CEREDIGION COUNTY COUNCIL

Report to:	**Governance and Audit Committee**
Date of meeting:	**3 June 2021**
Title:	**Strategy on Counter-Fraud, Corruption and Bribery (to include Anti-Money Laundering)**
Purpose of the report:	**To provide Members with an update of the Strategy**
Cabinet Portfolio and Cabinet Member:	**Cllr Ray Quant MBE, Deputy Leader of the Council and Cabinet Member for Legal and Governance, People and Organisation, and Democratic Services**

Ceredigion County Council has a duty to the public to safeguard money that should be used in the public interest.

To help organisations achieve this by addressing their risks to fraud, CIPFA has produced a Code of Practice on Managing the Risk of Fraud and Corruption.

The Code states that an organisation needs a counter fraud strategy setting out its approach to managing risks and defining responsibilities for action.

This document is intended to serve this purpose, and applies to all employees, elected Members and Lay Members of the Council.

Recommendation(s):	**To Endorse the Strategy for presentation to Cabinet and Council for final approval**
Reasons for decision:	**To progress the publication and implementation of the Strategy**
Appendices:	**Strategy on Counter-Fraud, Corruption and Bribery (to include Anti-Money Laundering)**
Head of Service:	Elin Prysor Corporate Lead Officer Legal & Governance Services / Monitoring Officer
Reporting Officer:	Stephanie Land Apprentice Assistant Auditor
Date:	24 May 2021

Mae'r Strategaeth yma ar gael yn Gymraeg. This Strategy is available in Welsh.

Ceredigion County Council's Strategy on Countering Fraud, Corruption and Bribery (to include Anti-Money Laundering)

Cyngor Sir
CEREDIGION
County Council

Approved by Cabinet:

June 2021

Ceredigion County Council's Strategy on Countering Fraud, Corruption and Bribery (to include Anti-Money Laundering)

CONTENTS

1. Introduction

The CIPFA "Code of practice on managing the risk of fraud and corruption," states that an organisation needs a counter fraud strategy setting out its approach to managing risks and defining responsibilities for action. This document is intended to serve this purpose.

This policy applies to all employees, elected Members and Lay Members of the Council.

This policy sits alongside the Council's various other policies, including:

Officers:	Members:
Code of Conduct for Local Government Employees	Members Declaration and Registration of Hospitality and Interests Policy
Concerns and Complaints Policy	Code of Conduct for Members
Contract Procedure Rules	Member Handbook
Corporate Risk Register	Members' Allowances
Disciplinary Policy	
Domestic Violence Policy	**Members and Officers:**
Employees Declaration and Registration of Hospitality and Interests Policy	Data Protection and GDPR Policy
	Email Policy
	Information Security Policy
Pay Policy	Policy and Guidelines for Safeguarding Children and Adults at Risk
Political Restrictions Policy	
RIPA – Policy	Disclosure and Barring Service (DBS) Safe Recruitment Policy
Social Media Policy	
Suspension Policy and Procedures	Financial Regulations
Whistleblowing Policy	Modern Slavery Policy

The Council acknowledges its responsibilities for ensuring that the risks associated with fraud, corruption and bribery are managed effectively across all areas of the organisation.

The Council will have regard to various relevant legislation, Regulations, statutory guidance and codes of practice, including CIPFA's Code of Practice on Managing the Risk of Fraud and Corruption, Fighting Fraud and Corruption Locally, and Protecting the Public Purse.

Ethics

Employees working for the Council serve the whole Authority, are accountable to, and owe a duty to the Council. Employees must act in accordance with the Council's Code of Conduct for Local Government Employees. The Code of Conduct is underpinned by the ethical principles stated in '[The Seven Principles of Public Life]':

Selflessness | Integrity | Objectivity | Accountability

Openness | Honesty | Leadership

Identifying the Risk Areas: Definitions

Fraud	The Fraud Act 2006 defines the categories of fraud as: • false representation, • failing to disclose information, and • abuse of position. False representations include having an intention to make a gain for yourself or another, or exposing another to the risk of loss. CIPFA's publication "The Public Sector Internal Audit Standards" defines fraud in its Glossary as: *"Any illegal act characterised by deceit, concealment or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organisations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage".*
Corruption	HM Government's UK Anti-Corruption Plan states "There is no universally accepted definition of 'corruption'. A number of organisations, including 'Transparency International' define it as 'the abuse of entrusted power for private gain'. The World Bank defines a 'corrupt' practice as the 'offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party'".
Bribery	The Bribery Act 2010 sets out the offences of bribery as: • Bribing another person, and • offences relating to being bribed.

Bribery (continued)	A defence may be available if the conduct was necessary for specific reasons. Ministry of Justice guidance on the Bribery Act 2010 defines bribery as: *"Giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so".* Commercial organisations are liable for failure to demonstrate adequate procedures are in place to prevent these offences taking place.
Money Laundering	Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The Proceeds of Crime Act 2002 sets out the following principal offences: • Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327); • 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 (section 328); and • Acquiring, using or possessing criminal property (section 329). There are also two additional separate offences: • failure to disclose any of the primary offences (sections 330-332) and • tipping off (section 333). Potentially any person could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. Tipping off is where someone informs a person or people who are, or are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation. Specific defences may be available where there is reasonable excuse or where the disclosure is authorised. Whilst the risk to the Council of contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities: serious criminal sanctions may be imposed for breaches of the legislation. The key requirement on employees is to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO)

Risk areas

Asset Misappropriation	Occurs when those entrusted to manage the asses of an organization steals from it. Assets can include cash, cash equivalents, physical assets but also data or intellectual property	**False payroll records** **Purchasing cards**
Bribery & Corruption	The offer, promise or conferring of a financial or other advantage to another person with the intention to induce them to perform improperly a relevant function or activity or to reward for the same	**Manipulating tenders** **Securing deals**
Misstatement & Misreporting	Deliberate mis-recording, manipulation and reporting of elements of company performance or other factual information. This may be part of internal goals or contractual or legislative requirements	**Regulatory reporting**
Third Party Relationships	Heightened fraud risk exists in the operation of a range of third party relationships not under an organisation's direct control. Objectives, controls and ethical standards may not be aligned	**Overcharging** **Substitution of materials**
Information and Cyber Fraud	Occurs through sophisticated cyber hacking and exploits both physical and behavioural weaknesses to steal critical information and intellectual property	**Client identities** **Corporate identities**
Conflict of Interest	Occurs when employees are in a position to benefit themselves, or a third party, with whom there is an association including family members or friends	**Employee-owned supplier**

The Scale of Fraud in the Public Sector

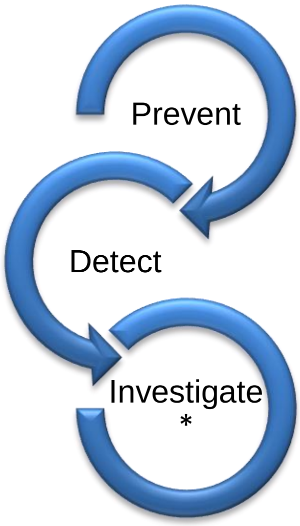
According to CIPFA, the following fraud types are most common:

- Housing
- Debt[1]
- Business Rates
- Council tax fraud
- Blue badge scheme
- Housing benefit
- Other fraud[2]

1 'Debt' is the avoidance of payment of a debit excluding Council Tax,

2 'Other fraud' includes social care, procurement, insurance, grant, pensions, investments, payroll and expenses.

Aims and objectives



Ceredigion County Council has a duty to the public to safeguard money that should be used in the public interest. Fraudulent behaviour at this scale threatens the Authority; therefore there is a high degree of commitment to ensure an effective strategy exists which is designed to protect, detect and investigate.

*Identify a clear path for investigating fraud, bribery and corruption, and any other malpractice to include money-laundering.

This will allow public money to be used on public services (boosting the economy, investing in people's future, enabling individual and family resilience and promoting environmental and community resilience) rather than being lost to fraud.

2. Culture, Responsibility and Prevention

The Council acknowledges the importance of promoting a culture that is resilient to the threats of fraud and corruption. The Council is determined that the culture and tone of the organisation should uphold honesty and integrity. The Council also acknowledges its responsibility for ensuring the management of its fraud and corruption risks and will be accountable for the actions it takes through its governance reports and procedures.

The Council maintains a specific goal of ensuring and maintaining its resilience to fraud and corruption, and explores opportunities for financial savings/prevention of financial loss from enhanced detection and prevention.

The Council's Financial Regulations (para 1.8.3) state that in "preventing fraud and corruption the Council will not tolerate fraud, corruption or any acts of malpractice in the administration of its responsibilities, whether from inside or outside the Council. The Council's expectation of propriety and accountability is that Members and employees at all levels will lead by example in ensuring adherence to legal requirements, rules, procedures and practices. The Council also expects that individuals and organisations (e.g. suppliers, contractors, service providers) with whom it comes into contact will act towards the Council with integrity and without thought or actions involving fraud and corruption".

Roles and Responsibilities

Role	Responsibility
Elected members	As elected representatives, all Members of the Authority have a duty to protect the Council and public money from any acts of fraud and corruption. This is done through existing practice, compliance with the Members' Code of Conduct, the Council's Constitution including Financial Regulations and Standing Orders and all relevant legislation.
Monitoring Officer	The Monitoring Officer is responsible for ensuring that all decisions made by the Authority are within the law. The Monitoring Officer also promotes and maintains high standards of conduct throughout the Authority by developing appropriate governance arrangements including codes of conduct and other standards and policies, together with appropriate reporting and enforcement. The Monitoring Officer is the Senior Responsible Officer (SRO) for the National Fraud Initiative (NFI). The SRO is responsible for ensuring that the Council meets the statutory requirements of the NFI. The Monitoring Officer is also the SRO for the National Anti-Fraud network (NAFN).

Section 151 Officer	The Corporate Lead Officer – Finance and Procurement has been designated with the statutory responsibilities as defined by s151 of the Local Government Act 1972 (the "Section 151 Officer") for the proper administration of its financial affairs. 'Proper administration' encompasses all aspects of local authority financial management including compliance with the statutory requirements for accounting and internal audit. Under these statutory responsibilities the Section 151 Officer contributes to the counter-fraud and corruption framework of the Authority. All suspected fraud or irregularities should be reported to the Corporate Lead Officer – Finance and Procurement – see Point 5 below. The Section 151 Officer is also the Money Laundering Reporting Officer (MLRO) – see Point 6 below.
Internal Audit (IA)	The Internal Audit Service protects organisational value by providing objective assurance, advice and insight. It evaluates and improves effectiveness of risk management, control and governance processes. This will help prevent the opportunity for fraud, although this is not its primary aim or responsibility. The IA Service may be required to undertake an investigation as a result of any irregularities – see Point 5 below. The Corporate Manager - Internal Audit provides an Annual Internal Audit Counter-Fraud Report to the Governance and Audit Committee. The report summarises the work internal audit have undertaken to counter fraud.
DWP's Fraud and Error Service	All powers held under the Social Security (Fraud) Act 1992 is now exercised by the DWP's Fraud and Error service, including the investigation of alleged housing benefit fraud. The Council has the power to investigate fraud relating to the Council Tax Reduction Scheme. These powers are contained within The Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (Wales) Regulations 2013.
External Auditors	The role of External Auditor is currently undertaken by Audit Wales (AW), who may, alternatively, appoint another approved body to undertake this role on its behalf. This role covers: • Auditing the Council's financial statements, • Considering the risks of material misstatements in the accounts due to fraud, • Certification of specified grants, • Assessing the Council's value for money arrangements, • Evaluating the Council's performance and improvement, and • Reviewing the Council's compliance with the sustainable development principle.

All employees	The Authority's employees are expected to abide by the Authority's 'Code of Conduct for Local Government Employees' as well as any code of conduct related to their personal professional qualifications. The Authority's Code includes expected standards and rules to include those relating to the declaration of personal interest, hospitality and gifts. All Members and employees of the Authority are required to declare any relevant interests and any offer of gifts or hospitality which is in any way related to the performance of their duties. Chief Officers are required to do this annually. They are also required to disclose any interests whether direct or indirect, in respect of the Authority's business eg close personal associations, contracts, directorships, members/clerkships of Town/community councils. The adequacy and appropriateness of the authority's internal controls, risk management and governance procedures are independently reviewed by both internal and external audit. Sound systems will allow for innovation but at the same time minimise the opportunity for fraud or any other misappropriation. Management should respond positively to internal and external audit recommendations if any weaknesses are found in their areas of responsibility, by implementing all actions required to ensure sufficient procedures are in place and are operating as expected. ICT systems used by the Council log usage of internet, e-mail, telephones and application systems down to individual PC / Laptop address and telephone number / extension number. All users of ICT and telephone systems are formally notified that these logs will be monitored from time to time and appropriate action taken for any misuse.
Recruitment	The Authority recognises that a preventative measure in the fight against fraud and corruption is to take effective steps at the recruitment stage to establish a previous record of prospective employees in terms of their propriety and integrity. Staff recruitment is therefore required to be in accordance with the Authority's Human Resource policies, to include the Disclosure and Barring Service / Safe Recruitment Policy.
Public	Although this policy is primarily aimed at those within the Council, it is also expected that the public would report any fraudulent behaviour so it can be investigated as necessary.

3. Detection and Investigation

The responsibility for the prevention and detection of any irregularities primarily rests with Leadership Group and managers.

The Council takes into account reports and recommendations by Audit Wales to tackle fraud effectively (e.g. 'Raising our Game' - Tackling Fraud in Wales and The National Fraud Initiative in Wales 2018-2020).

All managers produce business plans which include their business risks – fraud can be input as a risk if deemed appropriate with mitigating actions noted. Managers use the Risk Assessment Criteria to score the risk from low to critical. Managers score fraud risk based on likelihood (rare to certain) the impact of the risk (negligible to severe) on the Council's finances, service provision, health & safety, etc. If a risk is scored high enough it is added to the Council's Corporate Risk Register and reported regularly to Leadership Group and Governance and Audit Committee.

The Council will make use of joint working and/or partnership approaches and opportunities to managing its risks, where possible and appropriate.

The Council will promote both a proactive and reactive approach to detection and enforcement. Actions taken within the Council which can provide indicators of any fraudulent activity include:

Proactive

- Undertaking regular reviews and audits of systems where significant income and/or expenditure is involved, eg grants
- Ensuring frequent audits of the key controls present in the Authority's main financial systems, eg payroll, creditor payments, etc
- Using techniques such as data analysis to validate data where appropriate, eg IA's use of Active data software
- Publicising the Authority's Protection of Vulnerable Adults from Abuse document, and other relevant policies
- Making use of national and local initiatives to detect/prevent fraud eg the National Fraud Initiative exercise
- Publicising the Council's anti-fraud and corruption stance, and actions it takes against fraudsters
- Acting on notifications from CIPFA, NAFN (National anti-fraud network) and other external bodies which may alert the Council of any prevalent national / corporate fraud
- Ensuring the DWP's hotline number is easy to find
- Responding to any notifications received from other Local Authorities, network groups, etc citing any fraudulent attempts / incidents they have experienced / are made aware of

Reactive

Detecting fraud through data and intelligence analysis	Investigating fraud referrals	Implementing effective whistleblowing arrangements	Promoting the use of and applying sanctions, including internal disciplinary, regulatory and criminal
	Seeking redress, including the recovery of assets and money where possible		

Despite the best efforts of employees, fraud is often discovered as a result of chance or through a 'tip-off'. The Authority has systems in place to deal with such incidents correctly. This can be through the application of the Authority's Codes of Conduct, Financial Regulations, Complaints System, Protection of Vulnerable Adults from Abuse document and/or the Whistleblowing Policy, as well as this Strategy.

In accordance with the Authority's Financial Regulations (Point 1.8.3), all suspected fraud or irregularities should be reported to the Corporate Lead Officer – Finance and Procurement and/or Corporate Manager Internal Audit. It may also be reported to the Monitoring Officer, under the Whistleblowing Policy.

Pending investigation and reporting, the Corporate Lead Officer – Finance and Procurement will take all steps necessary to prevent further loss and to secure records and documentation against removal or alteration. The IA Service may be required to undertake a review to strengthen procedures and ensure no recurrence of such an incident.

The investigation will depend on the nature of the incident. An internal investigation may be required by an appointed Investigating Officer, which may lead to disciplinary action. Depending on the circumstances and available evidence, the investigation may be referred to the Police or another appropriate external body.

4. Deterrence and Awareness

When individuals are considering fraudulent behaviour they deliberate the reward against the risk of the activity. If fraudulent behaviour is often discovered and met with harsh penalties it increases the risk factor which in turn minimises the probability of the fraudulent act. Raising the awareness of the consequences of discovery therefore improves the effectiveness of deterrents such as:

Publicising the fact that the Authority acts robustly in relation to fraud, corruption and any malpractice, and states this at every appropriate opportunity. E.g. clauses in contracts, statements on claim forms, websites and publications.	Acting robustly and decisively when any malpractice is suspected and proven. E.g. terminating a contract, dismissing an employee, prosecuting defrauders.

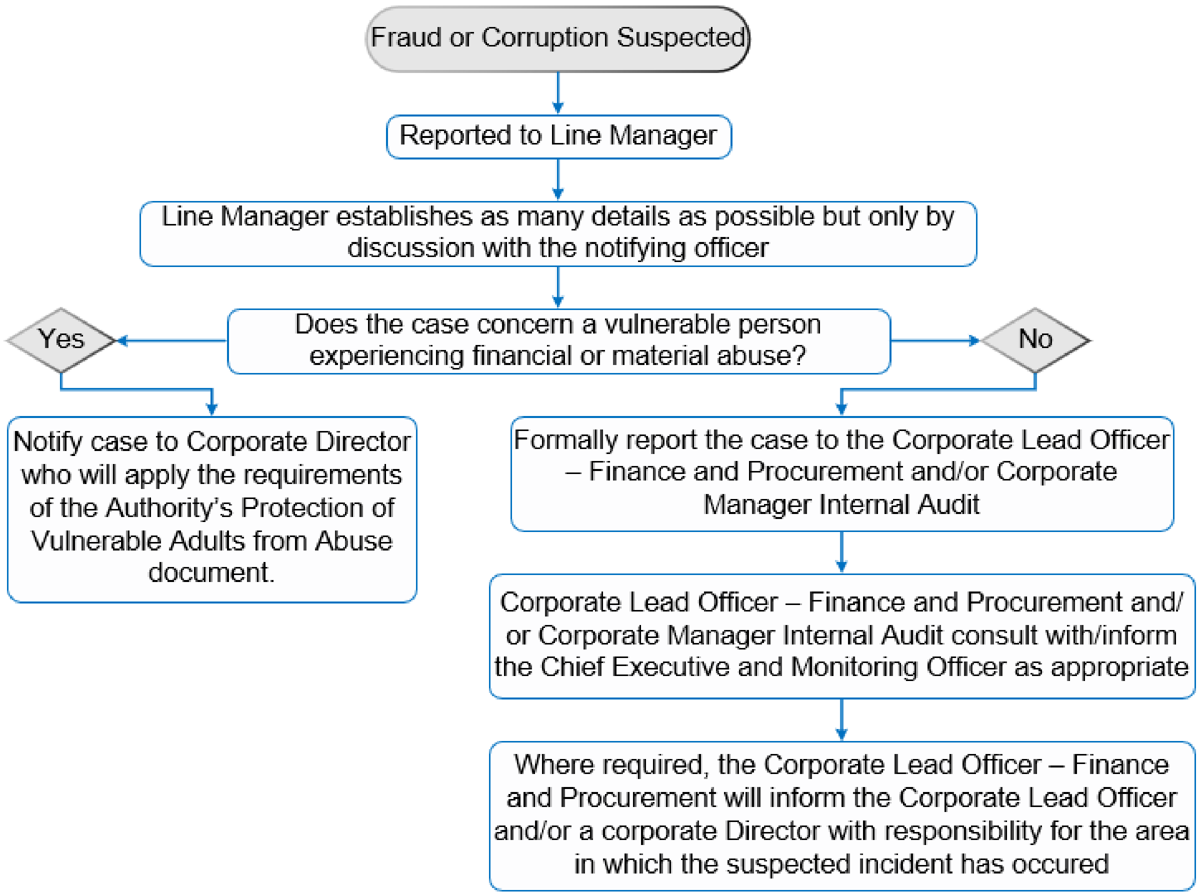
Taking action to effect the maximum recoveries for the Authority. E.g. through agreement, court action, penalties.

5. Fraud, Bribery and Corruption Response Plan

Determined perpetrators will always find a way around systems and procedures. Therefore, all officers and Members must be aware of what is required in the event of a suspected incident of fraud, bribery and corruption. It is vitally important that the plan is followed by all concerned in order to ensure that the situation is handled professionally and to safeguard against the case being compromised.

Notifying Suspected Fraud or Corruption

The Authority's staff and elected Members are positively encouraged to raise concerns regarding suspected fraud, bribery and corruption. They can do this in the knowledge that such concerns will be treated confidentially, as far as possible. A suspicion of wrongdoing must be reasonably held. The Authority will ensure that any allegation of any kind, including anonymous letters or telephone calls, will be looked at and thoroughly investigated in an appropriate manner. Reporting should be carried out as a matter of urgency. The normal route for expressing a concern should be via line managers.



On occasion where this is not appropriate, a route other than their normal line manager may be used to raise such concerns, such as via:

Corporate Lead Officer - Finance and Procurement/s151 Officer	Stephen Johnson 01970 633110 stephen.johnson@ceredigion.gov.uk
Chief Executive	Eifion Evans 01545 572021 eifion.evans@ceredigion.gov.uk
Corporate Manager - Internal Audit	Amanda Roberts 01970 633320 amanda.roberts@ceredigion.gov.uk
Corporate Lead Officer – Legal and Governance Services / Monitoring Officer	Elin Prysor 01545 572120 elin.prysor@ceredigion.gov.uk
Corporate Lead Officer – People and Organisation	Geraint Edwards 01545 572019 geraint.edwards2@ceredigion.gov.uk
Audit Wales	02920 320500 info@audit.wales
Other Corporate Lead Officers	See Council directory
Leader of the Council; Cabinet or other Members	See Council Website

Investigating Suspected Fraud, Bribery or Corruption

Once fraud is suspected, it is critical that any investigation is conducted in a professional manner aimed at ensuring that the current and future interests of both the Council and the suspected individual(s) are protected. The latter is equally important as a suspicion should not be seen as automatic guilt.

The Authority's IA Service has experience in fraud investigation. The Corporate Manager - Internal Audit and Audit Manager hold a CIPFA Certificate in Investigative Practice (CCIP). The Senior Auditor is an Accredited Counter Fraud Technician (ACFTech). In accordance with relevant legislation and the Council's Financial Regulations (Point 1.8.2) the IA Service has authority to:

a) Enter any Council premises or land at any reasonable times,
b) Access all assets, records, documents, correspondence and control systems relating to any financial or other transactions of the Council,
c) Require and receive any such information and explanation considered necessary

concerning any matter under consideration/examination,

d) Require any employee of the Council to account for cash, stores or any other Council property under his or her control, and

e) Have access to records belonging to third parties, such as contractors or partnership agencies, according to the relevant contractual terms.

It may therefore be appropriate to request the IA Service to undertake the investigation. However, if the allegations are of a professional or very specialist malpractice nature, the Corporate Lead Officer – Finance and Procurement may have to appoint another expert as the Investigating Officer. The Council periodically trains a 'pool' of internal investigators across all services; and certain enforcement staff have PACE training.

Reporting Arrangements

As soon as the initial "detection" stage of the investigation has been completed a written confidential Interim Report should be made by the Investigating Officer in accordance with the agreed reporting process.

The Interim Report should set out the findings to date and the interim conclusions drawn from those findings. This will help the Corporate Lead Officer – Finance and Procurement, Monitoring Officer and Corporate Lead Officer / Corporate Director with responsibility for the area investigated decide whether the investigation should continue to the next level.

If it is to proceed, the Chief Executive, the Chair of Governance and Audit Committee and the Authority's external auditors need to be made aware of the incident. A Final Report will be issued as soon as possible after the completion of all necessary investigatory work.

The format of the Final Report will not always be the same as each case is unique, but will frequently set out:

- How the investigation arose,
- Who the suspects are,
- Their position in the Council and their responsibilities,
- How the investigation was undertaken,
- The facts and evidence which were identified, and (where appropriate),
- Summary of findings and recommendations.

Any system weaknesses identified during the investigation will normally be reported separately in an internal audit report.

The Final Report will supersede all other reports and be the definitive document on which management (in a disciplinary situation) and possibly the police (in a criminal situation) will base their initial decisions.

All reports must be substantiated by the strongest evidence and avoid contents that could be considered to be defamatory in the event of the report being made public.

Defamation in law is defined as: “the publication of a statement which tends to lower a person in the estimation of right-thinking members of society generally or which tends to make them shun or avoid that person”. [Winfield]

Liaison with the Police

Initial contact with the Police should only be undertaken following discussion between the Investigating Officer, Corporate Lead Officer – Finance and Procurement, Chief Executive and Monitoring Officer, who will consider whether the matter should be referred for further investigation.

Where a case involves a vulnerable person, the decision will be made by the statutory Director of Social Services, in consultation with the relevant Corporate Director and/or the Safeguarding Team.

It is the policy of the Police to welcome early notification of suspected fraud. The matter will be considered for referral by the Police to the Crown Prosecution Service for a decision as to whether the suspect should be charged with any criminal offence.

If the Police decide that a formal investigation is necessary, all staff are expected and required to co-operate fully with any subsequent requests or recommendations. All contact with the Police following their initial involvement will usually be via the Investigating Officer.

Where the Police decide to formally investigate, this will not, if at all possible, prejudice any internal disciplinary procedures; these should continue as normal. However, the internal investigation and the Police investigation should, wherever and whenever possible be co-ordinated to make maximum use of resources and information.

The identity of the notifying employee will be protected as far as possible, in accordance with the Whistleblowing policy.

Disciplinary action

The Authority will deal swiftly and thoroughly with any incidents of malpractice. Employees will face disciplinary or other action in accordance with the Council’s HR Policies.

Disciplinary or other action will be taken in addition to, or instead of criminal proceedings (this depends on the circumstances of each individual case), in keeping with the Council's Disciplinary Policy.

Resources

The Council will:

- Make an annual assessment of whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk, in its annual response to the external auditor regarding matters in relation to fraud.
- Make use of an appropriate mix of experienced and skilled staff.
- Grant unhindered access to its employees, information and other resources as required for investigation purposes.
- Make use of joint working and partnership facilities, as well as data and intelligence sharing to support counter fraud activity.

6. Anti-Money Laundering

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 came into force on 10 January 2020 and sets out the amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The 2019 Regulations implement the EU's 5th Directive on Money Laundering.

The Regulations apply to "relevant persons" acting in the course of business carried out by them in the UK. Relevant persons are now obliged to adopt a more risk-based approach towards anti-money laundering, in particular in how they conduct due diligence.

Not all of the Council's business is relevant for the purposes of the legislation; however, the safest way to ensure compliance with the law is to apply them to all areas of work.

All members of staff are therefore required to comply with the reporting procedure set out in the policy.

The obligations on the Council are to:

- Appoint a Money Laundering Reporting Officer (MLRO) to receive disclosures from employees of money laundering activity;
- Implement a procedure to enable the reporting of suspicions of money laundering;
- Maintain client identification procedures in certain circumstances;
- Maintain record keeping procedures; and

- Conduct a money laundering and terrorist financing risk assessment and adopt appropriate internal controls.

The Money Laundering Reporting Officer (MLRO)

The officer nominated to receive disclosures about money laundering activity within the Council is the Corporate Lead Officer – Finance and Procurement (Section 151 Officer) who can be contacted as follows:

Stephen Johnson
Finance and Procurement
Canolfan Rheidol
Rhodfa Padarn
Llanbadarn Fawr
SY23 3UE
Telephone: 01970 633110

Identification of potential money laundering situations

The following may raise employees' suspicions, and should be reported immediately to the MLRO**:**

- A transaction involving a large amount of cash,
- Making a cash payment that later requires a refund,
- Secretive customer, eg refusal to provide requested information without a reasonable explanation,
- Concerns about the location or identity of a customer,
- Unnecessary routing or receipt of funds from third parties or through third party accounts,
- Involvement of an unconnected third party without a legitimate reason,
- No obvious legitimate source of funds,
- Weak internal accounting controls or business records,
- Previous transaction for the same customer that should have been or has been reported to the MLRO,
- Individuals or companies that have funds even though they are insolvent,
- Lack of traceability of the people involved.

Cash payments

No payment to the Council exceeding £5,000 will be accepted in cash (including notes, coins or travellers cheques in any currency) without the approval of the MLRO.

Reporting to the Money Laundering Reporting Officer (MLRO)

If employees are asked to collect a payment exceeding £5,000 in cash they must provide details to the MLRO using the pro-forma report attached at Appendix 1, so that precautionary checks can be performed. The report must include as much detail as possible. This does not mean that transactions below this sum should never raise suspicions. Professional alertness should be exercised at all times, taking into account the factors above.

If an employee has reasonable grounds to suspect money laundering activities in respect of a lesser sum, the matter should be reported to the MLRO in the same way.

The employee must then follow all directions from the MLRO and must not make any further enquiries themselves into the matter. Additionally they must not take any further steps in the transaction without authorisation from the MLRO.

To prevent the suspect becoming aware of the suspicion the employee must not discuss the matter with others or note on a file that a report has been made to the MLRO.

The MLRO will promptly evaluate the circumstances of each case and make a decision as whether to report the matter to the National Crime Agency (NCA) via its website or by its 24 hour phone line: 0370 496 7622.

Where the MLRO concludes that there is no reasonable grounds to suspect money laundering then he shall mark the report accordingly and give his consent for any ongoing or imminent transactions to proceed.

It is a criminal offence if the MLRO knows or suspects, through a disclosure being made to him, that another person is engaged in money laundering and he does not disclose this as soon as possible to the NCA.

All reports made must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

Customer Due Diligence

Regulation 28 Customer due diligence measures - The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Where the Council is carrying out certain regulated business (accountancy, audit and tax services and legal services, relating to financial, company or property transactions), and part of this:

- Forms an ongoing business relationship with a client,

- Undertakes a one off or occasional transaction amounting to €15,000 or more whether carried out as a single transaction or several linked ones, or
- The officer suspects money laundering or terrorist financing:

then the customer due diligence procedure below must be followed before any business is undertaken for that client.

Customer due diligence means:

- Identifying the customer and verifying the customer's identity on the basis of information obtained from a reliable and independent source eg conducting a search at Companies House.
- Obtaining information on the purpose and intended nature of the business relationship.

Where the "relevant business" is being provided to another UK public sector body then written, signed instructions on the body's headed paper should be obtained prior to the transaction being completed.

The requirement for customer due diligence applies immediately for new customers and should be considered on a risk sensitive basis for existing customers. Customer due diligence means that the Council must know its clients and understand their businesses in order to determine whether there is suspicious activity that should be reported.

The Regulations require that the Council identifies its customers and verifies that identity on the basis of documents, data or information obtained from a reliable source. Where there is a beneficial owner who is not the customer, then the Council must identify that person and verify the identity. Where the beneficial owner is a trust or similar then the Council must understand the nature of the control structure of that trust. Finally the Council must obtain information on the purpose and intended nature of the business relationship. The Regulations stipulate the need for the Council to consider both customer and geographical risk factors in deciding what due diligence is appropriate.

These checks must generally be undertaken by the Council before it establishes a business relationship or carries out an occasional transaction, or if it suspects money laundering or terrorist funding or doubts the veracity of any information obtained for the purposes of identification or verification. However, the Council is not required to undertake these checks if its customer is another public authority, unless it suspects money laundering or terrorist funding.

The Council is also obliged to maintain ongoing monitoring of its business relationships which means it must scrutinise transactions throughout the course of the relationship to ensure that the transactions are consistent with the Council's knowledge of the customer and keep the information about the customer up-to-date.

Enhanced Customer Due Diligence and Ongoing Monitoring

Regulation 33 Obligation to apply enhanced customer due diligence - The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

In certain circumstances it will be necessary to undertake what is noted in the Regulations as Enhanced Customer Due Diligence. In summary, this will be necessary where:

- The customer has not been physically present for identification purposes; or
- In any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

Where this applies, the Council will need to take adequate measures to compensate for the higher risk. For example, this will mean ensuring that the customer's identity is established by additional documents, data or information.

In this instance, the Regulations impose a special obligation to carry out ongoing monitoring of its business relationships which means it must scrutinise transactions undertaken throughout the course of the relationship to ensure that these transactions are consistent with the Council's knowledge of the customer, his/her business and risk profile; and keep documents, data or information obtained for the purpose of applying Customer Due Diligence measures up-to-date.

Redress

The Council will endeavour to seek redress, including the recovery of assets and money where possible. This may include recovery proceedings action pursuant to the Proceeds of Crime Act 2002.

Record Keeping

Where the "relevant business" is carried out then the customer due diligence identification evidence and the details of the relevant transaction(s) for that client must be retained for at least five years.

7. Training

The continuing success of the Authority's Counter Fraud, Corruption and Bribery and Anti-Money Laundering arrangements will be partly reliant on the effectiveness of staff training and responsiveness throughout the Authority. Managers should therefore ensure that adequate and appropriate training and development is provided for their staff, especially those involved in the internal control system.

The Money Laundering Regulations require that relevant staff are made aware of the law relating to money laundering and terrorist financing, and to the legal requirements of the data protection act, and are regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.

The MLRO should maintain a written record of the measures taken and training provided.

A series of webinars are due to be provided on Cyber Crime to Council employees from April 2021 onwards; and a training module on Ethics & Fraud is due to be presented to the Council's Corporate Workshop on 28th May 2021. The Council's Corporate Workshop will be used as an opportunity to raise awareness of this Strategy.

MBL Seminars Ltd, which the Council subscribes to, offers seminars on Anti-Money Laundering.

Managers ensure that staff are made aware of any other training opportunities.

8. Conclusion

The Authority has in place a clear network of systems and procedures to fight against fraud and corruption that is available to all stakeholders. It is essential that these arrangements keep pace with any future developments in both preventative and detection techniques.

Appendix 1

CONFIDENTIAL

Report to Money Laundering Reporting Officer

Re: Suspected money laundering activity

From: ____ (employee name)

Service: ____________________________________ Ext No: __________

Details of suspected offence:

Name(s) and address(es) of person(s) involved: (if a company / public body please include details re nature of business)

Nature, value and timing of activity involved: (please include full details eg what, when, where, how; attach a separate sheet if necessary

Nature of suspicions regarding such activity: Please attach a separate sheet if necessary

Signed: _________________________________ Dated: ________________

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which carries a maximum penalty of 5 years' imprisonment.