

Counter-fraud and Corruption

Policy Statement and Strategy
2020-2023

June 2020

Contents

Counter Fraud and Corruption Policy Statement	3
Anti Fraud and Corruption Strategy	4
What is Fraud?	4
What is Corruption?	4
What is Bribery?	4
What is Theft?	4
What is Money Laundering?	4
Scope.....	6
What are the aims and objectives of the strategy?	6
What is SDC’s approach to Countering Fraud?	8
Managing the Risk of Fraud and Corruption	8
Fighting Fraud and Corruption Locally: Acknowledge, Prevent, Pursue	10
Responsibilities	12
Reporting, Advice and Support this section to be discussed with karen	14
Employees.....	14
Members of the Public / External Providers / Partners	15
Further Information	16
Strategy Review.....	17
Appendix 1 Key fraud indicators	18
Appendix 2 Types of Fraud.....	19
Appendix 3 SDC’s Fraud Response Plan to discuss	20
Appendix 4 Anti-Bribery Policy.....	21
Appendix 5 Anti-Money Laundering Policy	23

Counter Fraud and Corruption Policy Statement

The Annual Fraud Indicator produced by Crowe Clark Whitehill estimated that the fraud threat to local authorities may be as high as £7.8bn in 2017 of which procurement fraud was estimated as £4.3bn. This study estimated that the total threat faced by the public sector was £40.4bn.

The Government’s Economic Crime Plan 2019 states that the number of fraud offences rose by 12% during 2018 to 3.6 million – constituting a third of all crimes in the UK.

This statement sets out the Council’s policy in relation to fraud and corruption. It has the full support of the Council, the Council’s Audit and Standards Committee and Corporate Team.

The Council takes its responsibilities to protect the public purse very seriously and is fully committed to the highest ethical standards, in order to ensure the proper use and protection of public funds and assets.

The Council will not tolerate fraud or corruption by its councillors, employees, suppliers, contractors, partners or service users and will take all necessary steps to investigate all allegations of fraud, or corruption and pursue sanctions available in each case, including removal from office, disciplinary action, dismissal and/or prosecution. The required ethical standards are included in both our Members Code of Conduct and Employees Code of Conduct.

To fulfil the Council’s Strategy, we need to maximise the financial resources available to us. In order to do this, we aim to reduce fraud and misappropriation to zero.

This policy statement is underpinned by a Counter-Fraud Fraud and Corruption Strategy, which sets out the key responsibilities with regard to fraud prevention, what to do if fraud is suspected and the action that will be taken by management.

The strategy is based upon five key themes: **Govern, Acknowledge, Prevent, Pursue and Protect** and adheres to Fighting Fraud and Corruption Locally, A strategy for the 2020s (FFCL), which is supported by the Chartered Institute of Public Finance and Accountancy (CIPFA) Counter Fraud Centre.



Counter-Fraud and Corruption Strategy

Stroud District Council has a **zero tolerance** stance to all forms of fraud, bribery, corruption and theft, both from within the Council and from external sources. We recognise fraud can:

- Undermine the standards of public service that the Council is attempting to achieve;
- Reduce the level of resources and services available for the residents of Stroud; and
- Result in major consequences which reduce public confidence in the Council.

Definitions

Fraud

Fraud is defined by the [Fraud Act 2006](#) (at [UK Legislation](#)):

The Act describes fraud as the intention to make gain or cause loss under three main headings:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

There are further subheadings of fraud described including possession of articles for use in fraud, making or supplying articles for use in frauds, participating in fraudulent business and or obtaining services dishonestly.

Theft

Theft is the physical misappropriation of cash or other tangible assets. A person is guilty of “theft” if he or she dishonestly takes property belonging to another, with the intention of permanently depriving the other of it.

Corruption

Corruption is defined as the offering, giving, soliciting or acceptance of an inducement or reward, or showing any favour or disfavour which may influence any person to act improperly.

[The Bribery Act 2010](#) came into force on 1 July 2011. Bribery is defined in the Act “as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward a person for having already done so, in order to gain personal, commercial, regulatory or contractual advantage”. It is the most common form of corruption. The Council’s responsibilities are set out within the Anti-Bribery Policy (Appendix 4).

Money Laundering

Money laundering is the term used for a number of offences involving concealing the proceeds of crime or terrorist funds, so that they appear they have come from a legitimate source. Money laundering involves one or more of three principal offences: concealing, arranging and acquisition / use / possession.

The burden of identifying and reporting acts of money laundering rests within the Council. Any service that receives money from an external person or body is potentially vulnerable to a money laundering operation.

The need for vigilance is vital and any suspicion concerning the appropriateness of a transaction should be reported and advice sought from the Money Laundering Reporting Officer.

The Council recognises its responsibilities under [the Money Laundering and Terrorist Financing \(Amendment\) Regulations 2019](#) and the [Proceeds of Crime Act 2002](#).

These responsibilities are set out within the Council's Anti-Money Laundering Policy **(Appendix 5)**

Scope

This strategy applies to:

- All Stroud District Council employees (including volunteers and agency staff);
- Councillors;
- Staff and Committee Members of council funded voluntary organisations;
- Stroud District Council partners;
- NHS partners;
- Stroud District Council's suppliers, contractors and consultants;
- Service Users; and
- Stroud District residents.

What are the aims and objectives of the strategy?

We aim to:

- Protect the Council's valuable resources by ensuring they are not lost through fraud but are used for improved services to Stroud's residents and visitors;
- Provide a Counter Fraud Service which:
- Ensures that the resources dedicated are sufficient and those involved are trained to deliver a professional counter fraud service to the highest standards;
- Proactively deters, prevents and detects fraud, bribery, corruption and theft;
- Investigates suspected or detected fraud, bribery, corruption and theft;
- Enables the Council to apply appropriate sanctions and recover all losses. In addition wherever possible the Council seeks to recover all proven financial losses through court action or by invoicing an individual. Where an employee is a member of the Local Government Pension Scheme, then in accordance with the provisions of the pension scheme, the Council will seek to recover any money owing as a result of that employee's grave misconduct, criminal, negligent or fraudulent acts or omission from the employee's pension benefits. Alternatively and again in accordance with the provisions of those pension schemes, the Council will seek full forfeiture of that members pension benefits where applicable.

- Provides recommendations to inform policy, system, risk management and control improvements, thereby reducing the Council's exposure to fraudulent activity.
- Create an environment that enables the reporting of any genuine suspicions of fraudulent activity. However, we will not tolerate malicious or vexatious allegations or those motivated by personal gain and, if proven, we may take disciplinary or legal action; and
- Work with our partners and other investigative bodies to strengthen and continuously improve our arrangements to prevent fraud and corruption.

What is SDC's approach to Countering Fraud?

Managing the Risk of Fraud and Corruption

- As with any risk faced by the Council, it is the responsibility of managers to ensure that fraud risk is adequately considered when preparing risk assessments in support of achieving strategic priorities, business plan, projects and programmes objectives and outcomes. In making this assessment it is important to consider the risk of fraud occurring rather than the actual incidence of fraud having occurred in the past. Once the fraud risk has been evaluated, appropriate action should be taken to mitigate those risks on an ongoing basis.
- Any changes in operations or the business environment must also be assessed to ensure any impacts, which might increase the risk or otherwise change the risk of fraud, bribery and corruption, are properly taken into account.
- Good corporate governance procedures are a strong safeguard against fraud and corruption. Adequate supervision, recruitment and selection, scrutiny and healthy scepticism must not be seen as distrust but simply as good management practice shaping attitudes and creating an environment opposed to fraudulent activity.
- Whilst all stakeholders in scope have a part to play in reducing the risk fraud, SDC's Members, Strategic Directors and Management are ideally positioned to influence the ethical tone of the organisation and play a crucial role in fostering a culture of high ethical standards and integrity.
- The Council believes the best defence against fraud, corruption and bribery is to create a strong count-fraud culture within the organisation and that a culture of honesty and openness is a key element in tackling fraud. The codes of conduct for Members and employees are based upon the Nolan principles of Standards in Public Life. In cases where Members or employees fail to adhere to these codes appropriate action will be taken against them. The seven Nolan principles of Standards in Public Life are:

Selflessness: you must act solely in terms of the public interest and not in order to gain financial or other material benefits for yourself, family, or friends;

Integrity you should not place yourself under any financial or other obligation to outside individuals or organisations that might seek to influence you in the performance of your official duties;

Objectivity you must make choices on merit when making decisions on appointments, contracts, or recommending rewards and benefits for individuals;

Accountability you are accountable for your decisions and actions to the public and you must submit yourself to whatever scrutiny is appropriate;

Openness you should be as open as possible about all decisions and actions that you take. You should give reasons for your decisions and restrict information only when the wider public interest clearly demands;

Honesty you have a duty to declare any private interests relating to your work and you need to take steps to resolve any conflicts arising in the way that protects the public interest;

Leadership you should promote and support these principles by leadership and example.

- SDC will fulfil the responsibility to reduce fraud and protect our resources by a strategic approach consistent with that outlined in Fighting Fraud and Corruption Locally, A strategy for the 2020s.

Fighting Fraud and Corruption Locally: Acknowledge, Prevent, Pursue

GOVERN	<p>Arrangements and Executive Support</p>	<p>We have robust arrangements and executive support to ensure counter-fraud, bribery and corruption measures are embedded throughout the Council. The internal arrangements that are put in place are communicated throughout the Council and publicly available to demonstrate the culture and commitment to preventing fraud.</p>
---------------	---	--

ACKNOWLEDGE	<p>Committing Support</p>	<p>The Council’s commitment to tackling the threat of fraud is clear. We have strong whistleblowing procedures and support those who come forward to report suspected fraud. All reports will be treated seriously and acted upon. We will not, however, tolerate malicious or vexatious allegations.</p>
	<p>Assessing Risks</p>	<p>We will continuously assess those areas most vulnerable to the risk of fraud as part of our risk management arrangements. These risk assessments will inform our internal controls and counter fraud priorities. In addition, Internal Audit will carry out work in these high risk areas to assist management in detecting existing and new types of fraudulent activity. Examples of fraud indicators are provided at Appendix 1 and types of fraud are provided at Appendix 2.</p>
	<p>Robust Response</p>	<p>We will strengthen measures to prevent fraud. Internal Audit will work with our internal partners such as management, HR, Finance, Legal, policy makers and external partners, to ensure new and existing systems and policy initiatives are adequately fraud proofed.</p>

PREVENT	<p>Better use of Information Technology</p>	<p>We will make greater use of data and analytical software to prevent and detect fraudulent activity. We will look for opportunities to share data and fraud intelligence to increase our capability to uncover potential and actual fraud.</p>
	<p>Counter Fraud Culture</p>	<p>We will promote and develop a strong counter fraud culture, raise awareness, provide a fraud e-learning tool and provide information on all aspects of our counter fraud work. This will include publicising the results of all proactive work, fraud investigations, successful sanctions and any recovery of losses due to fraud.</p>

PURSUE	Fraud Recovery	A crucial element of our response to tackling fraud is recovering any monies lost through fraud. This is an important part of our strategy and will be rigorously pursued, where possible.
	Punishing Fraudsters	We will apply realistic and effective sanctions for individuals or organisations where an investigation reveals fraudulent activity. This may include legal action, criminal and/or disciplinary action, where appropriate.
	Enforcement	Appropriately trained investigators will investigate any fraud detected through the planned proactive work; cases of suspected fraud referred from internal or external stakeholders, or received via the confidential reporting procedure (whistleblowing). We will also work with relevant internal and external partners/external agencies/organisations.

PROTECT	Recognise the harm	We will recognise and protect the organisation against serious and organised crime.
	Protect itself	We will protect public funds, protect the organisation from fraud and cybercrime and also monitor and protect the Council from future fraud risks.
	Protect its' residents	We will endeavour to protect individuals from becoming victims of crime and protect against the harm that fraud can do to the community.

Responsibilities

Stakeholder	Specific Responsibilities
Chief Executive	<p>Accountable for the overall effectiveness of the Council’s arrangements for countering fraud and corruption by:</p> <ul style="list-style-type: none"> • Ensuring that the Council has a trained counter fraud resource in the organisation or has access to one; and • Providing the Audit and Standards Committee with regular reports on the work of those leading on fraud.
Monitoring Officer	<p>To advise Councillors and Officers on ethical issues, standards and powers to ensure that the Council operates within the law and statutory Codes of Conduct/Practice. Overall responsibility for the maintenance and operation of the Confidential Reporting Procedure for Employees (Whistleblowing) and ensuring that:</p> <ul style="list-style-type: none"> • Members, Audit and Standards Committee and portfolio leads are aware of counter fraud activity and that training is available to them; and • That the fraud team is independent of process and it produces reports to relevant committees that are scrutinised by members.
Strategic Director of Resources (Section 151 Officer)	<p>To ensure the Council has adopted and implemented an appropriate Counter Fraud and Corruption Policy/Strategy and that the Council has an adequately resourced and effective Internal Audit service to deliver “counter fraud” activity by ensuring that:</p> <ul style="list-style-type: none"> • The Chief Internal Auditor is assessing counter fraud resources, capability and has sufficient internal unfettered access; • The Counter Fraud Team produce regular reports on activity, success and future plans; • The Council participates fully in the bi-annual National Fraud Initiative (NFI) exercise and reports outcomes accordingly; and • The Council is measuring itself against the FFCL checklist.

Audit and Standards Committee	<p>To monitor the adequacy and effectiveness of the arrangements in place for combating fraud and corruption by:</p> <ul style="list-style-type: none"> • Receiving a report quarterly on the counter fraud activity which includes proactive and reactive work; • Proactively supporting and challenging counter fraud activity; and • Monitoring the adequacy and effectiveness of the arrangements in place for combating fraud and corruption.
Members	<p>To comply with the Members Code of Conduct and related Council policies and procedures, to be aware of the possibility of fraud, corruption, bribery and theft, and to report any genuine concerns accordingly.</p>
External Audit	<p>Statutory duty to ensure that the Council has adequate arrangements in place for the prevention and detection of fraud, corruption, bribery and theft.</p>
Internal Audit	<ul style="list-style-type: none"> • Responsible for developing and promoting to the Council the requirements of the Counter Fraud and Corruption Strategy and monitoring and/or undertaking the investigation of any reported issues. • To ensure that all suspected or reported irregularities are dealt with promptly and in accordance with this strategy and that action is identified to improve controls and reduce the risk of recurrence; and • To present the Counter-Fraud and Corruption Policy Statement and Strategy to Council for approval and annually to Audit and Standards Committee, to support them fulfil their role. <p>Please see Appendix 3 – Fraud Response Plan.</p>
Heads of Service, Service Managers	<p>To promote staff awareness and ensure that all suspected or reported irregularities are immediately referred to the Monitoring Officer and/or the Chief Internal Auditor. To ensure that there are mechanisms in place within their service areas to assess the risk of fraud, corruption, bribery and theft and to reduce these risks by implementing strong internal controls.</p>
Staff	<p>To comply with Council policies and procedures, to be aware of the possibility of fraud, corruption, bribery and theft, and to report any genuine concerns to management, the Monitoring Officer, Chief Internal Auditor or via the Whistleblowing procedure.</p>
Public, Service Users, Partners, Suppliers, Contractors and Consultants	<p>To be aware of the possibility of fraud and corruption against the Council and report any genuine concerns / suspicions.</p>

Reporting, Advice and Support

The Council recognises that the primary responsibility for the prevention and detection of fraud rests with management. If you believe that someone is committing a fraud or you suspect corrupt practices, these concerns should be raised, in the first instance, directly with your Head of Service / Service Manager.

Alternatively, you may raise any concern with the Council's Monitoring Officer, S151 Officer, Human Resources Manager or the Council's Internal and / or external auditors in accordance with the Council's [confidential reporting procedure \(whistleblowing\)](#).

Internal Audit also provide a 24 hour Whistleblowing hotline answerphone service available on **01452 427052** for individuals to report any concerns.

We will treat all concerns or suspicions with discretion and in confidence.

Employees

Employees who wish to raise a serious concern, require advice and/or support, should do so verbally or in writing (marked 'Confidential') to either of the following:

Role	Officer Name/Co.	Tel. No.	E-mail Address
Monitoring Officer	Patrick Arran	01453 754369	Patrick.Arran@stroud.gov.uk
Strategic Director of Resources (S151 Officer)	Andrew Cummings	01453 754115	Andrew.Cummings@stroud.gov.uk
Human Resources Manager	Lucy Powell	01453 754286	lucy.powell@stroud.gov.uk
External Auditors	Deloitte LLP (UK)	029 20460000	www.deloitte.co.uk
SDC's Chief Internal Auditor	Theresa Mortimer	01453 754111	theresa.mortimer@stroud.gov.uk
Protect	(Independent whistleblowing charity)	Helpline: (020) 3117 2520	E-mail: whistle@protect-advice.org.uk Website: https://protect-advice.org.uk/

Members of the Public / External Providers / Partners

If the informant is a member of the public, external contractor or partner they should contact the Council's Chief Internal Auditor to report any concerns of fraudulent activity.

However, the above process does not relate to reporting housing benefit fraud allegations which are now dealt with by the Department for Work and Pensions. In these cases, the informant should contact the Revenue and Benefits Manager either by e-mail **simon.killen@stroud.gov.uk** or by telephone **01453 754013**.

All concerns in relation to possible financial impropriety will be reported to the S151 officer and/or the Chief Internal Auditor.

Further Information

Further information on relevant Council policy and practice and relevant publications can be found in the following documents:

- The [Constitution](#) includes Financial Regulations, Members Code of Conduct and Contract Standing Orders;
- [Confidential Reporting Procedure \(Whistleblowing\)](#);
- [Fraud Response Plan](#) (Appendix 3);
- Anti Bribery Policy (Appendix 4);
- Anti Money Laundering Policy (Appendix 5);
- [Risk Management Policy Statement and Strategy](#);
- [Internal Audit Charter](#);
- Information Security Policy;
- [Members Code of Conduct](#);
- [Employees Code of Conduct](#);
- [The Local Government Transparency Code 2015](#) (at [Gov.uk](#));
- [National Fraud Initiative](#) (NFI) (at [Gov.uk](#));
- [Fighting Fraud and Corruption Locally, A strategy for the 2020s](#) (at the [Chartered Institute of Public Finance & Accountancy](#)); and

Strategy Review

The S151 Officer and the Audit and Standards Committee will ensure the continuous review and amendment of this strategy and the relevant associated policies as necessary to ensure that it remains compliant with good practice, national public sector Codes of Practice and meets the needs of the Council.

Responsible Officer: Chief Internal Auditor

Review date: Frequency as required by legislative changes / May 2021

Appendix 1: Key Fraud Indicators

A number of frauds can come to light because of suspicions aroused by, for instance, the behaviour of certain individuals. It is impossible to give a definitive list of fraud indicators or warning signs. However, the following are indicators that may, either alone or cumulatively with other factors, suggest the possibility of fraud and may therefore warrant further investigation or enquiry.

- **Unusual employee behaviour:** Refusal to comply with normal rules and practices, fails to take leave, refusing promotion, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regularly working long hours, job dissatisfaction / unhappy employee, secretiveness or undue defensiveness.
- **Financial irregularities:** Key documents missing (e.g. invoices, contracts); absence of controls and audit trails; missing expenditure vouchers and official records; general ledger out of balance; bank and ledger reconciliations are not maintained or cannot be balanced; excessive movements of cash or transactions between accounts; numerous adjustments or exceptions; constant overdue pay or expense advances; duplicate payments; ghost employees on the payroll; large payments to individuals; excessive variations to budgets or contracts.
- **Poor procurement practice:** Too close a relationship with suppliers/contractors; suppliers / contractors who insist on dealing with only one particular member of staff; unjustified disqualification of any bidder; lowest tenders or quotes passed over with minimal explanation recorded; defining needs in ways that can be met only by specific contractors; single vendors; vague specifications; splitting up requirements to get under small purchase requirements or to avoid prescribed levels of review or approval.
- **Disorganisation:** Understaffing in key control areas; consistent failures to correct major weaknesses in internal control; inadequate or no segregation of duties.
- **Inadequate supervision:** Policies not being followed; lack of senior management oversight; inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation); low staff morale, weak or inconsistent management.
- **Lax corporate culture:** Management frequently override internal control; climate of fear or a corporate culture; employees under stress without excessive workloads; new employees resigning quickly; crisis management coupled with a pressured business environment; high employee turnover rates in key controlling functions.
- **Poor work practices:** Lack of common sense controls; work is left until the employee returns from leave; post office boxes as shipping addresses; documentation that is photocopied or lacking essential information; lack of rotation of duties; unauthorised changes to systems or work practices.

Appendix 2: Types of Fraud

Local authorities have reported a wide range of fraud types. The main areas of fraud that were previously reported continue to feature as significant risks. However, there are also new fraud types emerging and some of these are more prevalent in particular parts of the country. It is clear that a one size fits all approach is not appropriate and therefore the council needs to remain vigilant and be aware of these types of fraud risks.

Known Fraud Risks Remaining Significant

Council tax – Discounts and exemptions, council tax support.

Grants – Work not carried out, funds diverted, ineligibility not declared.

Identity fraud – False identity / fictitious persons applying for services / payments.

Internal fraud – Diverting Council monies to a personal account; accepting bribes; stealing cash; misallocating social housing for personal gain; working elsewhere while claiming to be off sick; false overtime claims; selling Council property for personal gain; wrongfully claiming benefit while working.

Payroll – False employees, overtime claims, expenses.

Pensions – Deceased pensioner, overpayments, entitlement overstated.

Procurement – Tendering issues, split contracts, double invoicing.

Tenancy – Fraudulent applications for housing or successions of tenancy, and subletting of the property.

Recruitment – Failing to disclose convictions or gaps in employment, misstating of qualifications and experience, and nepotism.

Emerging / Increasing Fraud Risks

Business rates – Fraudulent applications for exemptions and reliefs, unlisted properties.

Commissioning of services – Including joint commissioning, third sector partnerships – conflicts of interest, collusion.

Cyber dependent crime and cyber enabled fraud – Enables a range of fraud types resulting in diversion of funds, creation of false applications for services and payments.

Disabled Facility Grants – Fraudulent applications for adaptations to homes aimed at the disabled.

Immigration – Including sham marriages. False entitlement to services and payments.

Insurance Fraud – False claims including slips and trips.

Local Enterprise Partnerships – Voluntary partnerships between local authorities and businesses. Procurement fraud, grant fraud.

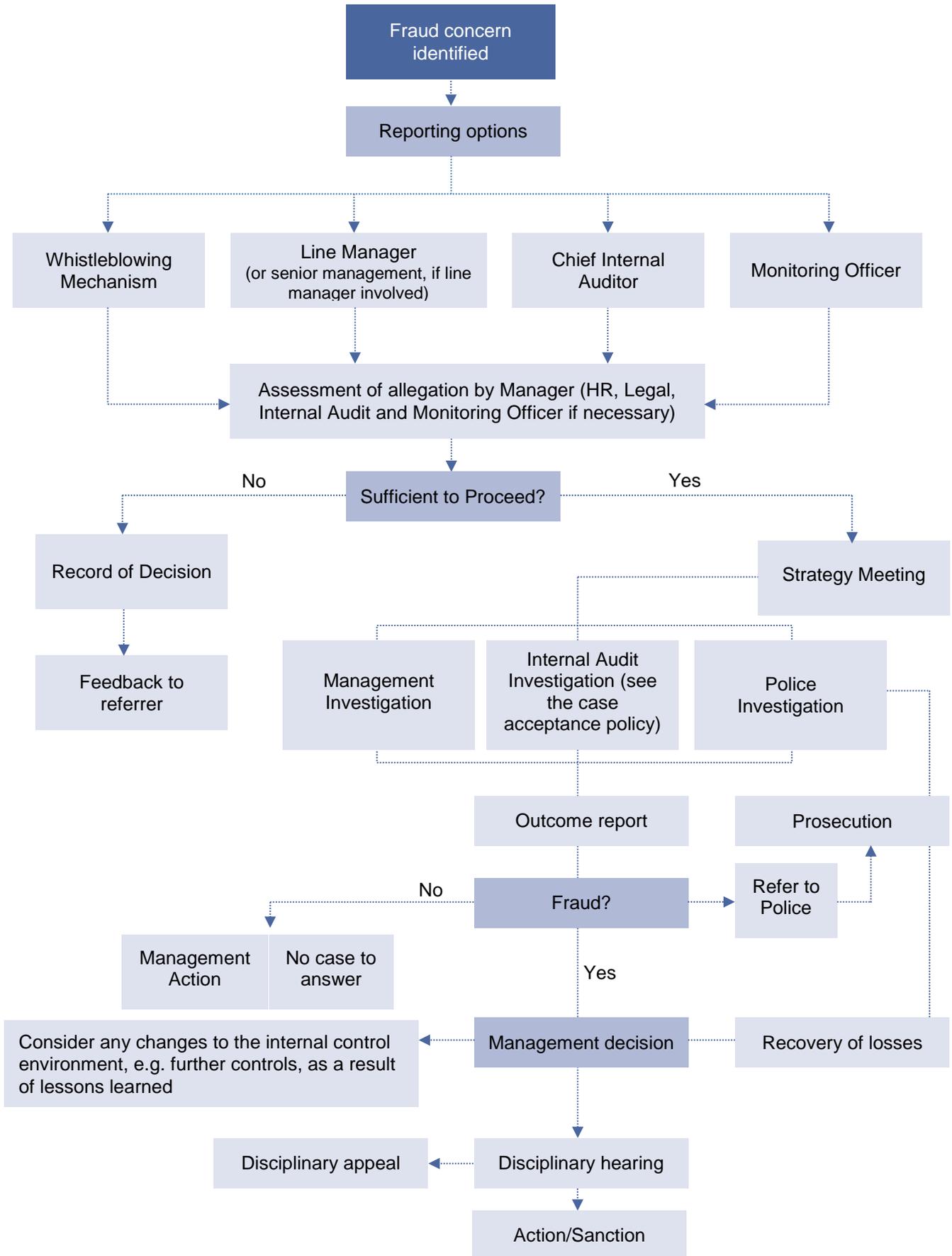
New Responsibilities – Areas that have transferred to local authority responsibility e.g. Public Health grants, contracts.

Money laundering – Exposure to suspect transactions.

No recourse to public funds – Fraudulent claim of eligibility.

Right to buy – Fraudulent applications under the right to buy/acquire scheme.

Appendix 3: SDC's Fraud Response Plan



Appendix 4: Anti-Bribery Policy

Introduction

The Council is committed to implementing and enforcing effective systems to counter bribery. Therefore, it is the Council's policy to conduct all aspects of its business in an honest and ethical manner at all times.

Bribery Act 2010

The Bribery Act 2010 came into force in the UK on 1st July 2011. It amends and reforms the UK criminal law and provides a modern legal framework to combat bribery in the UK and internationally. Staff need to be aware of their obligations under this Act, which sets out the criminality of accepting and giving of bribes. This applies to both individual staff and the Council corporately. The Bribery Act creates the following offences:

- Active bribery: promising or giving a financial or other advantage;
- Passive bribery: agreeing to receive or accepting a financial or other advantage;
- Bribery of foreign public officials; and
- The failure of commercial organisations to prevent bribery by an associated person (corporate offence).

The penalty under the Bribery Act is an unlimited fine and/or imprisonment up to a maximum of 10 years.

Full details of the Act can be found at:

<http://www.legislation.gov.uk/ukpga/2010/23/contents>

Policy

The aim of this policy is to help the Council act in accordance with the Bribery Act 2010, maintain the highest possible standards of business practice, and advise individuals of the Council's 'zero-tolerance' to bribery.

This policy applies to all councillors, permanent and fixed-term staff employed by the Council, and any contractors, consultants or other persons acting within or on behalf of the Council.

The Council will not:

- Make contributions of any kind with the purpose of gaining any commercial advantage;
- Provide gifts or hospitality with the intention of persuading anyone to act improperly, or to influence a public official in the performance of their duties; and
- Make, or accept, inducements of any kind.

Council Responsibility

The Council will:

- Keep appropriate internal records that will evidence the business reason for making any payments to third parties;
- Encourage employees to raise concerns about any issue or suspicion of malpractice at the earliest possible stage; and
- Ensure that anyone raising a concern about bribery will not suffer any detriment as a result, even if their concerns are not validated, providing there is no malicious intent.

Employee Responsibility

Employees must not:

- Accept any financial or other reward from any person in return for providing some favour;
- Request a financial or other reward from any person in return for providing some favour; and
- Offer any financial or other reward to any person in return for providing some favour.

Non Compliance

All employees have a role to play in enforcing the policy and are required to report any suspected breach in accordance with the Council's whistleblowing policy.

The Council will not tolerate bribery or corruption by its councillors, employees, suppliers, contractors, partners or service users and will take all necessary steps to investigate all allegations of bribery or corruption and pursue sanctions available in each case, including removal from office, disciplinary action, dismissal and/or prosecution under the Bribery Act 2010.

Appendix 5: Anti-Money Laundering Policy

Introduction

The Proceeds of Crime Act (POCA) 2002 (amended by the Criminal Finances Act 2017), Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017 and the Terrorism Act 2000 place obligations on the Council and its employees with respect to suspected money laundering. These obligations impact on certain areas of local authority business and require local authorities to establish internal procedures to prevent the use of their services for money laundering. This Policy sets out how any concerns should be raised.

Whilst the majority of money laundering activity in the UK falls outside of the public sector, vigilance by employees of the Council can help identify those who are or may be perpetrating crimes relating to the financing of terrorism and money laundering.

Scope of the Policy

This Policy applies to all employees of the Council and aims to maintain the high standards of conduct which currently exist within the Council by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Council to comply with its legal obligations.

Failure by a member of staff to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Policy and Procedure.

What is Money Laundering?

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. In other words, the process of changing 'bad' money into 'good' money in order to hide the fact that the money originated from criminal activity. Formally, the following acts constitute money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the Proceeds of Crime Act 2002); or
- 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);
- Acquiring, using or possessing criminal property (section 329);
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorism Act 2000);
- Tax evasion (Part 3 sections 45 and 46 the Criminal Finances Act 2017); and
- Gross human rights abuse and violation (Part 5 of POCA 2002, section 241 amended by the Criminal Finances Act 2017).

These are the primary money laundering offences and thus prohibited acts under the legislation. There are also two secondary offences: failure to disclose any of the primary offences and tipping off. 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.

Potentially any member of staff could be implicated 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.

Failure to disclose (section 330)

A person commits an offence if each of the following three conditions are satisfied;

- they know or have reasonable grounds to suspect that another person is engaged in money laundering;
- the information or knowledge in which they have grounds for suspicion is received in the course of business in the regulated sector; and
- the required disclosure is not made as soon as is practicable after the information comes to them.

A person does not commit an offence under this section if:

- there is a reasonable excuse for not disclosing this information or other matter;
- they provide professional legal advice and the information came to them in privileged circumstances; and
- they do not know or suspect money laundering, or have not been provided with such training as specified by the Secretary of State.

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.***

What are the Obligations on the Council?

Organisations conducting "relevant business" must:

- appoint a Money Laundering Reporting Officer ("MLRO") to receive disclosures from employees of money laundering activity (their own or anyone else's);
- implement a procedure to enable the reporting of suspicions of money laundering;
- maintain client identification procedures in certain circumstances; and
- maintain record keeping procedures.

Not all of the Council's business is "relevant" for the purposes of the legislation. It is mainly the accountancy and audit services carried out by the financial service functions within the Council and the financial, company and property transactions undertaken by Legal Services.

However, the safest way to ensure compliance with the law is to apply it to all areas of work undertaken by the Council; therefore, all staff are required to comply with the reporting procedure set out in the [Disclosure Procedure](#) section below.

The Money Laundering Reporting Officer (MLRO)

The officer nominated to receive disclosures about money laundering activity within the Council is the Strategic Director of Resources (S151 Officer) details are provided below:

Andrew Cummings: Strategic Director of Resources (S151 Officer)

Stroud District Council

Ebley Mill,

The Wharf,

Stroud,

Gloucestershire.

GL5 4UB

Email: Andrew.Cummings@stroud.gov.uk

Telephone: 01453 754115 (direct line)

In the absence of the MLRO, the Deputy S151 Officer is authorised to deputise.

Disclosure Procedure

Cash Payments:

No payment to the Council will be accepted in cash (including notes, coins or travellers cheques in any currency) if it exceeds £5,000. Cash payments in excess of £10,000 received in more than one transaction within a twelve month period must also be treated as suspicious.

Even if the cash value is less than £5,000 and there is suspicion that the monies are from proceeds of crime then it should still be reported to the MLRO.

Any officer involved in a transaction of this kind should ensure that the person(s) provide satisfactory evidence of their personal identity.

Reporting to the Money Laundering Reporting Officer

Where you know or suspect that money laundering activity is taking/has taken place, or become concerned that your involvement in a matter may amount to a prohibited act under the legislation, you must disclose this as soon as practicable to the MLRO.

Your disclosure should be made to the MLRO. The report must include as much detail as possible.

The employee must follow any subsequent directions from the MLRO or deputy 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 or deputy.

The employee must not disclose or otherwise indicate their suspicions to the person(s) suspected of money laundering otherwise you may commit a criminal offence of "tipping off". They must not discuss the matter with others or note on a file that a report has been made to the MLRO in case this results in the suspect becoming aware of the suspicion, through a request to see their file. The MLRO will keep the appropriate records in a confidential manner.

Full details of the people involved (including you, if relevant), e.g. name, date of birth, address, company names, directorships, phone numbers, etc. will be required. If you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327 - 329 of the 2002 Act, then your report must include all relevant details, as you will need consent from the National Crime Agency (NCA) via the MLRO, to take any further part in the transaction - this is the case even if the client gives instructions for the matter to proceed before such consent is given.

You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline;

Once you have reported the matter to the MLRO you must follow any directions he may give you. You must **not** make any further enquiries into the matter yourself: any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO who will refer the matter on to the Serious Organised Crime Agency (SOCA) if appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

Client Identification Procedure (Customer Due Diligence)

Where the Council is carrying out relevant business (e.g. accountancy, audit and certain legal services) it must apply customer due diligence measures:

- a) when you establish a business relationship;
- b) when you carry out an 'occasional transaction' worth €15,000 (approximately £13,000) or more, whether the transaction is carried out in a single operation or several operations which appear to be linked;
- c) when you suspect money laundering or terrorist financing;

- d) when you have doubts about a customer's identification information that you obtained previously; and
- e) when it's necessary for existing customers - for example if their circumstances change

A business relationship is one that you enter into with a customer where both of you expect that the relationship will be ongoing. It can be a formal or an informal arrangement.

When a new business relationship is established the Council needs to obtain information on:

- the purpose of the relationship
- the intended nature of the relationship - for example where funds will come from, the purpose of transactions, and so on.

The type of information that you need to obtain may include:

- details of your customer's business or employment
- the source and origin of funds that the customer will be using in the relationship
- copies of recent and current financial statements
- details of the relationships between signatories and any underlying beneficial owners
- the expected level and type of activity that will take place in the relationship.

Please note that unlike the reporting procedure, the client identification procedure is restricted to those operating relevant business, i.e. Financial Services and Legal Services.

In the above circumstances, staff in the relevant unit of the Council must obtain satisfactory evidence of the identity of the prospective client, as soon as practicable after instructions are received (unless evidence of the client has already been obtained). This applies to existing clients, as well as new ones, but identification evidence is not required for matters entered into prior to 1 March 2004.

Once instructions to provide relevant business have been received, and it has been established that any of paragraphs (a) to (e) apply, evidence of identity should be obtained.

With instructions from new clients, or further instructions from a client not well known to you, you may wish to seek additional evidence of the identity of key individuals in the organisation and of the organisation itself.

In all cases, the evidence should be retained for at least five years from the **end** of the business relationship or transaction(s).

If satisfactory evidence of identity is not obtained at the outset of the matter then the business relationship or one off transaction(s) cannot proceed any further.

Record Keeping Procedures

The MLRO should retain records of all referrals made to them and of any action taken. The precise nature of these records is not set out in law but should be capable of providing an audit trail during any subsequent investigation.

All records should be retained for at least five years. This is so that they may be used as evidence in any subsequent investigation by the authorities into money laundering.

Guidance and Training

In support of this policy, the Council will:

- make staff aware of the requirements and obligations under the anti-money laundering policy legislation; and
- provide training to those most likely to encounter money laundering.

Conclusion

The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This Policy has been written to support the Council to meet the legal requirements in a way which is proportionate to the very low risk to the Council of contravening the legislation.

Should you have any concerns whatsoever regarding any transactions then you should contact the MLRO.

Further Information

Further information relating to the anti-money laundering policy can be found at the following links:

- [National Crime Agency \(NCA\)](#)
- [The Money Laundering and Terrorist Financing \(Amendment\) Regulations 2019](#)
- [Terrorism Act 2002 - Code of Practice](#)
- [CIPFA Guidance on Money Laundering](#)
- [Proceeds of Crime Act 2002](#)
- Money Laundering Disclosure Form
- Guidance for MLRO
- [Criminal Finances Act 2017](#)

**Counter-Fraud
and Corruption**

Policy Statement and Strategy
2020-2023

June 2020

