PART O Anti-Fraud, Theft and Corruption Policy

Contents **Page**

Formatted: Tab stops: 6.77 cm, Left + 13.25 cm, Left

Section 1 – Introduction

1.1 Definition of Theft, Fraud and Corruption

Bribery is “offering, promising or giving a financial or other advantage where the advantage is intended to bring about an improper performance by another person of a relevant function or activity, or to reward such improper performance or where the person offering, promising or giving the advantage knows or believes that the acceptance of the advantage itself constitutes the improper performance of a relevant function or activity”.

Corruption is "the offering, giving, soliciting or acceptance of an inducement or reward which may influence the actions taken by the Authority, its Members, or officers". It also includes using personal relationships to influence actions.

Theft is "dishonestly appropriating property belonging to another, with the intention of permanently depriving them".

Fraud is "the intentional distortion of financial statements or other records by persons internal, or external, to the Authority, which is carried out to conceal the misappropriation of assets, or otherwise, for gain".

These records can include orders, invoices, travel claims, timesheets, flexitime variation sheets, holiday entitlement records, petty cash vouchers, or claims from independent contractors. It may also cover a number of other acts, such as failure to disclose information, or abuse of position.

Under the Fraud Act 2006 the following offences (all involving the purpose of gaining personally or causing loss to another) are defined:

Fraud by false representation – knowingly saying, writing or electronic communication of anything untrue or misleading or conduct that misleads.

Fraud by failing to disclose information – failing to disclose to another information that is legally required.

Fraud by abuse of position – applies to those abusing positions where they are expected to safeguard the financial interests of another person.

The Act also introduced new offences:

- Possession etc. of articles for use in frauds
- Making or supplying articles for use in frauds
- Participating in fraudulent trading
- Obtaining services dishonestly.

1.2 Introduction

We conduct all our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly, and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery and corruption.

This policy applies to all members of the Authority, employees, volunteers, contractors working for the Authority, service users, and agency staff. It provides information to people who may come across behaviour which they think may be fraudulent or corrupt.

Training on this policy forms part of the induction process for all individuals who work for us, and regular training will be provided as necessary.

Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

The primary responsibility for maintaining sound arrangements to prevent and detect theft, fraud and corruption rests with management but it is important that everyone knows:

- how to prevent/deter theft, fraud or corruption
- how to look for the signs of theft, fraud or corruption
- what to do if they suspect theft, fraud or corruption is taking place

If you have any concerns about theft, fraud, or corruption you should raise your concerns with the Head of Resources (as Section 151 Officer) or the Director of Sustainable Development (as Monitoring Officer). If concerns arise during an audit, you can raise them with the auditor who will speak to the Section 151 Officer about the matter. The Authority has also adopted a Confidential Reporting Procedure. This is referred to in Section 5.

It is important that you do not try to handle the problem yourself, without expert advice and assistance. A badly managed investigation may prejudice any Police prosecution, so there are several procedures which have to be followed.

1.3 Updating the Policy

The Authority Solicitor is responsible for updating this policy every three years for approval in accordance with the Authority's Scheme of Delegation. The policy will be available ~~within the Finance and People Teams' pages of~~ within the Authority Handbook page of Waymarker and linked to other appropriate sections. The policy will be publicised via Snapshot and on Team noticeboards.

1.4 Relationship with other policies etc.

The Authority has a range of interrelated policies and procedures (some of which are expressly referred to elsewhere in this policy) that provide a corporate framework to counter fraudulent activity. These have been formulated in line with appropriate legislative and professional requirements and include:

- Financial Regulations
- Contract Standing Orders
- Code of Conduct for Members
- Staff Code of Conduct

- Register of Members' interests
- Confidential Reporting Policy
- Register of Staff Interests in Contracts and other matters
- Sound internal control systems
- ICT Policy
- Effective internal audit (currently provided under contract with a professional audit company)
- Disciplinary Procedure

Section 2 - Prevention and Deterrence of Theft, Fraud and Corruption

2.1 Theft and Fraud - Role of Managers

Whilst it is impossible to create a 100% fraud-proof system, all managers must ensure that the systems they operate include a reasonable number of effective controls designed to detect and prevent fraud and error. The actions and controls that managers should consider are as follows:

- documenting procedures and controls for localised systems and training all employees in their use

- ensuring all employees are familiar with the Authority's Financial Regulations and Contract Standing Orders

- carrying out spot checks to ensure compliance with procedures/regulations

- ensuring separation of duties between staff (as far as possible) so that no one person is solely responsible for the initiation through to the completion of a transaction, i.e. authorising a transaction, processing the transaction, collecting cash/cheques where appropriate, receiving goods/services and recording the transaction

- assigning appropriate levels of delegation, e.g. orders over a certain value to be authorised by a restricted number of employees

- rotating staff responsibilities, where possible, to avoid one person always having sole charge over a given area

- introducing an adequate "internal check". At its simplest, this involves an independent officer checking the work/calculations/documentation prepared by the initiating officer. Internal check may also mean splitting the processing of a transaction between two or more officers, ego each supplier payment needs to be signed off by different officers for 'goods received' and 'authorisation', the payment is run checked and verified by an officer of the Finance Team before being finally sent for payment by a senior manager of the Authority. Unless there is extensive collusion between employees, this will reduce the opportunity for fraud

- ensuring expenditure is authorised prior to expenses being incurred

- ensuring expenses/petty cash claims are supported by receipts

- minimising cash/cheques/stock holdings. Bank cash/cheques regularly, preferably daily, depending on the value and the risk

- reviewing budget monitoring statements, be alert to trends, e.g. falling income or increasing travel expenses, and follow up variances

- ensuring employees take their proper allocation of holidays and that other employees undertake their duties in their absence. Cover arrangements should be robust

- regularly reviewing processes to identify 'weak links' that may be vulnerable to fraud.

2.2 Theft, Fraud and Corruption – Role of Authority Procedures

The Authority's policies and procedures are an important part of the overall framework for internal control. They need to be robust and updated on a regular basis to reflect regulatory good practice in the operation of the organisation at any time.

Financial Regulations and Contract Standing Orders

- ensure Financial Regulations and Contract Standing Orders cover the key risk areas

- ensure all Members and employees receive training on the Financial Regulations and Contract Standing Orders

- ensure Financial Regulations and Contract Standing Orders are updated periodically, changes are communicated, and additional training is given if necessary

- ensure the handling of breaches of Financial Regulations and Contract Standing Orders are fully documented and dealt with appropriately

- declare related party transactions as part of the preparation of financial statements each year

Conduct for Members and Officers

- provide all Members with a copy of the Code of Conduct and ask them to confirm that they understand the Code and provide training where necessary

- provide access for all employees to the Employees' Code of Conduct

- ensure the maintenance of the register of members' interests and register of officers' interests in contracts in accordance with statutory requirement

- ensure the maintenance of a register for declaration of interests of employees, reviewed by senior officers on a regular basis

- remind Members and employees of the need to declare interests and gifts/hospitality received in accordance with the relevant code of conduct

Contracts

- provide within the Procurement Guidance clear, written instructions, for employees involved in letting and controlling contracts (including the position regarding tender negotiations)
- regular review of the effectiveness of contractors and re-tendering of contracts on a regular basis
- ensure adequate supervision of/separation of duties between employees letting and controlling contracts, as far as practicable
- carry out an independent review of circumstances where particular contractors seem to be preferred
- ensure adequate justification for, and approval of, occasions when negotiated or restricted tendering is used and that this is fully documented
- ensure tenderers are chosen on a rational basis (such as approved lists, or multi-authority framework agreements) to ensure fair competition and equal opportunity to tender
- carry out spot checks to ensure rules relating to despatch and return of tenders are being complied with
- ensure contracts are signed by both parties.

Asset Disposals

- ensure there are clearly defined procedures for asset sales and that these are fully understood by all relevant Members and employees
- document all disposals so that it can be demonstrated that best value has been obtained.

Award of Planning Consents

- ensure there are written procedures covering delegated powers of Members/employees in awarding planning consents
- ensure decisions are fully documented so that it can be demonstrated that decisions are made on a consistent and rational basis
- monitor committee decisions on planning applications, particularly where planning officer recommendations are not followed.

2.3 Role of Internal Audit

The Authority's Annual Internal Audit Plan includes the audit of the major financial systems listed below over a rolling 3-year period:

- Payroll
- Creditors

- Treasury Management
- Main Accounting System
- Salaries
- Debtors and Income Collection

The audits of the major financial systems include a review of the key controls. This is based on best practice checklists. Where a specific checklist does not exist, audit will review the existing internal controls in line with the issues detailed in 2.1 above and make recommendations where appropriate. It is not possible to specify controls which will detect the actual receipt of corrupt inducements. Reliance has to be placed on having adequate procedures in place, based on Financial Regulations and Contract Standing Orders, to limit the possibility of corrupt practices. Audit work is limited to testing compliance with these procedures and drawing attention to any weaknesses.

Regular liaison meetings are held with our internal auditors and our external auditors. Fraud related issues are addressed as part of those meetings.

However, it is ultimately the responsibility of management (see section 2 above) to ensure adequate controls and procedures are in place to prevent and detect theft or fraud, in accordance with the guidelines provided under paragraph 2.1 of this code.

2.4 Role of Members

Members are required to comply with the Code of Conduct for Members and with the Authority's Standing Orders. All Members receive copies of these (which are found in the Authority Handbook) when joining the Authority and are required by law to sign a declaration that they will comply with the Code of Conduct. The Code of Conduct contains the rules setting out what interests need to be entered on the Register of Members' Interests and the declarations of interests at meetings.

After approving the Anti-Fraud, Theft and Corruption Policy Members will be expected to play an important role through leading by example and being seen to support it.

The Authority's Governance Committee has a role in promoting high standards of conduct by Members and to deal with complaints alleging breaches of the Code of Conduct for Members.

Section 3 - Detection and Awareness

3.1 Introduction

This section aims to outline particular risk areas and the different types of theft, fraud and corruption that may occur. National audit surveys have shown that there are far fewer proven instances of corruption than there are cases of fraud and theft.

3.2 Risk Areas

Fraud can happen wherever people working in or for the Authority or people outside the Authority complete official documentation and have the opportunity to take financial advantage of the Authority. The risk of fraud or corruption is increased where people working for the Authority, or outside agents, are in positions of trust or responsibility and are not checked or subjected to effective monitoring or validation.

Consequently, the following areas are particularly susceptible to theft, fraud and/or corruption:

- Claims from contractors/suppliers
- Travel and expense claims
- Cash/cheque receipts
- Petty cash/floats
- Payroll
- Purchasing
- Procurement of contracts
- Stocks and assets, particularly portable, attractive items
- Investments
- Disposal of Assets
- Award of Planning Consents
- Money Laundering (see section 3.4 below)
- Electronic Fraud (see section 3.5 below)

In addition, acceptance of gifts and hospitality, secondary employment and pressure selling (suppliers pressuring employees to order goods/services which are not required) can lead to corrupt practices.

3.3 Signs of Fraud and Corruption

Fraud often involves the falsification of records. Therefore, managers need to be aware of the possibility of fraud when reviewing or being presented with claims/forms/ documentation for authorisation. Issues which should give rise to suspicion are:

- documents that have been altered using different pens or different handwriting
- claims that cannot be checked because supporting documentation is inadequate (e.g. no vouchers/receipts)
- strange trends (in value, volume, or type of claim)
- illegible text/missing details
- delays in documentation completion or submission
- use of numerous cost centres to code expenditure (to avoid showing a large variation on one particular budget)
- large payments where no VAT number is quoted
- invoices that quote a PO Box number, rather than a specific address
- lack of authorisation for computer input/no supporting documentation.

There are also a number of indications that someone working for the Authority may be acting fraudulently:

- apparently living beyond their means

- under financial pressure
- exhibiting signs of stress or behaviour not in keeping with their usual conduct
- not taking annual leave
- refusing to allow another person working for the Authority to be involved in their duties
- attracting complaints from members of the public
- having private discussions with contractors
- unusual work patterns, e.g. always being the first in the office.

Suspicions of corruption usually come from outside the normal course of work. Sources should be followed up promptly in accordance with Section 4.7 of this policy.

3.4 Money Laundering

Money laundering is the practice whereby criminals attempt to 'clean' the proceeds of criminal activity by passing it through a legitimate institution. The Money Laundering Regulations 2007 as amended by The Money Laundering (Amendment) Regulations 2012, and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, impose an obligation on a variety of organisations, including local authorities, to report any incident that leads them to suspect that an individual or other body is making transactions with the proceeds of any criminal activity.

The Sanctions and Anti-Money Laundering Act 2018 also permit a minister to make regulations regarding money-laundering.

The Money Laundering Regulations require that the Authority put in place certain controls to prevent the Authority from being used for money laundering. These include:

- assessing the risk of the Authority being used by criminals to launder money
- checking the identity of customers
- checking the identity of 'beneficial owners' of corporate bodies and partnerships
- monitoring customers' business activities and reporting anything suspicious to the Serious Organised Crime Agency
- making sure the necessary management control systems are in place
- keeping all documents that relate to financial transactions, the identity of customers, risk assessment and management procedures and processes
- making sure that employees are aware of the regulations and have had any necessary training

Almost all the major cash transactions of the Authority occur as part of its Treasury Management operations, whereby the Authority lends, and is repaid, large sums. This is dealt with in the Authority's Treasury Management Policy Statement. Any attempt to launder cash will tend to involve larger sums of money. The only other area where large sums of money are received is the sale of assets. The Authority can take confidence from the following:

(a) the Legal Services Team will deal with the sale and will identify the payee during the course of the process of sale;

(b) receipts will normally be paid by BACS, CHAPS or cheques and the relevant bank will be required to comply with the money laundering regulations for their client;

(c) most customers will be long-standing tenants or known businesses; and

(d) comprehensive records of each transaction are maintained.

However, all staff who receive cash as part of their jobs should be vigilant for any unusual transactions that might indicate that an attempt is being made to launder money. Any suspicions should immediately be reported to the Head of Resources.

As an additional safeguard, receipts of notes, coins or travellers' cheques will not be accepted over £3,000 for any one transaction.

3.5 Bribery

The Bribery Act 2010 creates 4 criminal offences:

- giving, promising or offering a bribe;
- requesting, agreeing to receive or accepting a bribe;
- bribery of public officials;
- a relevant commercial organisation failing to put in place adequate procedures to prevent persons associated with them from giving or receiving bribes.

To ensure that the Authority complies with the legislation the Authority will ensure that:

- its employees comply with the Authority's Staff Code of Conduct and will ensure that the Code is reviewed and updated regularly;

- the Authority's Procurement requirements and Financial and Contract Standing Orders are strictly adhered to;

- Directors, Heads of Service and Team Leaders foster a culture within the organisation in which bribery is never acceptable; and

- The nature and extent of its exposure to potential external and internal risks of bribery on its behalf by employees and other persons associated with it are assessed and reviewed periodically and that such assessments are documented.

3.6 Electronic Fraud

Electronic fraud is a growing area. It may take several forms, such as:

- external hacking into systems and accessing bank details etc - a specialist company is commissioned to test the vulnerability of the Authority's IT network from external attack.

- identity theft of Authority employees - this is particularly important where staff have access to an Authority credit card, or hold passwords required to access

bank details etc. Staff are periodically reminded about basic safeguards to help prevent identity theft.

- Obtaining data from information that is not adequately safeguarded on a portable computer or portable storage device.

The Authority's internal and external audit functions conduct routine audits of computer systems to help identify any internal control weaknesses in this area.

The Authority deploys several systems to mitigate risk from fraud, including but not limited to:

- Mail filtering to block malware and spoofed emails (mails from hackers which appear to be internal)
- Enforcing password protection on memory sticks before information can be saved to them
- Encryption of laptop hard drives
- Enforced PIN protection and remote wipe capability on mobile phones
- National Cyber Security Centre systems to block malicious websites

However, it should be recognised that systems are one line of defence, but each officer must remain vigilant. All staff should remain alert, specifically:

- Do not share password or PINS or allow any unauthorised person to work under your account
- Adhere to the guidance in the ICT Policies
- Ensure no third parties have access to LDNPA systems without ICT training
- Install all software updates when prompted
- Be suspicious of any unexpected phone calls or emails requesting bank information, invoices to be paid, links to click
- Report any suspicions or issues to the ICT helpdesk promptly
- Complete all training modules which will be made available to staff on an annual basis

Line managers should support staff in making time and space available for training modules

3.7 Annual Fraud Report

An annual report on the Authority's anti-fraud activities and any instances of fraud will be included in the annual internal audit report considered by the Governance Committee.

Section 4 - Theft, Fraud and Corruption Response Plan

4.1 Introduction

This section sets out the responsibilities of officers and actions to be taken in cases where theft, fraud or corruption is suspected within the Authority.

The following procedure is where fraud, theft and corruption are the predominant feature of a particular case. There will be other cases where minor fraud is a subsidiary element of a broader case. In such a case, it may be appropriate for the lead officer to be a senior officer, other than the Internal Auditor. However, the Head of Resources should still be informed of any fraud as soon as it is discovered.

4.2 Discovery of Theft, Fraud and Corruption

Cases of theft, fraud and corruption often come to light in the following ways:

- management follow-up in areas where there is evidence of controls not being applied
- routine system checks
- tip-offs from a third party.

Where actions are thought to be deliberate, the possibility of theft, fraud or corruption should be considered.

If you discover or suspect theft, fraud, or corruption, it is essential that you inform the Head of Resources immediately. In his or her absence concerns may be raised with the Financial Services Manager (the Authority's Deputy Section 151 Officer).

If it is not practical to inform the officers above, you should inform your Head of Service. Out of office hours, senior officers who have been notified of a suspected incident should use their discretion as to whether to inform the Police. This is particularly relevant in cases of theft where a delay in reporting to the Police may be undesirable.

Where suspicions are aroused during audit reviews, the details should be immediately brought to the attention of the auditor, who will discuss the matter with the Head of Resources. The Head of Resources will then consider whether to consult the Police, depending on the scale of the issue under consideration.

Initial reports should be treated with discretion and caution, as apparently suspicious circumstances may turn out to have a reasonable explanation, or could be malicious. Initial interviews of those suspected of significant theft, fraud, or corruption, should be undertaken by the Internal Auditor and the Head of Resources. Minor allegations may be dealt with by the appropriate manager, following consultation with the Head of Resources. As soon as it becomes clear that a prosecution may be pursued, any interviews are best conducted by the Police.

If it is the Head of Resources that is suspected of theft, fraud or corruption, the details should immediately be brought to the attention of the Chief Executive, who will use the principles of this policy to conduct an appropriate investigation of the matter.

4.3 Responsibilities of the Head of Resources

As soon as possible, the Head of Resources should:

- consider the most appropriate Authority policy and procedure to use to expedite the matter effectively for the Authority (e.g. Disciplinary Policy or this policy).
- appoint an officer to lead the investigation (the Lead Officer), normally the Internal Auditor, but may be any Director or Head of Service as appropriate. If it appears that, prima facie, the Police may ultimately be involved, an informal discussion with the Police may be appropriate
- inform other managers as appropriate, e.g. Chief Executive, the Monitoring Officer, the Head of People and Organisational Development.
- inform external audit as appropriate.

The preliminary findings of the Lead Officer should then be reviewed and a decision made whether to:

- discontinue the investigation
- continue with a full investigation
- involve the Police and/or external audit.

If the Lead Officer is to continue with the investigation, the Head of Resources should:

- agree the objectives and terms of the investigation, as proposed by the Lead Officer
- agree the resources that are necessary for the investigation, as recommended by the Lead Officer
- inform the Chief Executive, and other appropriate officers.
- manage any public relation issues that may arise and liaise with the Lead Officer throughout the investigation
- liaise with the Monitoring Officer and the Head of People and Organisational Development in considering whether disciplinary processes and actions should be instituted
- report the outcome to the Chief Executive and the Authority's Governance Committee.

4.4 Responsibilities of the Lead Officer

The Lead Officer will organise the investigation on behalf of the Head of Resources and keep him/her informed of significant events. In some circumstances the Lead Officer will be the Head of Resources.

If suspicions are confirmed by an initial consideration of the issues, the Lead Officer will set up a full investigation by:

- agreeing terms of reference, scope, key issues and target dates etc.

- identifying staff needs and likely cost.

The Lead Officer will be the point of contact for liaison with the Police, external audit etc. He/she should ensure there is consideration of whether, or not, the Regulation of Investigatory Powers Act 2000 and/or the Protection of Freedoms Act 2012 applies to any aspect of the investigation.

The Lead Officer will report progress to the Head of Resources and recommend action (internal disciplinary action or prosecution).

The Lead Officer will arrange any necessary recovery action.

The Lead Officer will prepare a summary note identifying system weaknesses and lessons to be learnt, together with an action plan specifying officers responsible and completion dates.

It is important that all documentation and articles are collated at an early stage.

Advice can be obtained from the Cumbria Constabulary. Guidelines are set out in the CIPFA booklet: *The Investigation of Fraud in the Public Sector* and key points include:

- prime documents should be removed to a safe place, with copies being used for working purposes (in order to maintain secrecy, batches of documents, as opposed to individual items, should be removed)

- working papers should be dated, initialled and set out in such a way that a lay person could understand them and they could be presented in Court

- surveillance should only be carried out if it is properly authorised in accordance with the Regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012. The Internal Auditor should be contacted for further information, or in their absence the Authority's Solicitor

- interviewing must observe the Police and Criminal Evidence Act 1984 requirements and is best done by the Police

- if interviewing is conducted by staff the Internal Auditor should be contacted for further advice, or in their absence the Authority's Solicitor

4.5 Responsibilities of Heads of Service

In conjunction with the relevant Director as necessary, Heads of Service will make any necessary arrangements:

- for the employee under suspicion to be suspended, if required, pending the investigation and provide alternative staff cover

- secure any documents, equipment, or premises that could be interfered with

- arrange to have documents etc available for scrutiny.

4.6 Responsibilities of the Head of People and Organisation Development

If employees are involved, the Head of People and Organisation Development will:

- advise on personnel and procedural issues in relation to:
    - investigations
    - suspension
    - disciplinary proceedings
    - dismissal
- liaise with employee's union representatives as appropriate, as set out in the Authority's Disciplinary Procedure
- advise on the wording of future references, file notes and personal file details.

4.7 Confidentiality

Confidentiality will be respected, and anonymous 'tip-offs' will be assessed and followed up where appropriate. It is in your interest to report suspicions. Full details should be made available to the officer the matter is reported to. You need to take care that your actions do not arouse the suspicions of those who may be involved. The Authority's Confidential Reporting Policy (also on Waymarker and the Authority's website) gives full details of how confidentiality is dealt with and how those with concerns can report outside the Authority if they are unhappy with the Authority's response.

During an investigation, details should not be discussed with anyone other than members of the investigation team, as this may jeopardise the successful outcome of an investigation.

Media attention should be directed to the Head of Resources, who will liaise with the Head of Communications and Engagement and the Police as appropriate.

Once a potential offence is suspected to have been committed, a decision will need to be taken on whether, and when, to involve the Police or any investigation agency. This decision will be taken by the Head of Resources in consultation with the Chief Executive and any appropriate Member. The decision should be taken promptly. Care should be taken not to affect any prospective Police investigation. Account should be taken of the seriousness of the offence, its nature, effect and impact in deciding whether to call the Police. If Police intervention is thought necessary, or likely, they should be informed at the earliest possible stage. Advice should be sought from the Police, or the Authority's Solicitor, if necessary. Contact should be maintained by the Investigation Officer until any investigation has been concluded.

4.8 Contact Telephone Numbers

Internal

Head of Resources	Ext 266354
Monitoring Officer (Director of Sustainable Development)	Ext 2622
Head of People and Organisation Development	Ext 260349

External

Chief Internal Auditor – TIAA Ltd	0845 300 3333
Cumbria Police (ask for the Fraud Office)	0845 330 0247

4.9 Prosecution Policy

It is Authority policy that any apparent criminal activity committed against this Authority will be referred to the Police, or other appropriate enforcement agency.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

Section 5 - Authority Guidelines

List of Guidelines

The Authority has various guidelines which are designed to give a framework for internal control and to ensure that sound systems are in place. It is important that all Members and employees are aware of the content of these guidelines. The most important documents in respect of anti-fraud and corruption are:

- Financial Regulations
- Standing Orders
- Code of Conduct for Members
- Code of Conduct for Officers
- Confidential Reporting Policy (Whistleblowing)

Section 6 – Updating the Policy

6.1 This policy will be amended every 3 years, or as necessary to keep up to date with regulatory guidance. Any revisions to the policy, outside of the scheme of delegation will be considered by the Governance Committee.

6.2 In drafting the amended version, the Authority Solicitor will consult as appropriate:

Directors
Heads of Service
Internal Audit
Key officers on property sales and cash collection.

If you have any queries on the content of these guidelines, please contact the Authority Solicitor or Section 151 Officer.

Version	Author	Revised	Changes
v.1 Original	**Julie Wood**	**24/03/2023**	
v.2	**Julie Wood**	**28/07/2025**	Reviewed and amended to correct

			grammatical and spelling errors Amended to reflect changes to organisational structure. Introduction of a zero-tolerance statement. Reference to training included. Clarification of sanctions.