responsible for ensuring that the Council has effective counter fraud and corruption procedures; that these comply with best practice and good governance standards; and that they are embedded across the organisation.

4.4 [Veritau] (who provide internal audit and counter fraud services to the Council) is responsible for reviewing the Council's counter fraud and corruption policies on a regular basis and recommending any changes needed. In addition, [Veritau] leads on fraud prevention and detection for the Council and is responsible for investigating suspected cases of fraud or corruption. The internal audit team carries out audit work to ensure that systems of control are operating effectively. This helps to reduce opportunities for fraud to be committed.

4.5 All managers are responsible for preventing and detecting fraud in their service areas. This includes maintaining effective systems of control and ensuring that any weaknesses identified are addressed promptly.

4.6 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 money laundering regulations.

4.7 All staff should be aware that fraud and corruption is a threat to the Council and are required to report any suspicions of fraud to [Veritau]. Where appropriate, staff can use the Whistleblowing Policy to raise concerns anonymously.

4.8 Officers within Human Resources are responsible for supporting service departments when pre-disciplinary investigations are required, or disciplinary processes are to be applied.

5 Overall Counter Fraud Arrangements

Introduction

5.1 The purpose of this section is to set out the Council's overall framework for countering the risks of fraud and corruption. The Council aims to follow best practice in countering fraud risks[1], but recognises that new and emerging fraud risks require a dynamic approach to fraud prevention and detection.

Measurement

5.2 The Council will assess potential risks and losses due to fraud and corruption. It will use this information to prioritise counter fraud activity and determine the resources needed to mitigate those risks. A summary of fraud risks and proposed counter fraud activity will be reported to the Audit Committee on an annual basis.

Culture

5.3 The Council will promote a culture where all employees, councillors, service users, and contractors are aware that fraud or corruption in any form is unacceptable. To do this, it will:

- ensure that there are clear arrangements in place for anyone to report suspicions of fraud or corruption (including employees, councillors, partners, contractors, the public or any other stakeholders)
- investigate suspicions reported and take appropriate action wherever evidence of fraud or corruption is found
- ensure that the consequences of committing or taking part in fraud or corruption are widely publicised.

Prevention and Detection

Controls

5.4 As part of normal operations the Council aims to ensure that proper systems of internal control are in place. This includes controls that can directly prevent and detect fraud. For example, separation of duties,

[1] For example the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption.

management review, vetting as part of recruitment processes, and systems for declaring interests or gifts and hospitality. The effectiveness of the systems of control are monitored by internal audit and reported to the Audit Committee.

5.5 Services will be encouraged to consider the risk of fraud as part of the Council's risk management process. Any information on risks identified will be used to inform the annual review of counter fraud activity.

Proactive Work

5.6 The Council will carry out targeted project work (for example data matching exercises) to identify fraud and corruption in known high risk areas. This work will be carried out by [Veritau] as part of its annual work plan. Resources will be prioritised based on an annual assessment of fraud and corruption risks. Work may include joint exercises with other agencies, including other councils.

5.7 The Council will take part in projects led by other agencies that can help to identify potential fraud and corruption – for example the Cabinet Office's National Fraud Initiative. Resources will be allocated to take part in these exercises and to follow up any high risk data matches identified. [Veritau] will support service departments to ensure data is available to be used for matching exercises – for example advising on data protection considerations.

Relationships

5.8 The Council will establish and maintain relationships with external agencies that can help it prevent and detect fraud. These include:

- the police
- the courts
- the Cabinet Office
- the Department for Levelling Up, Housing, and Communities
- the Department for Work and Pensions
- other councils
- other public sector organisations (eg housing associations)
- charities, community and voluntary groups.

5.9 [Veritau] will work with Council departments to ensure that systems for reporting and investigating suspected fraud and corruption are robust.

Fraud Awareness Training

5.10 As part of the annual counter fraud workplan, [Veritau] will provide targeted fraud awareness training to groups of staff in areas at higher risk of fraud and corruption.

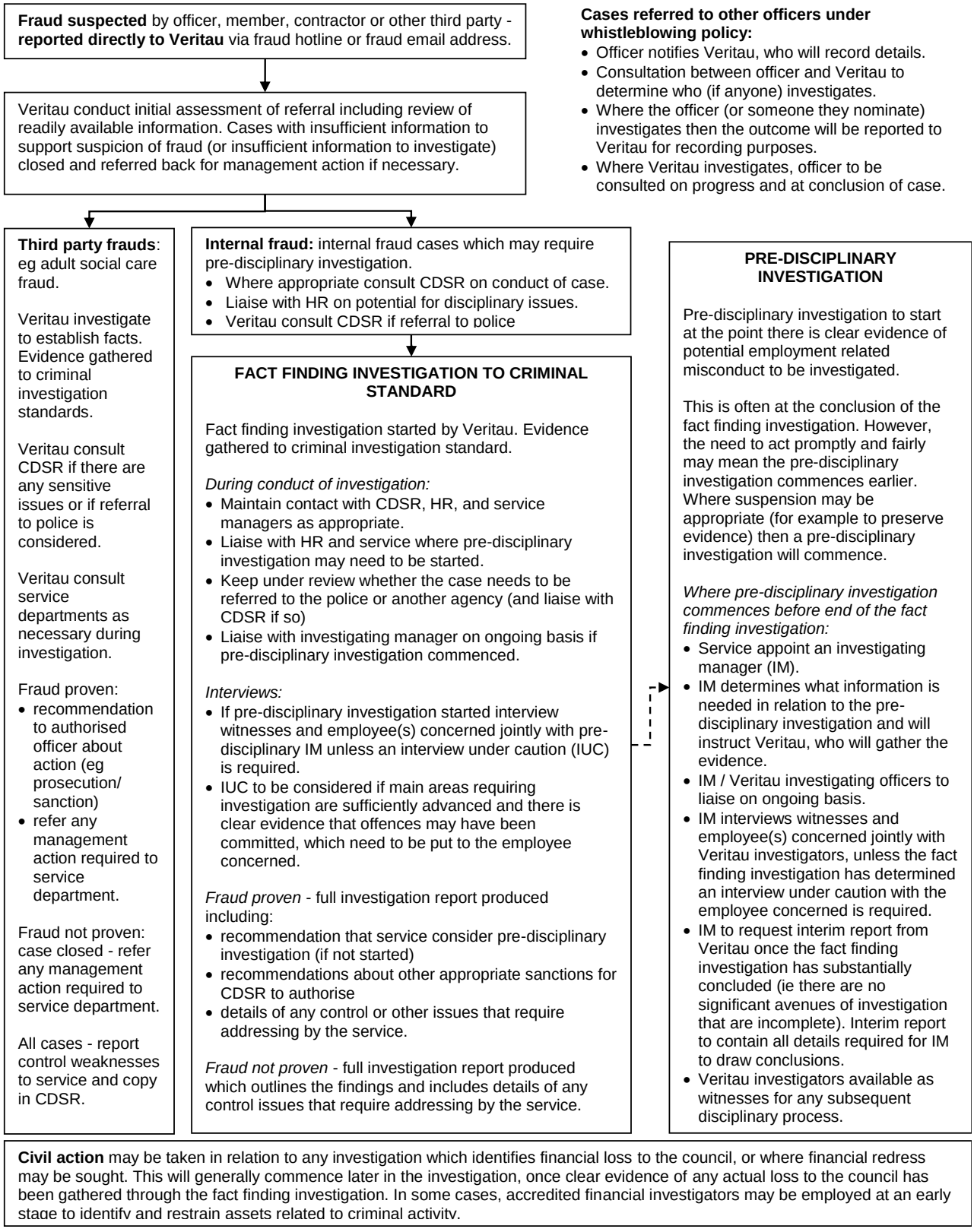
Investigation

5.11 Suspected cases of fraud, corruption, theft, or other irregularities considered a high risk will be investigated. The nature of the investigation will depend on the circumstances of each case. Any suspected fraud should be reported to [Veritau] in the first instance. [Veritau] will assess all cases referred and provide advice on whether other agencies should be notified (such as the police). In more complex cases, the extent of investigation required will be decided in consultation with the [CFO / s151 officer], [Monitoring Officer], service department, and human resources, as appropriate. Where necessary, [Veritau] may refer cases to other agencies (for example the police) at the discretion of the Head of Internal Audit. Figure 1 overleaf outlines the fraud referral and investigation process.

5.12 All staff involved in the investigation of fraud will be appropriately trained. They will be required to comply with any relevant legislation and codes of practice. For example, the Police and Criminal Evidence Act (PACE), Regulation of Investigatory Powers Act (RIPA), the UK General Data Protection Regulation (UK GDPR), the Criminal Procedure and Investigations Act (CPIA), and any relevant guidance from the Attorney General. Investigators will consider the individual circumstances of anyone subject to investigation; adjustments to procedure will be made where necessary to ensure that all parties are treated equitably (where it is appropriate and reasonable to do so).

5.13 Every investigation will consider whether weaknesses in controls have contributed to the fraud or error occurring, in addition to other objectives. Where needed, recommendations to improve controls will be made.

Figure 1: North Yorkshire Council investigation process



5.14 The Head of Internal Audit will ensure that systems for investigating fraud are reviewed on an ongoing basis, to ensure that they remain up to date and comply with best practice.

Publicity

5.15 Targeted publicity will be used to raise awareness of fraud risks to employees, councillors, the public, and other agencies. This will include internal and external publicity. The aim of this will be to ensure that stakeholders:

- are alert to the risks of fraud and corruption
- know how to report suspicions of fraud
- are aware of the Council's zero tolerance approach to fraud and corruption.

5.16 The Council will publicise all successful prosecutions by itself or by partner organisations, to act as a deterrent against future fraud.

Recovery of Monies

5.17 Fraud and corruption will generally result in a loss to the Council or additional costs being incurred. Where this is the case, the Council will seek to recover its loss (or costs) from the individual or organisation responsible. This action helps to reduce the financial impact of fraud and acts as a deterrent. As a further deterrent, the Council will seek to apply any appropriate fines or penalties where it is possible and desirable to do so.

5.18 Methods of recovery include (but are not limited to):

- civil enforcement through the courts
- recovery from assets held by the organisation or individual using the Proceeds of Crime Act or other relevant legislation
- recovery from salary payments for Council employees
- recovery from pension benefits for members of the LGPS
- petitioning for bankruptcy if appropriate.

6 Monitoring & Review Arrangements

6.1 The arrangements set out in this policy will be reviewed on an annual basis as part of the counter fraud workplan. If required, updates will be presented to the Audit Committee for approval.

POLICY APPROVED XX XX 2022

ANNEX A

FRAUD AND CORRUPTION PROSECUTION POLICY

1 Scope and Purpose

1.1 The Council is committed to deterring fraud and corruption and recovering public funds. The decision to prosecute an individual is always a serious matter; however fair and effective enforcement is essential in protecting the Council from fraud.

1.2 Prosecution has a serious effect on suspects, witnesses, victims, and the public, so it is essential that the Council makes fair, consistent, and timely decisions in all cases. Where appropriate, lesser sanctions can be considered instead of prosecution.

1.3 This policy sets out the decision-making process for those cases where fraud or corruption has been found to have been committed against the Council.[2] Decisions should be fair, appropriate, and in the best interests of both the public and the Council.

1.4 The policy is based on principles set out in the Crown Prosecution Service's Code for Crown Prosecutors.

2 Principles

2.1 All decisions on intended prosecutions should be transparent and independent from the investigating officer(s) involved in the case. Any decision to prosecute should only be made after a review by appropriate officers and be authorised by a senior council officer. All decisions and the reasons for them should be properly documented.

2.2 When making decisions on prosecutions, officers must be fair and objective. They must not let any personal views about the ethnic or national origin, gender, disability, age, religion or belief, sexual orientation or gender identity of the suspect, defendant, victim or any witness influence their decisions. Neither must they be motivated by political considerations. In prosecuting individuals, the Council must always be acting in the interests of justice and not solely for the purpose of obtaining a conviction. Decisions should be consistent with Council policy and the law on equalities and human rights. The circumstances of the offence and any mitigation offered by the offender should be taken into consideration when making a decision.

2.3 The consistent application of the policy will help ensure that those who have perpetrated fraud and corruption are appropriately penalised. It will also act as a meaningful deterrent to those who are contemplating

[2] This policy does not cover internal disciplinary procedures which are the subject of separate policies, nor does it cover offences other than fraud and corruption which are dealt with by relevant service departments under other policies and specific legal powers.

committing fraud or corruption. The Council recognises the deterrent value of good publicity and therefore information regarding successful prosecutions and sanctions will be made public.

2.4 Staff and members who are found to have committed fraud or corruption against the Council may be prosecuted in addition to such other action(s) that the Council may decide to take, including disciplinary proceedings in the case of staff, and referral to the Standards Committee in the case of members. Any decision not to prosecute a member of staff for fraud and corruption does not preclude action being taken in accordance with the Council's disciplinary procedures or other policies.

2.5 Irrespective of the action taken to prosecute the perpetrators of fraud and corruption, the Council will take whatever steps necessary to recover any losses incurred, including taking action in the civil courts.

3 Prosecution

3.1 Local authorities are granted the power to prosecute under the Local Government Act 1972 (section 222). The legislation states that these powers should only be used for "the promotion or protection of the interests of the inhabitants of their area".

3.2 Not every contravention of the law should be considered for prosecution. The Council should weigh the seriousness of the offence alongside other relevant factors, including the circumstances of the offender, the level of any financial loss to the Council, mitigating circumstances and other public interest criteria.

3.3 A prosecution should only be considered if the investigation has passed two tests: the evidential test and the public interest test.

3.4 To pass the evidential test, authorised officers must be satisfied that there is a realistic prospect of conviction based on the available evidence (that is, there must be sufficient admissible, substantial and reliable evidence to secure a conviction). They should also consider what the defence case may be, and how it is likely to affect the prospects of conviction.

3.5 In deciding whether there is sufficient evidence to prosecute, the Council should consider the following questions:

- Is the evidence admissible in court
- Is the evidence reliable
- Is the evidence credible

- Is there any unused or unexamined material that might undermine the proposed charges
- Is there any additional evidence that could be obtained through further reasonable lines of enquiry?

3.6 Where there is sufficient evidence to justify a prosecution, authorised officers should consider whether a prosecution is required in the public interest. They should consider:

- How serious is the offence committed
- What is the level of culpability of the suspect
- What are the circumstances of, and harm caused to the victim
- What was the suspect's age and maturity at the time of the offence
- What is the impact on the community
- Is prosecution a proportionate response
- Do sources of information require protecting?

3.7 Where an investigation is found to meet the evidential test, but not the public interest test consideration should be given to lesser sanctions such as a formal written warning or a financial penalty (where appropriate).

3.8 Investigating officers and prosecutors will review the appropriateness of pre-charge engagement where prosecution is considered. This is likely to occur where such engagement may lead the defendant to volunteer additional information that may identify new lines of inquiry. Pre-charge engagement may be instigated by the investigating officer, the Council prosecutor, the defendant's representative or a defendant themselves (if unrepresented).

4 Alternatives to Prosecution

4.1 If a case is considered strong enough for prosecution but there are mitigating circumstances which cast a doubt as to whether a prosecution is appropriate then the Council may consider the offer of a sanction instead. The two sanctions available are:

- a formal written warning
- a financial penalty.

Formal Written Warnings

4.2 A formal written warning can be given to a person who has committed an offence, as an alternative to prosecution in certain circumstances. All warnings are recorded internally and kept for six years. If a person who has received a formal warning re-offends then this will influence the decision on whether to prosecute or not.

4.3 For less serious offences a formal warning will normally be considered where all of the following apply:

- there is no significant public interest in prosecuting
- it was a first offence, and
- a financial penalty is not considered to be appropriate (for Council Tax Support offences).

Only in very exceptional circumstances will a further warning be issued for a second or subsequent offence of the same nature.

4.4 Offenders will usually be asked to attend the Council's offices to receive the formal written warnings in person. For more minor offences an advisory letter can be issued by post.

Financial Penalties

4.5 In cases of Council Tax Support fraud, legislation[3] allows for a financial penalty to be offered to offenders as an alternative to prosecution. The penalty is set at 50% of the amount of the excess reduction, subject to a minimum of £100 and a maximum of £1,000. Once a penalty is accepted, the claimant has 14 days to consider their decision.

4.6 Subject to the criteria set out in the guidelines below, a financial penalty will normally be offered by the Council in the following circumstances:

- the council believes that there is sufficient evidence to prosecute
- it was a first offence or a previous offence was dealt with by way of a formal warning, and
- in the opinion of the Council, the circumstances of the case mean it is not overwhelmingly suitable for prosecution, and
- the claimant has the means to repay both the overpayment and the penalty, and
- there is a strong likelihood that both the excess reduction and the penalty will be repaid.

4.7 It is important to note that the claimant does not need to have admitted the offence for a financial penalty to be offered. Financial penalties will be administered by authorised officers. If a financial penalty is not accepted or the acceptance is later withdrawn then the Council will usually consider the case for prosecution. In such cases the court will be informed that the defendant was offered a penalty but declined to accept it.

[3] The Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013

5 Proceeds of Crime Act 2002 (POCA)

5.1 In addition to the actions set out in this policy, the Council reserves the right to refer all suitable cases for financial investigation with a view to applying to the courts for restraint and/or confiscation of identified assets. A restraint order will prevent a person from dealing with specific assets. A confiscation order enables the Council to recover its losses from assets which are found to be the proceeds of crime.

6 Implementation Date

6.1 This policy is effective from 1 April 2023 and covers all decisions relating to prosecutions and sanctions after this date.

ANNEX B

ANTI-BRIBERY POLICY

1 Introduction

1.1 The Bribery Act became law in 2011. It enables appropriate action to be taken against all forms of bribery.

1.2 Bribery is defined as the offering, giving, receiving, or soliciting of any item of value to influence the actions of an official or other person in charge of a public or legal duty. The act of bribery is the intention to gain a personal, commercial, regulatory, or contractual advantage. The Council does not tolerate any form of bribery.

1.3 Facilitation payments are unofficial payments made to public officials to secure or expedite actions. These are not tolerated and are illegal.

1.4 This policy should be read in conjunction with the [Council's Gifts and Hospitality Protocol].

2 Principles

2.1 The Council is committed to preventing, detecting, and deterring bribery. It aims to:

- ensure all employees, workers, councillors, and other relevant groups are aware of their responsibilities under this policy by publicising it and providing training
- encourage employees to be vigilant and report any suspicions of bribery
- investigate any allegations of bribery or assist the police or other agencies in any investigations or prosecutions they undertake
- take action against anyone involved in bribery in relation to Council business.

3 Scope

3.1 This policy relates to all Council activities. It applies to employees, workers, agency staff, volunteers, consultants, and councillors.

3.2 For partners, joint ventures, and suppliers, we will seek to promote the adoption of policies consistent with the principles set out in this policy.

3.3 The Council requires employees, councillors and other relevant people to:

- raise concerns if they believe that this policy has been breached or may be breached in the future

- comply with the spirit, as well as the letter, of the laws and regulations of all jurisdictions in which the Council operates, in relation to the lawful and responsible conduct of activities.

3.4 As well as potential civil action and criminal prosecution, employees breaching this policy may face disciplinary action. This could result in dismissal in cases of gross misconduct.

4 Offences

4.1 There are four key offences under the Bribery Act 2010.

Section 1 – Offence of bribing another person

4.2 This section makes it an offence when a person offers, promises, or gives a financial or other advantage to another person and intends the advantage to induce a person to perform improperly a relevant function or activity or to reward a person for the improper performance of such a function or activity.

4.3 It is also an offence when a person offers, promises, or gives a financial or other advantage to another person and knows or believes that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity.

Section 2 – Being bribed

4.4 This section makes it an offence when a person requests, agrees to receive or accepts a financial or other advantage intending that, in consequence, a relevant function or activity should be performed improperly.

4.5 It is an offence when a person requests, agrees to receive or accepts a financial or other advantage and the request, agreement, or acceptance itself constitutes the improper performance of the person of a relevant function or activity.

4.6 It is an offence if a person requests, agrees to receive or accepts a financial or other advantage as a reward for the improper performance of a relevant function or activity.

4.7 It is also an offence if a person in anticipation of or in consequence of the person requesting, agreeing to receive, or accepting a financial or other advantage, a relevant function or activity is performed improperly.

Section 6 – Bribery of foreign public officials

4.8 Under this section of the Act an offence is committed when a person intends to influence a foreign official in their official capacity and intends to obtain or retain business or an advantage in the conduct of business.

4.9 It is also an offence to offer, promise or give any financial or other advantage to a foreign public official.

Section 7 – Failure of a commercial organisation to prevent bribery

4.10 A relevant commercial organisation is guilty of an offence if a person associated with the organisation bribes another person intending to obtain or retain business for the organisation or to obtain or retain an advantage in the conduct of business for the organisation and the organisation fails to take reasonable steps to implement adequate procedures to prevent such activity.

Corporate responsibility

4.11 While the first three offences of the Bribery Act relate to the actions of people, a section 7 offence relates to the inaction of an organisation to prevent bribery. The legislation was drafted with commercial businesses in mind and after the legislation was adopted there was some debate as to whether public sector organisations could be found liable of the offence. In 2012 the government published guidance which clarified that any public sector organisation that "engages in commercial activities, irrespective of the purpose for which profits are made"[4] could be found guilty of a Section 7 offence.

4.12 North Yorkshire Council should be considered as commercial organisation under the legislation and could therefore be found to be corporately responsible for acts of bribery that occur within it. It is therefore important that it takes steps to prevent bribery from occurring.

4.13 If an offence has occurred, then the courts will consider six tests to determine whether the Council had any responsibility for the act.

[4] Paragraph 35 of Bribery Act 2010: Guidance to help commercial organisations prevent bribery https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/832011/bribery-act-2010-guidance.pdf

- Does the Council have proportionate procedures in place to prevent bribery by persons associated with it? These should be clear, practical, and accessible?
- Is there top-level commitment to preventing bribery? This includes support by councillors as well as officers.
- Is the Council's exposure to potential external and internal risks of bribery periodically assessed?
- Does the Council take a proportionate and risk based approach to mitigate bribery risks?
- Are anti-bribery policies and procedures embedded and understood throughout the organisation? Are they communicated internally and externally?
- Are procedures monitored and reviewed regularly?

Penalties

4.14 A person guilty of an offence under sections 1, 2, or 6 of the Bribery Act may be sentenced to:

- a maximum prison sentence of 12 months and/or a fine not exceeding £5,000 (if convicted in a magistrates court)
- a maximum prison sentence of 10 years and/or an unlimited fine (if convicted at a crown court).

4.15 An organisation found guilty of allowing bribery offences to occur may be subject to an unlimited fine that is in part determined by the gain that was sought to be made through bribery offences and an assessment of an organisation's culpability by the court.

5 How to raise a concern

5.1 All stakeholders have a responsibility to help the Council prevent and detect bribery and corruption. Any suspicions should be reported as soon as possible.

5.2 Members of staff should report suspicious activity to the counter fraud hotline on [0800 9179247 or by email to counter.fraud@veritau.co.uk.]. Alternatively, employees, workers, or contractors may raise concerns through the Council's Whistleblowing arrangements.

5.3 The Council will support anyone who reports suspicions or raises concerns, even if those concerns prove to be incorrect. It is committed to ensuring nobody suffers detrimental treatment because they refuse to take part in bribery or corruption, or because they report a concern that they believe is true.

6 What to do if someone reports a concern

6.1 All reports of possible bribery should be reported without delay to the Council's [CFO / s151 officer], [Monitoring Officer], and [Veritau].

WHISTLEBLOWING POLICY

1 INTRODUCTION

1.1 This policy provides a framework for employees, workers, and contractors to raise concerns about issues happening at the Council. For example, health and safety risks, criminal or unlawful activity, or activities that could damage the environment. It sets out how concerns can be raised and the protection that people working for the Council have if they raise an issue.

1.2 This policy covers concerns raised by employees, workers, and contractors. It reflects the specific protections they have in law when making a protected disclosure. This is also known as raising a whistleblowing concern or blowing the whistle. Further information on what a protected disclosure is, and who the law protects is set out below.

1.3 North Yorkshire Council is committed to maintaining high standards of integrity and accountability. It aims to create an open environment in which employees and those working on behalf of the Council can raise issues and be confident that they will be acted upon. The Council's message to anyone working for the council is straightforward - if in doubt, raise it!

1.4 The Public Interest Disclosure Act 1998 (PIDA) is the law that protects people against detrimental treatment or dismissal if they make a protected disclosure. It is part of the Employment Rights Act 1996. This policy is designed to reflect the legislation[1] as well as guidance from the government and other organisations[2].

1.5 A guide for managers and other employees on what to do if they receive a whistleblowing report is contained in appendix A of this policy. A training package for managers on whistleblowing can be found on the Council's Learning Zone. The Learning Zone also includes a training package for all employees about whistleblowing. This provides further information on the issues set out in this policy.

2 AIMS AND SCOPE OF THE POLICY

2.1 This policy aims to:

- encourage workers to raise concerns they have about their workplace or working practices
- make sure managers know what a whistleblowing concern is and how they must address it

[1] PIDA 1998 was updated by the Enterprise and Regulatory Reform Act 2013.
[2] Whistleblowing guidance has been issued by the Department for Business, Energy & Industrial Strategy, the National Audit Office and the charity, PROTECT.

- ensure that workers receive a response to any concern raised
- inform workers about how they can pursue an issue further if they are not satisfied with the action taken by the Council
- reassure workers that they will be protected from dismissal or negative treatment if they raise concerns.

2.2 This policy applies to most people working for the Council. This includes employees, workers, staff in maintained schools, agency personnel, contractors and staff seconded to or from a third party. Throughout the rest of the policy, the terms worker, or workers is used to mean anyone covered by the policy and the protections of PIDA.

2.3 PIDA does not provide protection under the law for job applicants, genuinely self-employed workers, or volunteers.

Definitions

2.4 Protected disclosures are concerns raised that are protected under PIDA. To be a protected disclosure, anyone raising a concern must:

- reasonably believe that their concern is in the public interest – this is explained in paragraph 2.6.
- reasonably believe their concern is a type of wrongdoing covered by the law – a list of the types is included in paragraph 2.7.
- raise it in a way that that is in accordance with the law – further information on this is provided in section 7.

2.5 A reasonable belief is one where the whistleblower has some reasonable grounds or basis for believing there has been wrongdoing. It does not actually have to be true. For example, it does not matter if it turns out they were mistaken if they had reasonable grounds for believing it when they originally raised the concern.

2.6 An issue in the public interest means that it will usually affect people other than just the person raising it. Something that relates only to an individual's own employment may not be covered by the law. Although there are some circumstances when this could still be in the public interest. For example, an issue about bullying or harassment that reflects a wider cultural issue in a team. This policy is intended to cover workers raising an issue in the public interest. If a person needs to address a problem that relates only to their own employment, then they should refer to the [Raising Concerns at Work Policy].

2.7 The list below sets out the types of concerns that qualify for protection under the law if they are raised.

- A criminal offence – for example corruption, theft, or fraud.
- Failure to comply with a legal obligation such as a statutory requirement, a contract, or common law obligations (eg negligence).
- A miscarriage of justice.
- Health and safety risks. This includes risks to anyone, not just workers – for example risks to customers and service users.
- Environmental damage – any wrongdoing that endangers or damages the environment.
- Cover up. This includes anything where wrongdoing in any of the above areas has been deliberately concealed.

3 SAFEGUARDS

3.1 The Council recognises that a decision to report a concern can be a difficult one. In many cases it is workers who are best placed to learn of wrongdoing within service areas and schools or to hear about issues where standards have fallen below those that the Council and public expect. The Council is grateful to everyone who reports their concerns.

3.2 Workers should have nothing to fear by reporting their concerns if they have grounds for believing what they are reporting is true. Even if it is later found to be incorrect. No action will be taken against anyone genuinely reporting a concern.

3.3 While rare, deliberately false reports are sometimes made. If false or deliberately misleading information is provided, then this would be considered a serious matter. It could result in action being taken under the Council's disciplinary policy. Equally, deterring another worker from reporting a genuine concern is also a serious matter and may result in disciplinary action being taken.

3.4 The Council will not tolerate any negative treatment (including harassment or victimisation) of a worker who has raised a whistleblowing concern, by anyone (including colleagues and managers). Any allegations of negative treatment of someone raising a concern will be investigated. Where evidence of mistreatment is found then this could result in disciplinary action being taken.

3.5 The Council recognises that workers may want to raise a concern in confidence under this policy. If a worker asks the Council to protect their anonymity, then efforts will be made to protect their identity from being disclosed. However, this cannot be guaranteed. For example, if evidence needs to be presented in court, or revealed as part of a subsequent investigation. If it becomes clear that a whistleblower's anonymity cannot

be protected, then this will be discussed with them before any disclosure is made.

3.6 The Council encourages workers to put their names to information they disclose. Concerns expressed anonymously will be considered by the Council. However, they can be harder to investigate. This may make it more difficult to gather evidence to confirm wrongdoing. It will also not be possible to provide feedback to an anonymous whistleblower during or following an investigation. Anonymous reports are however preferred to silence.

4 HOW TO RAISE A CONCERN

4.1 Many whistleblowing concerns are raised and properly addressed within individual service areas. In most cases, workers are therefore encouraged to raise concerns with their line manager in the first instance[3]. Line managers will provide feedback to the whistleblower about the action they are taking. Contractors should report issues to the Council's designated contract or client manager.

4.2 Concerns do not have to be made in writing. Any issues raised verbally will be treated just as seriously.

4.3 If a worker raises an issue with their line manager but it is not adequately addressed or if the concern involves the line manager, then they should speak to a more senior officer. School-based workers can escalate issues to the chair of governors.

4.4 The Council recognises that there may be times when whistleblowers feel unable to speak to anyone in their own service area. For example, if they believe the issue involves more senior officers or if the issue has already been raised through the normal channels but has not been addressed. In this situation workers can contact the Council's independent whistleblowing hotline on [0800 9179 247, which is overseen by Veritau].

4.5 If anonymous concerns are raised through social media, then they will be considered under the more general counter fraud or complaints policies unless it is beyond doubt that the person raising the concern would fall under the whistleblowing policy.

[3] People raising a concern may not directly say they are whistleblowing or making a protected disclosure. It is therefore essential that managers understand when an issue raised with them would be considered whistleblowing. Further information is available in the guidance notes included with this policy. Training is also available through the Learning Zone. Managers can also contact [Veritau] for advice on any issues raised.

5 HOW THE COUNCIL WILL RESPOND

5.1 All whistleblowing reports will be carefully considered. Initial enquiries will be made to help decide whether an investigation is needed or what action may be required.

5.2 The Council aims to acknowledge all whistleblowing reports within five working days. The line manager or other officer dealing with a whistleblowing issue will try to write or speak to the whistleblower promptly, to provide additional information on what is being done. For example, whether an investigation is needed or if specific action is to be taken.

5.3 If an investigation is undertaken, the line manager or investigating officer will provide feedback on the outcome, and details of action to be taken as far as possible. Although it may not always be possible to provide full details. For example, it would not be appropriate to share personal data about other people.

6 INVESTIGATION AND REPORTING PROCESS

6.1 The steps line managers need to take will depend on the nature, complexity, and seriousness of the issue raised. An outline of the process managers should follow is set out below. Further information for managers on who they need to inform about whistleblowing issues is set out in the guidance at appendix A.

6.2 Straightforward whistleblowing issues may be dealt with directly by line managers. The manager must ensure the requirements for acknowledging concerns and providing feedback are followed (see section 5 above). When the issue has been dealt with, the line manager must provide details to [Veritau] of the concern raised and the outcomes ([Veritau] keeps a record of all whistleblowing concerns raised, on behalf of the Council).

6.3 For more complex cases, and any case involving suspected fraud, corruption, or theft, managers must refer the issue to [Veritau] at the outset. [Veritau] will liaise with the manager to decide how the issue should be investigated. The officers assigned to investigate each case will depend on the nature of the issue. For example, safety issues may be investigated by the Health & Safety Team, alleged fraud or criminality by the Counter Fraud Team, or employment issues by the manager or a manager from another team, with support from Human Resources.

6.4 The amount of contact between officers investigating whistleblowing concerns and the whistleblower will depend on the nature of the matters

raised and the clarity of the information provided. If necessary, further information may be sought from the whistleblower.

6.5 If a face to face meeting is necessary or desirable the whistleblower has the right, if they so wish, to be accompanied by a Union representative or a colleague who is not involved in the area of work to which the concern relates.

6.6 The Council will take steps to support whistleblowers during an investigation, where possible. For example, if they are required to give evidence in any proceedings, the Council will provide advice and support with the process as far as appropriate. Whistleblowers should contact HR if they suffer any negative treatment as a result of raising an issue. Investigating managers should be alert to the possibility of a whistleblower being mistreated and should liaise with the Head of HR or relevant HR business partner if they have concerns.

6.7 All whistleblowing issues raised will be logged centrally by Veritau. The Chief Executive, [CFO / s151 officer], and [Monitoring Officer] will be notified of relevant whistleblowing issues. Numbers of whistleblowing concerns raised and significant trends will also be reported annually to the Audit Committee.

7 HOW MATTERS CAN BE TAKEN FURTHER

7.1 This policy aims to provide workers with the means to raise concerns within the Council. If workers have reported an issue in accordance with the policy, but are not satisfied that it has been addressed then they may contact the following prescribed bodies:

- the Council's External Auditor – [TBD]
- the NSPCC or Ofsted (for concerns about children at risk of abuse)[4]
- relevant professional bodies or regulatory organisations[5], for example, the Information Commissioner's Office, Care and Quality Commission (CQC), and the Health and Safety Executive.

7.2 Disclosure of issues to a non-prescribed body (such as a newspaper or through social media) does not provide whistleblowers with protection under PIDA. Workers who are considering making a disclosure, other than to the prescribed bodies, should obtain specialist legal advice before doing so.

[4] The NSPCC and Ofsted offer dedicated national whistleblowing hotlines (see www.nspcc.org.uk and www.gov.uk/government/organisations/ofsted for further details).
[5] The Department for Business, Innovations and Skills maintains a list of prescribed persons and organisations who may be contacted, www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies.

8 INDEPENDENT ADVICE

8.1 Free confidential advice on how to raise a concern about malpractice at work can be sought from the independent charity PROTECT. They can be found at www.protect-advice.org.uk, or contacted by email at info@protect-advice.org.uk. The charity's lawyers can give free confidential advice about how to raise a concern about serious malpractice at work.

9 DATA PROTECTION

9.1 When managing whistleblowing reports, the Council processes personal data collected in accordance with its information governance policies. Data collected following receipt of a whistleblowing concern is held securely. It is only accessed or disclosed to individuals as necessary to manage, investigate, or take action in relation to the concern raised.

10 REVIEW OF THE POLICY

10.1 This policy will be reviewed at least every three years or when any significant changes to whistleblowing legislation, guidance or case law occurs.

Appendix A

Managers' Guidance on Whistleblowing

1 Introduction

1.1 The Council's whistleblowing policy aims to encourage employees, workers, and contractors[6] to raise concerns about activities in the workplace. It contains further information about what whistleblowing is and should be read alongside this guidance.

1.2 All managers are expected to take concerns raised by workers seriously and to follow the process set out in this guidance. Further training on whistleblowing is available through the Council's Learning Zone.

2 What is a whistleblowing complaint?

2.1 Managers need to consider any concern raised by a worker about working practices or malpractice, to assess whether it is a whistleblowing issue.

2.2 The concern does not have to be raised in writing. Issues raised verbally should be treated as seriously as those raised in writing. You should carefully document anything raised verbally with you.

2.3 It is not necessary for the term "whistleblowing" or "protected disclosure" to be used for an issue to be considered whistleblowing. Any concern that falls under the types of issues covered by the policy (see paragraph 2.7 of the main policy) may be a whistleblowing issue. The range of issues that could qualify is very broad and could include problems that may not initially appear very serious. For example, relatively minor breaches of health and safety processes or issues concerning a breach of contract. Care must therefore be taken to assess any issue raised with you, to consider whether it is whistleblowing.

2.4 Whistleblowing will generally be about issues that relate to more people than the individual who raised it. If it is clear that a concern relates only to an individual worker, then it should be considered under the [Resolving Issues at Work Policy]. However, care is needed when deciding this. For example, a report of bullying could just be about one worker. However, it could also reflect a culture of bullying and harassment in a service area. In this case the concern may be whistleblowing.

2.5 Whistleblowing reports can only come from people who work for the Council (including contractors). Further detail about who can report a concern is set out in paragraphs 2.2 and 2.3 of the policy. Concerns raised by members of the public or other groups would not be considered as whistleblowing. They should still be taken seriously though and directed to

[6] Throughout the rest of the guidance, the terms worker, or workers is used to mean anyone covered by the whistleblowing policy and the protections of PIDA.

the relevant team. For example, the Council's [complaints and feedback team] or the counter fraud team.

2.6 Whistleblowing reports are often made anonymously. Where an anonymous report is made, you should try to encourage (but not pressure) the person to give their name. For example, if you are taking information by phone or have an email address you can respond to. Make it clear that it can be more difficult to investigate concerns if contact with the whistleblower is not maintained.

2.7 Concerns or complaints about councillors are not covered by the whistleblowing policy. They would come under the Council's Standards procedures. Any issues relating to councillors should be referred to the [Monitoring Officer] for advice.

2.8 If you are not sure whether an issue should be classed as whistleblowing then advice can be sought from [Veritau] [7].

3 Reporting the receipt of a whistleblowing concern

3.1 Section 6 of the policy sets out what managers should do when they receive a whistleblowing concern. Managers should also notify their assistant director (or the chair of governors, for schools). They should also inform the Head of HR or HR business partner responsible for their area.

3.2 If the issue involves any of the people named above then you should tell a more senior officer such as the corporate director, [CFO / s151 officer], the Head of Internal Audit or the [assistant director for education] (in the case of schools).

3.3 [Veritau] maintains a central log of all whistleblowing reports received. Where a whistleblowing issue is handled within a service area or directorate, the outcome of any investigation and action taken should be reported to [Veritau] once the matter is completed.

3.4 If you are unsure about how to deal with a whistleblowing issue then you can seek advice from [Veritau]. Any complex issues, or any case involving fraud, corruption or theft should be reported to [Veritau] immediately. [Veritau] will determine how the issue should be investigated, in consultation with other relevant officers.

3.5 If you receive details of a whistleblowing concern raised with an external body (one of the prescribed persons and organisations set out in section 7 of the policy), the information should be forwarded to [Veritau].

[7] [Veritau] can be contacted by email on whistleblowing@veritau.co.uk

4 Initial response

4.1 If you are notified of a concern, you should acknowledge it immediately. Unless it was raised anonymously (with no reply address) then this should usually be done by email. If you are notified verbally, you should try to find out as much information as possible and document it. Try to obtain contact details if possible. Where information is received in writing you should usually try to arrange a meeting with the whistleblower to gather further information.

4.2 This initial meeting can be done in person, in or outside of the Council's offices, or by telephone. It is important to find an environment that the whistleblower feels comfortable with. They may be supported by a trade union representative or colleague. A note taker can be brought to the meeting with prior agreement from the whistleblower.

4.3 If anonymity is requested then every effort should be made to keep the whistleblower's identity concealed. However, anonymity cannot be guaranteed and you should not promise this. If it becomes apparent that a whistleblower's identity may become known, then they should be told about this as soon as possible.

4.4 All information relating to a whistleblowing report or gathered during a subsequent investigation should be kept confidential. Information should only be shared on a strictly need to know basis.

4.5 A record of any meetings with the whistleblower should be made either contemporaneously or as soon as possible afterwards. These notes must be kept securely.

4.6 No commitments should be made about the process or outcome of a whistleblowing investigation. However, the whistleblower should be reassured that their concerns will be taken seriously.

4.7 Any additional information you obtain should be shared with the people you have already notified (paragraphs 3.1 and 3.2 above) or with [Veritau], if the issue is to be referred to them.

5 Conducting an investigation

5.1 At the start of an investigation, the person looking into the issue should inform the whistleblower that they are investigating the matter.

5.2 Updates should be provided to the whistleblower during the investigation if this is possible. However, only appropriate information can be shared. Personal data about other people must not be shared. Nor can any

information that may prejudice the investigation. In some cases, it may be better to wait until the end of the investigation before sharing any details (although personal data cannot be shared at any point).

5.3 Notes should be made throughout the investigation about the action being taken and evidence collected. Conclusions should also be documented.

5.4 The investigator should consider whether any action to be taken during the investigation is likely to lead to the identity of the whistleblower becoming known. If it becomes apparent that the investigation cannot be pursued without the whistleblower's identity becoming known, then they should be made aware of this before further action is taken. The whistleblower's name should only be made known to other people on a need-to-know basis.

5.5 Investigations should be completed as quickly as possible. Where a whistleblowing investigation leads to other Council processes being considered or commencing (such as a pre-disciplinary investigation) then relevant officers should be made aware at an early stage.

5.6 At the conclusion of an investigation a report should be prepared setting out all of the evidence gathered and stating whether it confirms or contradicts the original issue raised. It should also set out the conclusions reached, and recommendations. The report should be shared with those notified of the issue originally (paragraphs 3.1 and 3.2 above). A copy should also be sent to [Veritau].

6 Special circumstances

Safeguarding concerns

6.1 If a concern raised includes issues relating to safeguarding, then the manager notified should ensure that it is raised immediately through normal Council safeguarding arrangements.

Anonymous concerns

6.2 If a concern has been made anonymously then it must still be treated as credible and dealt with through the procedure detailed in this guidance.

Negative treatment of the whistleblower

6.3 The Council will not tolerate any negative treatment of whistleblowers. If any manager becomes aware of any mistreatment of a whistleblower, they should report this to the Head of HR or relevant HR business partner as soon as possible. The Council may be in contravention of whistleblowing legislation if action is not taken to address this behaviour.

Vexatious or malicious reports

6.4 If a whistleblower acts in bad faith or raises malicious, vexatious, or knowingly untrue concerns then they may be subject to disciplinary action. If you have reasonable grounds to suspect that this may be the case, then the matter should be reported to the Head of HR or relevant HR business partner.

External disclosures

6.5 It is important to be supportive and encouraging to those raising a concern. However, if a worker indicates that they are considering taking their concerns outside of the Council, for example to the media or social networking sites, you should advise them of the following:

- You will not be able to support them if they take this action
- Their disclosure may not be covered by the whistleblowing policy and relevant legislation
- Their action may represent an unauthorised disclosure
- They could jeopardise any legal protection that they may have in law
- They could be subject to disciplinary action themselves.

6.6 If a whistleblower makes an external disclosure, then this should be reported to [Veritau] as soon as possible. Some types of disclosure are covered by legislation. However, consideration of whether the action taken is appropriate or not will need to be considered on a case by case basis.

Support

6.7 If you have any queries or issues about whistleblowing then you can seek further advice from [Veritau].

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 [insert job title] and can be contacted on [insert telephone]. If the MLRO is unavailable the Council has a Deputy MLRO. The Deputy MLRO is [insert job title] and can be contacted on [insert telephone].

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 [Monitoring Officer] and can be contacted on [insert telephone].

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 Policy and Procedure].

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 CLMCO 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 Report 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 XX XX 2022

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.

Concerns about a client

- 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.

Concerns about property transactions

- 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 [Monitoring Officer] 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