

COUNTER FRAUD PROTOCOL

(To include Bribery, Corruption & Anti-Money Laundering)



Cyngor Sir
CEREDIGION
County Council

Protocol & Strategy approved by Council: 07/10/2025

Document Owner: Corporate Lead Officer, Finance &
Procurement

Review Date: 7th October 2028

Contents

COUNTER FRAUD PROTOCOL	3
Foreword	3
Purpose	3
Fraud Risks	5
Detection & Reporting	6
Roles and Responsibilities	7
Definitions	10
FRAUD RESPONSE PLAN	12
Immediate Actions	12
Investigating Suspected Fraud, Bribery or Corruption	13
Resources	13
Liaison with Police	14
Reporting Fraud Investigations	14
Disciplinary Action	15
Review & Continuous Improvement	16
FRAUD RESPONSE PLAN FLOWCHART	17
ANTI-MONEY LAUNDERING POLICY	18
Report to Money Laundering Reporting Officer	23

COUNTER FRAUD PROTOCOL

Foreword

Fraud is the most commonly experienced crime in the UK, accounting for around 40% of all crime. Audit Wales noted in their National Fraud Initiative 2024/25 work programme 'in the public sector, it has been estimated that in 2021-22, the level of gross fraud and error was between £39.8 billion and £58.5 billion, outside of COVID19 specific schemes'.

The Council is funded by public money, through council tax, business rates and other sources. Fraud against the council is essentially theft of this money, and the council takes its role as a guardian of these public funds seriously. For these reasons, the council will not tolerate any fraud, bribery or corruption and has a zero-tolerance approach.

This protocol supports the Council's Counter Fraud Strategy and includes the Council's Fraud Response Plan, which guides officers on action to take in reporting suspicious activity.

Purpose

The purpose of this protocol is to provide a framework for managing fraud, bribery, and corruption risks.

Ceredigion County Council is committed to safeguarding public money and ensuring that the citizens of Ceredigion have confidence that the Council operates in an open, honest, and fair way.

It is essential to remain vigilant against the risk of fraud and corruption. Fraud and corruption can be a factor in preventing the Council from achieving its goals and serving the residents of Ceredigion to the best of its ability.

Legislation

The Council has considered the 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.

Application

This protocol and the accompanying Counter Fraud Strategy applies to:

- All Ceredigion County Council employees (including volunteers and agency staff)
- Councillors and Lay Members

- Ceredigion County Council's Schools
- Suppliers, contractors, and consultants, and
- Members of the Public

This protocol sits alongside the Council's various other policies, including but not limited to:



The Council acknowledges its responsibilities for ensuring that the risks associated with financial crimes are managed effectively across all areas of the organisation.

Council employees and Elected Members must act in accordance with the Council's Codes of Conduct for Local Government Employees and the Code of Conduct for Members.

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".

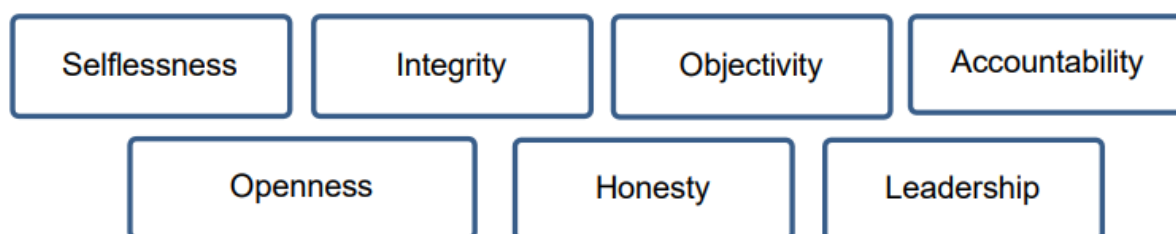
Culture

Ceredigion County Council is committed to creating and promoting a culture that is resilient to the threats of fraud and corruption as well as upholding our core values integrity, honesty, openness and accountability.

Ceredigion County Council promotes a zero-tolerance culture and attitude to fraud,

bribery, and corruption and is committed to preventing, detecting and investigating all occurrences where crime is suspected. This will allow public money to be used on public services to deliver the Council's Corporate Strategy.

Values matter to us. They set out our expectations for ourselves, each other and the way we conduct business with organisations that we work with on your behalf. Our organisational values are underpinned by the ethical principles stated in the '[Seven Principles of Public Life](#)':



These values provide a foundation for everyone attached to our organisation to be accountable in delivering on our vision to deliver:

‘Value for money, sustainable bilingual public services, that support a strong economy and healthy environment, while promoting well-being in our people and our communities’.

By protecting public funds from fraud, the Council can continue to deliver its wellbeing objectives, which are:

- Boosting the economy, supporting businesses and enabling employment
- Creating caring and healthy communities
- Providing the best start in life and enabling learning at all ages
- Creating sustainable, green and well-connected communities

Preventing and detecting financial crimes against the Council is the responsibility of Elected and Lay members, internal employees, external partners, contractors and the members of the public. All have a duty to report any suspicion of fraudulent activity.

Fraud Risks

Not all instances of fraud, corruption or bribery are associated with a particular service in the Council. Anyone can come across fraud, so it is important to be vigilant and aware of the counter fraud risks and how to report suspected fraud.

An annual Fraud Risk Assessment is coordinated by the Corporate Manager – Internal Audit. The risk assessment is sent to all Corporate Managers to obtain and collate fraud risks and monitor how fraud risks are mitigated and managed by services, including

existing counter fraud internal controls. The results of the annual Fraud Risk Assessment forms the basis of the Council's annual Fraud Assessment and feeds into the Fraud Risk Register.

The Fraud Risk Register is monitored by the Corporate Manager – Internal Audit and scores individual risks of fraud. The overall assessment of fraud risk is reported as a service risk by the Corporate Lead Officer – Finance & Procurement.

However, the list below sets out the common high-risk areas of fraud in the public sector.

- Council Tax
- Social Care
- Grants
- Payroll & Human Resources
- Business Rates
- Housing
- Procurement & Commissioning
- Blue Badges

Detection & Reporting

Where fraud is suspected or detected it is vitally important to ensure that information and evidence is contained and remains unaltered.

Employees or managers must NOT do the following, as it may affect any further investigation:

- alter, remove or delete any documentation or evidence
- attempt to investigate any incidents of suspected fraud and/or corruption
- discuss the matter with any suspected individual or colleagues.

In accordance with the Authority's Financial Regulations (Point 1.8.3), all instances of suspected or confirmed fraud must be notified to the Corporate Lead Officer, Finance & Procurement and the Corporate Manager – Internal Audit. This can be done directly using the details above or by emailing fraud@ceredigion.gov.uk.

Any allegation of fraud 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 in the first instance, where appropriate. However, in instances where reporting to their normal line manager is not appropriate, other key routes may be used to raise such concerns.

The following Reporting Officers can be contacted through telephoning Clic at 01545 570881 or emailing clic@ceredigion.gov.uk:

- Corporate Lead Officer – Finance & Procurement (Section 151 Officer)
- Corporate Manager – Internal Audit
- Chief Executive
- Corporate Lead Officer – Legal & Governance (Monitoring Officer)
- Corporate Lead Officer – People & Organisation
- Leader of the Council; Cabinet or other Members
- Audit Wales info@audit.wales

Roles and Responsibilities

Whilst in practice, countering fraud and corruption is the responsibility of all Council employees and stakeholders, the Council recognises that managing fraud and corruption is the responsibility of those charged with governance. Key roles and responsibilities are delegated to key officers and committees, as set out below.

All employees

Employees play various crucial roles in the Council's counter fraud efforts. They are responsible for implementing and maintaining controls to prevent fraud. This includes understanding fraud risks, recognising prevention opportunities, and collaborating with others to design, implement, and evaluate controls.

Employees should continuously monitor and improve fraud prevention and detection measures to adapt to evolving fraud risks and ensure the organisation remains resilient against fraud. 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 procedures are in place and are operating as expected.

When fraud is detected, employees must respond appropriately by reporting concerns in accordance with the Fraud Response Plan within the Counter Fraud Protocol.

Council 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 Code includes expected standards and rules to include those relating to the declaration of personal interest, hospitality and gifts. All employees must ensure they complete the relevant fraud awareness training appropriate to their role (the Ethics and Fraud Awareness eLearning module is mandatory for all Council employees) and promote a culture of fraud awareness and ethical behaviour.

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.

Section 151 Officer

The Corporate Lead Officer—Finance and Procurement has been designated with the statutory responsibilities as defined by Section 151 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 Council by:

- Ensuring effective procedures are in place to investigate promptly any suspected fraud, irregularity or malpractice, carrying out surveillance where necessary (subject to proper authorisation).
- Developing and maintaining an Anti-Fraud and Corruption Strategy policy document.
- Reporting on any fraud and/or corruption in accordance with the Council’s Anti-Fraud and Corruption Strategy

All suspected fraud or irregularities must be reported to the Corporate Lead Officer—Finance and Procurement. The Section 151 Officer is also the Money Laundering Reporting Officer (MLRO).

Governance & Audit Committee

The Governance & Audit Committee has oversight of the effectiveness of the Council’s counter-fraud framework and receives periodic assurance updates. They ensure, through assurances they receive, that the Council’s systems of governance and internal control are effective for managing the authority’s exposure to the risks of fraud and corruption. Their responsibilities also include reviewing the assessment of fraud risks and monitoring the Counter-Fraud Strategy, actions, and resources.

Monitoring Officer

The Monitoring Officer is responsible for ensuring that all decisions made by the Authority are within the law. The Monitoring Officer 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), 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).

Chief Officers

Chief Officers are responsible for maintaining adequate and effective counter fraud internal control arrangements.

Additionally, Chief Officers must notify the Chief Finance Officer and/or the Corporate Manager – Internal Audit immediately of any suspected fraud, theft, irregularity, improper use or misappropriation of the Council's property or resources. Pending investigation and reporting, they should take all necessary steps to prevent further loss and to secure records and documentation against removal or alteration.

Internal Audit

The Internal Audit function strengthens the organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

It enhances the organization's successful achievement of its objectives, governance, risk management, and control processes, which will help prevent the opportunity for fraud, although this is not its primary aim or responsibility.

The IA Service may be required to undertake investigations as a result of any irregularities. The Corporate Manager—Internal Audit produces an Annual Internal Audit Counter-Fraud Report to summarise the work Internal Audit have undertaken to counter fraud.

Elected Members

As elected representatives, all Members of the Authority have a duty to protect public money from any acts of fraud and corruption. This is done through compliance with the Members Code of Conduct, the Council's Constitution including Financial Regulations and Standing Orders and all relevant legislation.

Department of Work and Pensions 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 specific 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 principal.

The Public

Although this protocol document 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.

Definitions

Term	Definition
Fraud	Fraud is a criminal activity where deception is used for gain or to cause a loss. The Fraud Act 2006 introduces three ways of committing fraud: • Fraud by false representation; • Fraud by failure to disclose information when there is a legal duty to do so; and • Fraud by abuse of position.
Corruption	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. 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".
Money Laundering	Money laundering is the term used for a number of offences involving the proceeds of crime of 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, do nothing about it or tip off. 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).
--	---

FRAUD 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.

The purpose of this Fraud Response Plan is to provide a structured response to effectively handle and mitigate the impact of fraudulent activities suspected or confirmed fraud incidents.

It is vitally important that the Fraud Response Plan is followed by all concerned to ensure that the situation is handled professionally and to safeguard against the case being compromised. A flowchart of the Fraud Response Plan can be found in Appendix I.

The Fraud Response Plan must be followed when reports of fraud have been received in the following areas (this is not an exhaustive list):

- Internal Fraud e.g. payroll fraud, misappropriation.
- External Fraud e.g. supplier fraud, housing, grants, cyber fraud.
- Corruption
- Bribery

Immediate Actions

Once suspected fraud is detected and reported to officers set out within the Counter Fraud Strategy, the following steps must be undertaken immediately:

- Record key facts e.g. dates, times, locations and names and keep this information secure.
- Secure evidence and documentation – to maintain the integrity of evidence documents must not be deleted or altered in any way.
- Council officers MUST NOT attempt to investigate themselves or discuss with anyone other than the Reporting Officers.
- Notify Internal Audit (if not directly reported to them) of the suspected fraud so that all reports of fraud and investigations can be recorded in the Council's log of Fraud cases.

Upon discussion with the Corporate Lead Officer – Finance & Procurement, it may be necessary to action additional measures to prevent any further losses until any investigation concludes such as:

- Notifying key personnel and companies e.g. card companies, banks.
- Freezing accounts.
- Disabling access, or
- Suspending employees.

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 interest of both the Council and the suspected individuals are protected. The latter is equally important as a suspicion should not be seen as automatic guilt.

An Investigation Team will be formed dependent on the nature of the suspected fraud and expertise required and may include key officers from Legal Services, Finance & Procurement, Internal Audit, ICT & Digital and Human Resources.

The Authority's Internal Audit Service has experience in fraud investigations. The Corporate Manager—Internal Audit and Senior Auditor are Accredited Counter Fraud Technicians (ACFTech) whilst the Audit Manager holds a CIPFA Certificate in Investigative Practice (CCIP). In accordance with relevant legislation and the Council's Financial Regulations (point 1.8.2) the Internal Audit Service has authority to:

- Enter any Council premises or land at any reasonable time
- Access all assets, records, documents, correspondence, and control systems relating to any financial or other transactions of the Council
- Require and receive any such information and explanation considered necessary concerning any matter under consideration/examination
- Require any employee of the Council to account for cash, stores, or any other Council property under their control, and
- 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 Internal Audit 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 decide 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.

The scope of the investigation and reporting process must be agreed between the Investigation Team before commencing the fraud investigation. All investigatory steps will be consistent with relevant HR policies and employment law to protect fairness.

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.

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 (e.g. ICT, Internal Audit, Data Protection Officer and other trained professionals)
- Make use of appropriate resources including data analytic software
- 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

Liaison with 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 Police decide to formally investigate, this will not, if at all possible, prejudice any internal disciplinary procedures; these 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.

Reporting Fraud Investigations

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

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]

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. Internal Audit may be required to undertake a review to strengthen procedures and prevent recurrence of such an incident.

Fraud investigations will be reported to the Governance & Audit Committee and Leadership Group as part of regular Internal Audit reports.

Disciplinary Action

The Authority will deal swiftly and thoroughly with any incidents of malpractice. Employees may 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.

Redress & Recovery

The Council will always seek to pursue appropriate redress and recovery where error or fraud has been identified. The Council will actively pursue the recovery of any assets or funds lost due to fraud or error.

As and when appropriate, instances of proven fraud will be publicised by the Council.

Review & Continuous Improvement

Any system weaknesses identified during the investigation will normally be reported separately in an internal audit report. Internal Audit will work with services to suggest areas to strengthen existing internal controls to reduce the risk of fraud reoccurring.

The implementation of any agreed actions as a result of an investigation will be tracked by Internal Audit. Management Actions agreed will be reported to Leadership Group and the Governance & Audit Committee for corporate oversight and to monitor improvement action implemented by management.

Additionally, any training requirements identified as a result of a fraud investigation will be followed up.

FRAUD RESPONSE PLAN FLOWCHART

If you have a suspicion of fraud, corruption or bribery

YOU MUST REPORT AS
SOON AS POSSIBLE TO
fraud@ceredigion.gov.uk

DO:

- Act quickly!
- Record key facts e.g. dates & times, names, locations.
- Secure relevant documentation.

DO NOT:

- Ignore your concerns.
- Alter or delete any documentation.
- Discuss with anyone other than Reporting Officers.
- Investigate yourself.

Report ALL suspicion of fraud / corruption / bribery immediately to one of the below:

- Corporate Lead Officer – Finance & Procurement (Section 151 Officer)
- Corporate Manager – Internal Audit
- Corporate Lead Officer – Legal & Governance (Monitoring Officer)
- Or another approved Reporting Officer set out in the Counter Fraud Strategy

What to expect:

- Your concerns will be considered by relevant Reporting Officers
- Preventative measures may be taken to minimise further losses
- Investigating Officers will be appointed
- You may be asked to discuss your concerns further
- You will be asked to share relevant documentation
- Regular updates and outcomes of the investigation will be shared with key officers
- Where required, appropriate action will be taken including publicising proven fraud.

Criminal

- IA / External Investigating Officer
- Evidential package
- Refer to Police

Disciplinary

- HR investigates or refers to external investigator
- Outcome referred to HR

Redress

- Outcome referred to CLO F&P
- Recovery – invoice issued or civil action

No Further Action

- If no case to answer – record as closed

ANTI-MONEY LAUNDERING POLICY

Position Statement

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 came into force on 10 January 2020 and sets out the amendment to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The 2019 Regulation 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 control.

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:

Ceredigion County Council Offices
Penmorfa
Aberaeron
SA46 0PA
Telephone: 01545 570881

Role and Responsibilities of the Money Laundering Reporting Officer

The MLRO has a crucial role in preventing and detecting money laundering. They are responsible for ensuring the Council complies with relevant legislation and

regulations, including reporting suspicious activities to the National Crime Agency (NCA). The MLRO's duties include overseeing anti-money laundering policies, ensuring relevant staff receive anti-money laundering training, and acting as the point of contact for Anti Money Laundering related matters.

Identification of potential money laundering situations

The following may raise employee's 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 e.g. 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 traveller's 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 I, 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 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 are no reasonable grounds to suspect money laundering then he will 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 them, that another person is engaged in money laundering and 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: Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended provides the basis for customer due diligence.

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 customers identity on the basis of information obtained from a reliable and independent source e.g. conducting a search at Companies House as well as verify the directors and articles of association'.

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 business 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

The relevant regulation regarding enhanced customer due diligence is Regulation 33 'Obligation to apply enhanced customer due diligence' in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

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 terrorists financing.

Where this applies, the Council will need to take adequate additional steps 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, their

business and risk profile; and keep documents, data or information obtained for the purpose of applying Customer Due Diligence measures up-to-date.

Additional steps include:

- a) obtaining additional information on the customer and on the customer's beneficial owner;
- (b) obtaining additional information on the intended nature of the business relationship;
- (c) obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
- (d) obtaining information on the reasons for the transactions;
- (e) obtaining the approval of senior management for establishing or continuing the business relationship;
- (f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

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 transactions for that client must be retained for at least five years.

Training

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. Managers ensure that staff are made aware of training opportunities. The MLRO should maintain a written record of the measures taken and training provided.

Report to Money Laundering Reporting Officer

CONFIDENTIAL

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.