



BURY COUNCIL

ANTI-FRAUD AND CORRUPTION STRATEGY

**EXECUTIVE DIRECTOR OF RESOURCES &
REGULATION**

REVISED MAY 2019

CONTENTS

INTRODUCTION

PART 1 – POLICY AND STRATEGY

PART 2 – CONFIDENTIAL REPORTING (WHISTLEBLOWING)

POLICY (Updated May 2019)

PART 3 – HOUSING BENEFIT/COUNCIL TAX BENEFIT – FRAUD

PROSECUTION POLICY

PART 4 – STANDARDS OF CONDUCT – (LOCAL GOVERNMENT ACT
2000 PART III)

PART 5 – GUIDANCE FOR MEMBERS AND OFFICERS ON HOW TO
REPORT SUSPECTED FRAUD AND CORRUPTION WITHIN OUTSIDE
BODIES

PART 6 – LOCAL CODE OF CORPORATE GOVERNANCE

ANTI-MONEY LAUNDERING GUIDANCE

ANTI-BRIBERY POLICY

INTRODUCTION

Bury Council, in carrying out its functions and responsibilities, has always subscribed to a culture of openness and fairness and has expected that elected Members and employees at all levels will observe the highest standards of propriety and accountability. This is part of the ethos at Bury Council and is underlined by strong systems of internal control, including standing orders and financial regulations. Following the 1995 Nolan Report and subsequent legislation and regulations about how to improve ethical standards in public life including several well publicised fraud and corruption cases, it became accepted that standards and practices needed to be formalised and developed into a distinct anti-fraud and corruption strategy.

This strategy started life as a series of short statements declaring the Council's determination to root out and deal with fraud and corruption. It has gradually evolved into a compendium of strategies, setting out the various measures across the Council designed to combat fraud and corruption, and bringing them together in one document.

It is recognised that each of the parts making up this overall strategy will often need to be considered in their own right, without direct reference to the others. The strategy has therefore been produced in sections, so that each can be removed as a stand-alone document when required.

At the present time the strategy contains:

- Part 1: Policy and Strategy – a general section setting out the Council's stance with regard to fraud and corruption, and how it will be dealt with.
- Part 2: Confidential Reporting (Whistleblowing) Policy – setting out the arrangements in place for raising issues without fear of reprisal.
- Part 3: Housing Benefit/Council Tax Benefit Fraud Prosecution Policy – setting out the specific arrangements in place for this specialist area of work.
- Part 4: Standards of Conduct – a section dealing with Codes of Conduct under the Local Government Act 2000.
- Part 5: Guidance for Members and Officers – requested by Members to cover working with outside bodies.
- Part 6: Local Code of Corporate Governance – detailing the Council's Corporate Governance Framework.
- Part 7: Anti-Money Laundering Guidance – outlining the legal and regulatory framework and good practice.

- Part 8: Anti-Bribery Policy – setting out the Council’s stance on bribery in a coherent and consistent framework.

Copies of all the above policies can also be found on the Bury Council website within the Council Constitution:

<https://www.bury.gov.uk/index.aspx?articleid=10492>

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 1 – POLICY AND STRATEGY

POLICY

The public is entitled to expect conduct of the highest standard from Members and Officers of the Council. Bury Council recognises the need for the highest standards of probity in dealing with public money and is firmly committed to the prevention, detection and investigation of all forms of fraud and corruption. It will deal equally with perpetrators from inside and outside the Council. This strategy and all its individual measures will not compromise the Council's Equalities Policy or the requirements of the Human Rights Act 1998.

DEFINITIONS

- ***Fraud:***

"Those intentional distortions of financial statements or other records which are carried out to conceal the misappropriation of assets or otherwise for gain".

The "intentional" nature of the act distinguishes it from simple error.

- ***Corruption:***

"The offering, giving, soliciting or acceptance of an inducement or reward which may influence the actions taken by the authority, its Members or Officers".

FRAUD ACT 2006

The Act creates a new general offence of fraud.

There are three ways of committing the new offence of fraud:

- False representation
- Failing to disclose information
- Abuse of position

False representation

Any representation as to fact or law, express or implied, which they know to be untrue or misleading.

Failing to disclose information

Where a person fails to disclose information to a third party when they are under a legal duty to do so.

Abuse of position

Where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position – includes cases where the abuse consists of an omission.

The Act creates other new offences as follows:

- Obtaining services dishonestly
- Possessing articles for use in frauds
- Making or supplying articles for use in frauds
- Fraudulent trading by non-corporate traders

Note: this policy is intended to cover all financial and other irregularities, which may affect the Council, including theft. However, it will not compromise the Council's equal opportunities policy or any obligations as an employer under the code of conduct for local government employees.

STRATEGY

This strategy is concerned with the Council's philosophy on fraud and how it will react to fraud, helping to engender an anti-fraud culture throughout the Council. It sets out the various measures set in place to combat fraud and corruption as follows:

- minimising the risk of fraud and corruption arising
- measures taken to detect the occurrence of fraud
- procedures to be observed covering the investigation of fraud when it does arise

MINIMISING THE RISK OF FRAUD AND CORRUPTION

The Control Environment

The key to prevention of fraud is the creation of a sound control environment with well-established and accepted systems and effective controls. This is the approach adopted at Bury, where appropriate systems and controls are established and maintained by management. Members and Officers alike support the anti-fraud and corruption culture throughout the Council.

The Council's Ethical framework, which underpins the operation of the Council, has a number of facets that exist to protect the Council against losses from fraud. These include:-

- A Local Code of Corporate Governance;
- An established Standards Committee and an adopted Code of Conduct for Members;
- The Constitution, Financial Regulations, Standing Orders and the Scheme of Delegation;
- Internal control reviews by Internal Audit;
- A confidential reporting code (the Whistleblowing Policy);
- This Anti-Fraud and Corruption Strategy;
- Policies on the Regulation of Investigatory Powers Act;
- Data protection procedures;
- A complaints procedure;
- Freedom of Information policy;
- Risk assessed pro-active fraud work carried out by Internal Audit;
- Participation in national anti-fraud initiatives and membership of the National Anti-Fraud Network and the AGMA counter fraud Group;
- Effective disciplinary procedures;
- Effective recruitment procedures.

To deliver the Council's objectives, we need to optimise the financial resources available to us. In order to do this we must reduce fraud and misappropriation to a minimum. We seek the strongest possible sanctions against those who seek to defraud the Council. This includes our own Members, Officers, contracting partners and external individuals and

organisations. The Council takes very seriously its responsibilities for protecting our finances and those that we administer on behalf of the Government or the Community. In turn, our managers have a duty to protect their service area from losses due to fraud and irregularity and are responsible for implementing effective internal controls.

The following internal control measures are in force:-

The Monitoring Officer has a duty to report to the Council where it appears that any proposal, decision or omission by the Council, a Committee or Sub-Committee or Officer has given rise to (or is likely to give rise to) a contravention of any enactment, rule of law or statutory code of practice.

The Assistant Director of Resources & Regulation (Finance and Efficiency) has a statutory responsibility under Section 151 of the Local Government Act 1972 to ensure the proper administration of the Council's financial affairs.

Under the Accounts and Audit Regulations 2011 the Council is required to maintain an adequate and effective system of internal audit, to ensure it has a sound system of internal control and must undertake an adequate and effective internal audit of its accounting records and of its system of internal control in accordance with the proper practices in relation to internal control. Additionally, it must, at least once in each year, conduct a review of the effectiveness of its internal audit. This responsibility has been delegated to the Section 151 Officer.

Individual Executive Directors are responsible for ensuring that operational systems and procedures incorporate efficient and effective financial controls. The existence and appropriateness of these controls is independently monitored by Internal Audit.

Standards Committee

The "control environment" in its entirety is overseen by the Council's Standards Committee and embraces a wide range of managerial, financial and operational controls. This function is supported by the Council's Monitoring Officer.

Audit Committee

The Council has established an Audit Committee to oversee all internal and external audit activities relating to the Council and report to Standards Committee. The Council's Head of Financial Management reports directly to this committee.

Internal Audit

Under the guidance and management of the Executive Director of Resources & Regulation, the Council maintains a strong and independent internal audit function to provide a continuous review of systems and controls, and the control environment. Internal Audit reports to the Audit

Committee and is also subject to the scrutiny of the Council's external auditors.

Codified Guidance

Register of Members Interests, Members and Officers Codes of Conduct, the Council's ICT Security Policy and the Council Constitution provide the rules of conduct and a framework within which Members and Officers operate. Regular checks are carried out to ensure compliance with these.

N.B. The Code of Conduct for Members has been produced under the requirements of the Local Government Act 2000 and 2011 Localism Act. Details are shown in Part 4.

Deterrence

There are two elements to fraud, i.e. intent and opportunity. Our main weapon is the removal of opportunity. This, and the certainty that fraud will be rooted out and dealt with, helps to provide a deterrent.

DETECTING THE OCCURRENCE OF FRAUD

Internal Control

Management uses a wide range of control mechanisms as a means of prevention. However, the same controls also serve as a means of detection, and the different levels of scrutiny should assist in the early identification of any form of irregularity. The importance of maintaining controls at all times, particularly during periods of upheaval and changes cannot be over-emphasised.

Systems Testing

Internal Audit carries out tests specifically designed to identify any occurrences of fraud. These include sample testing based on the audit risk assessment, and checks in connection with data matching exercises and are, in addition to the tests, conducted as part of the systems audit process.

N.B. Data matching techniques assist in the prevention and detection of fraud by bringing together and comparing records maintained by public authorities.

Benefit Investigations

A dedicated Investigations and Overpayments team operates within the Resources and Regulation Department for the purposes of investigating Housing and Council Tax Benefit fraud. The team carries out proactive investigatory work, in addition to following up referrals.

N.B. It should be noted that over 95 percent of discovered fraud, in local government, relates to benefits.

Information Received

Irregularities that do come to light are often discovered as a result of information received from a range of sources. In particular, surveys have shown that employees often have knowledge, information or concerns, which for various reasons they are reluctant or afraid to pass on. The Council's Whistleblowing Policy (see Part 2) sets out the procedures for dealing with such concerns in a discreet and sympathetic manner and is designed to emphasise joint ownership of the "control environment". Whilst seeking to discourage any form of mischievous or malicious allegation, the Council will treat seriously any information received, and will endeavour to investigate information provided, whatever the source.

REPORTING AND INVESTIGATING FRAUD

Suspicion of Fraud

Detection of fraud is primarily a management responsibility, although there are several ways in which fraud can come to light. When an irregularity is suspected by management, procedures for notification are clearly set out in Financial Regulations.

Extract (4.3) from Financial Regulations:

"Whenever any matter arises which involves, or is thought to involve, irregularities concerning cash, stores or other property of the Council, or any suspected irregularities in the exercise of the functions of the Authority, then the Chief Officer concerned shall forthwith notify the Chief Executive and the Executive Director of Resources & Regulation who shall take such steps as they consider necessary by way of investigation and report."

Notification of Fraud

In practice the Chief Officer concerned will usually inform the Head of Financial Management who will consult the Assistant Director - Legal and Democratic Services. Any suspected frauds, discovered as a result of Internal Audit activity, will be reported to the appropriate level of management by the Head of Financial Management.

Liaison with Police

Advice will need to be given regarding police involvement. If there are immediate indications of criminal activity at the outset, then the police must be informed immediately. Otherwise, advice will be offered as the investigation proceeds. Internal Audit will maintain links with the local police and will make the necessary arrangements for police involvement.

Suspension

It may become necessary to suspend one or more Officers if the presence of such Officer(s) would impede an investigation, or be likely to lead to the loss or destruction of evidence. This is a management responsibility, in accordance with disciplinary procedure, but appropriate advice will be available from Personnel and Internal Audit.

Investigation

The Head of Financial Management and the Assistant Director - Legal and Democratic Services, after consultation with any other appropriate Chief Officer, will advise the reporting Chief Officer on the need for, and the conduct of, further investigations. Internal Audit will assist with, or conduct the investigation, if this is considered necessary. In any event they will need to be kept fully informed of any developments. This communication is essential. Incorrect procedures in the course of an investigation, particularly when conducting interviews, may render the evidence inadmissible at a later date. The Assistant Director - Legal and Democratic Services will advise on the application of PACE (the Police and Criminal Evidence Act), which contains specific provision for the conduct of interviews under caution. As a general rule all such interviews will be conducted by the police, who have the necessary facilities and expertise.

Benefit Fraud Investigation

The one exception to the above procedures is in respect of benefit frauds. The Resources and Regulation Department has its own Benefits Investigations and Overpayments team, trained to deal with benefits fraud and to interview under caution when necessary. Any decision to prosecute, as a result of such an investigation, will be taken in accordance with the Bury Council Housing Benefit/Council Tax Benefit Fraud Prosecution Policy (see Part 3), and will be the subject of a private prosecution.

Whistleblowing

Procedures are set out in Part 2.

Outside Bodies

Membership of outside bodies is a regular feature of duties performed by Members and Officers of the Council. Guidance is given in Part 5.

Disciplinary Procedures

It should be clearly understood that investigations carried out under Financial Regulation number 4 are entirely separate from the Council's disciplinary procedures. Following an investigation/report a Chief Officer may initiate action under those procedures. The investigation may lead to criminal proceedings, which can become a lengthy process, and which will usually require a higher degree of proof than that required in disciplinary

action. The outcome of one is not always dependent on the other, and disciplinary action should be concluded as quickly as possible, unless advice is specifically given to the contrary. The Assistant Director - Legal and Democratic Services will advise if such action is likely to jeopardise any other proceedings.

Guidance for Disciplinary Hearings

When an employee has been found to have committed an act of gross misconduct, involving theft from any client of the Council, member of the public, or other party, then the action to be taken should be in accordance with the Council's Disciplinary Procedure which states "offences of gross misconduct may lead to dismissal". The Council, whilst being fair, must equally also be seen to be firm and consistent.

Recovery of Losses due to Fraud

The Council will seek to recover all funds obtained fraudulently from the Council either from the individual/s concerned, (e.g. recovery of allowances through the Payroll which are found to be fraudulent), or through the Council's insurance policy.

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 2 – CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY (Updated May 2019)

1.0 INTRODUCTION

1.1 Whistleblowing is the raising of a concern, either within the workplace or externally, about a danger, risk, malpractice or wrongdoing or illegality which affects others. This can include:

- a criminal offence (e.g. fraud, corruption etc.) may have or has been committed;
- a miscarriage of justice has been or is likely to occur;
- abuse/harassment of a service recipient or council employee is taking place. Note where a child or vulnerable adult is the recipient of such treatment "Safeguarding" procedures could apply, please note these alternate procedures also adhere to the principles of this strategy.
- For adult safeguarding contact 0161 253 5151 or email adultcareservices@bury.gov.uk.
- For child safeguarding (aged under 18), please contact 0161 253 5678 or email childwellbeing@bury.gcsx.gov.uk.
- Unethical conduct and actions deemed unprofessional or inappropriate. This could include for example, Officers or Councillors attempting to use their position to influence political or professional practices or decisions, or could include breaches of regulations requiring School Governors to 'act with integrity, objectivity and honesty and in the best interests of the school' and breaches of the 'Nolan Principles' which are the basis of ethical standards expected of public office holders. (Appendix A);
- public funds are being used in an unauthorised manner;
- the environment has been, or is likely to be, damaged;
- the council's own rules have been or are being breached;
- abuse (e.g. physical or verbal) of a service recipient or council employee is taking place;
- discrimination towards a service recipient, (e.g. disability, race, gender).

- 1.2** The Nolan Committee on Standards in Public Life made clear recommendations that local authorities should adopt 'whistleblowing' procedures, and the Public Interest Disclosure Act (PIDA) 1998 (and subsequent Enterprise and Regulatory Reform Act 2013) gave protection to 'whistleblowers' who are treated unfairly.
- 1.3** Additionally, the Whistleblowing Commission, established in 2013 by whistleblowing charity Public Concern at Work, has developed a Code of Practice for effective whistleblowing arrangements. Bury Council's Whistleblowing Policy complies with this Code of Practice.
- 1.4** Employees are often the first to realise that there may be something seriously wrong within their workplace or within a Department of the Council itself. However, they may choose not to express their concerns if they feel that by speaking out it would be disloyal to their line manager(s), colleagues or to the Council, or if they fear harassment or victimisation. In such circumstances it may be easier to ignore the concern rather than report what may just be a suspicion of malpractice.
- 1.5** The Council's Whistleblowing Policy is a vital element of our governance arrangements. The Council is committed to the highest possible standards of honesty, openness, probity and accountability and will not tolerate malpractice or wrongdoing. In line with that commitment, employees and others with serious concerns about any aspect of the Council's work (including activities within schools or by voluntary staff, and Members), are encouraged to voice them. In so doing it is recognised that in certain cases they will have to proceed on a confidential basis.
- 1.6** This policy applies to all staff working for the Council, both full and part-time, temporary and casual including those that are based within the Council's schools and within aided and foundation schools. It also covers Council Members, School Governors and agency and contractors' staff. References to 'employees' within the Policy covers all of these categories.
- 1.7** This policy makes it clear that employees should be encouraged and enabled to raise serious concerns within the Council without fear of reprisal, rather than overlooking a problem or blowing the whistle outside. It is intended to help build an environment of openness within the Council.
- 1.8** If you are not a Council employee you can still contact the Council to report any concerns or disclosures over wrongdoing and these will be treated in the same way. Unlike disclosures made by employees, protection under PIDA law does not extend to disclosures made by Members of the Public. Please see separate document "Whistleblowing Arrangements for the General Public" on the Bury Council website.
- 1.9** The policy has been subject to local consultation with appropriate trade unions and professional associations and has their support.

2.0 AIMS AND SCOPE OF THIS POLICY

2.1 The policy aims to:

- provide an avenue for all those to whom the policy applies to raise concerns and receive feedback on any action taken;
- allow them to take the matter further if they are dissatisfied with the response received;
- reassure them that they will be protected from reprisals or victimisation for confidential reporting an incident where the employee has a reasonable belief that the matter is in the public interest. Such an act will be covered by "protected disclosure".

(Definition of protected disclosure – a source of information that the worker reasonably believes tends to show malpractice. It does not have to be true, as long as the worker reasonably believes it to be true).

The Enterprise and Regulatory Reform Act 2013 goes on to state that the disclosure must "in the reasonable belief of the worker making the disclosure" be "made in the public interest".

2.2 There are existing procedures in place for employees to legitimately complain about harassment, violence and aggression, discrimination and instances where they feel that they have a grievance. The Confidential Reporting Policy is intended to cover concerns that fall outside the scope of other procedures.

2.3 Part IV of the Employment Rights Act 1996 – The Public Interest Disclosure Act – sets out a framework for staff to make disclosures about various categories of wrongdoing, provided they reasonably believe it to be in the public interest to do so:

- a criminal offence
- failure to comply with statutory or legal obligations
- improper or unauthorised use of public or other funds
- a miscarriage of justice
- endangering health and safety
- damage to the environment
- maladministration, misconduct or malpractice
- deliberate concealment of any of the above

2.4 The disclosure will be protected if the member of staff discloses:

- a) in course of obtaining legal advice;
- b) to the employer;
- c) in certain circumstances, to a Minister of the Crown;
- d) to a 'prescribed person', reasonably believing that the information and any allegation contained within it is substantially true. The Secretary of State (for Business, Innovation and Skills) prescribes by list both the identity of the prescribed person (usually regulatory body) and its remit;
- e) to any person or body provided that a number of detailed conditions are satisfied. Those conditions include a requirement that the worker does not make the disclosure for purposes of personal gain and a requirement that it is reasonable to make the disclosure in the circumstances. A further section makes provision for a disclosure of an exceptionally serious failure to any person or body.

2.5 The Public Interest Disclosure Act makes it unlawful for an employer to dismiss or subject a worker to a detriment for having made a 'protected disclosure' of information. The protection provided by the Act is not subject to any qualifying period of employment and so is referred to as a 'day one' right in employment law. By contrast under ordinary unfair dismissal, there is a two year qualifying period.

2.6 Alternatively, the disclosure may be related to any breach of the Council's Standing Orders, Financial Regulations, policies or agreed procedures, including those relating to Governing Bodies.

2.7 The overriding concern should be that it would be in the public interest for malpractice to be corrected and, if appropriate, sanctions applied.

3.0 HOW TO RAISE A CONCERN

3.1 As a first step, you should normally raise concerns with your immediate manager or their line manager. This may include Head Teachers, Chairs of Governing Bodies or other senior Officers of the Council. However, much depends on the seriousness and sensitivity of the issues involved, and who you think is involved in the malpractice. If, for example, you believe that your own line manager or supervisor is involved, then you may prefer to approach a manager or supervisor from another unrelated service. You may also contact your trade union, departmental HR team or corporate HR.

3.2 In any event you may also approach one of the following Officers, in confidence, to raise a specific concern or to obtain advice and guidance on how matters of concern may be pursued:

- Chief Executive – Geoff Little, Tel: 0161 253 5102
- Section 151 Officer, Tel: 0161 253 5002
- Assistant Director - Legal and Democratic Services - Jayne Hammond, Tel: 0161 253 5002
- Head of Financial Management / Chief Internal Auditor - Andrew Baldwin, Tel: 0161 253 5034
- Assistant Director of Resources and Regulation (HR and OD) – Tracy Murphy, Tel: 0161 253 7775

3.3 Alternatively, you can call the dedicated Whistleblowing telephone number on 0161 253 6446 or email: Whistleblowing@bury.gov.uk.

3.4 You may also take the matter outside the Council to one of the bodies referred to in section 6.

3.5 Whilst concerns are best raised in writing they can also be expressed verbally through a telephone call. Where a concern is expressed verbally an employee can also ask for a meeting with an appropriate person.

3.6 In any event, as much information as possible should be given and this should include:

- the background to the concern;
- names of individuals, dates and places where applicable;
- the reasons why there are concerns.

3.7 The earlier you express the concern, the easier it is for action to be taken.

3.8 Although you are not expected to prove the truth of an allegation, you will need to demonstrate to the person contacted that there are sufficient grounds for your concern.

3.9 An employee making a complaint about their contract of employment should not use this policy but refer to the grievance procedures.

3.10 We aim to encourage openness and will support anyone who raises a genuine concern under this policy. Support can be through various means, for example counselling, coaching and mentoring.

4.0 HOW THE COUNCIL WILL RESPOND

4.1 Any Officer that receives a concern must make a full written note of the points raised and then pass on the concern to one of the Officers listed in paragraph 3.2.

4.2 Careful consideration will then be given to the matter and to the action to be taken depending upon the nature of the concern. In order to protect individuals and the Council, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take.

4.3 The action taken by the Council will depend on the nature of the concern. The matters raised may:

- be investigated internally (see paragraph 4.4 below)
- be referred to the Police
- be referred to Mazars (external auditor)
- form the subject of an independent inquiry.

4.4 Because of the specific responsibilities of Governing bodies, concerns relating to schools will be the subject of separate investigatory procedures. These may involve the Head Teacher of the relevant school, the Chair of the Governing Body (in conjunction with the Director of Learning), and one of the Officers referred to in paragraph 3.2.

4.5 Concerns or allegations that fall within the scope of specific procedures will normally be referred for consideration under those procedures. Allegations relating to child abuse for example will be dealt with in accordance with the Bury Safeguarding Children's Board Confidential Reporting (Whistle-blowing) Policy.
<http://intranet/CHttpHandler.ashx?id=16970&p=0>

4.6 Some concerns may be resolved by agreed action without the need for investigation.

4.7 Within ten working days of a concern being received, the Council will write to you:

- acknowledging that the concern has been received;
- indicating how it proposes to deal with the matter;
- giving an estimate of how long it will take to provide a final response, telling you whether any initial enquiries have been made, and telling you whether further investigations will take place, and if not, why not.

4.8 The amount of contact you have with the Officers considering the issues will depend on the nature of the matters raised, the potential

difficulties involved, and the clarity of the information provided. If necessary, further information will be sought from you in a discreet manner.

4.9 When any meeting is arranged, you can be accompanied by a trade union representative, an official employed by a trade union, or by a companion who is a fellow worker, if you wish. It is your responsibility to make these arrangements.

4.10 The meeting can be off site if requested.

4.11 The persons investigating the concerns will produce a written report that:

- outlines the complaint;
- details the investigation process;
- gives the outcome of the investigation;
- details recommendations where appropriate.

4.12 The Council accepts that employees need to be assured that the matter has been properly addressed. Thus, subject to legal constraints and confidentiality issues, you will receive information about the outcomes of any investigations.

4.13 If the person who expressed the concern is not satisfied with the outcome they have a right to take matters further as explained in section 6 of this policy.

4.14 The Council will take steps to minimise any difficulties that you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings, the Council will advise you about the procedure.

5.0 SAFEGUARDS

Harassment or Victimisation

5.1 The Council recognises that the decision to report a concern is not an easy one to make, not least because of the fear of reprisal from those reported for the malpractice. The Council will not tolerate harassment, bullying or victimisation based upon race, religion or belief, gender, gender reassignment, sexual orientation, disability and age from employees, managers or governors, and will take appropriate action, including the application of the Disciplinary Procedure, to protect an employee who raises a concern that they reasonably believe to be "in the public interest".

5.2 In accordance with Part IV of the Employment Rights Act 1996 - The Public Interest Disclosure Act - an employee cannot be dismissed or selected for redundancy as a result of making a disclosure that they

reasonably believe to be “in the public interest”. In addition, an employer cannot withhold a pay rise, object to a promotion or not give training. Other examples that will not be tolerated where a member of staff is disadvantaged because they blew the whistle could include (but is not limited to) ostracism, closer monitoring, blocking access to resources, unrequested re- assignment or re-location, demotion, suspension, failure to provide an appropriate reference and failure to investigate subsequent concern.

- 5.3** This does not mean that if an employee is already the subject of disciplinary or redundancy procedures that those procedures will be halted as a result of confidential reporting.

Confidentiality

- 5.4** The Council will respect confidentiality and all steps will be taken to ensure that confidentiality is maintained throughout the process. However, it must be appreciated that the investigation process may reveal the source of the information. Any statement made by you may be required as part of the evidence.

Anonymous Allegations

- 5.5** The Council would encourage employees to put their name to allegations because concerns expressed anonymously are much less powerful. However, the Council also recognises that some employees would not wish to do this. Where a concern is expressed anonymously it will be considered at the discretion of the Council and in exercising this discretion the factors to be taken into account would include:

- the seriousness of the issue(s) raised
- the credibility of the concern
- the likelihood of confirming the allegation from attributable sources.

Untrue Allegations

- 5.6** If an employee makes an allegation that they reasonably believe to be “in the public interest” but it is not confirmed by the investigation, no action will be taken. If however, an employee makes a malicious or vexatious allegation, disciplinary action may be taken.

6.0 HOW THE MATTER CAN BE TAKEN FURTHER

- 6.1** This policy is intended to provide you with an avenue to raise concerns **within** the Council, and the Council hopes you will be satisfied with the response to your concern. **If you are not satisfied with the response, please indicate this to the Chief Executive.**

If you feel it is right to take the matter outside the Council, the list below shows possible contact points:

- any Member of the Council
- any Member of the Governing Body (in the case of any issue relating to a school)
- external auditor (Mazars) (telephone 0161 238 9200)
- relevant trade unions, professional bodies or regulatory organisations eg. UNISON, Ofsted, Care Quality Commission
- your solicitor
- the Police

6.2 If, at any stage, you are unsure whether to use this procedure, or decide that you need independent advice, you may seek advice from the independent charitable body 'Public Concern at Work'. This organisation operates a help-line and a mediation service and can be contacted on 0207 404 6609. They can give you free, confidential advice at any stage of the process. For further information visit www.pcaw.org.uk

6.3 If you do take the matter outside the Council, then you need to ensure that you do not disclose confidential information, or that disclosure would be privileged. You can check this with one of the contact points listed in section 3.2.

6.4 If concerns are raised through professional bodies, or trade unions, then it is expected that the professional body/trade union representatives will act in accordance with this policy, and with the Public Interest Disclosure Act, with regard to the information disclosed. Such a disclosure made by an employee will not be treated as grounds for disciplinary proceedings.

7.0 DATA PROTECTION AND FOI

7.1 The Freedom of Information Act 2000 gives a general right of access to all types of recorded information held by Public Authorities. As such the Council often receives requests for information under the Freedom of Information Act.

7.2 The Council has a legal obligation to provide the information unless it falls under one of the exemptions of the Act.

7.3 The Freedom of Information Act contains exemptions which may be applicable to permit the withholding of information identifying the whistleblower, including:

- Section 40 Personal Data
- Section 41 Information which, if disclosed, would give rise to an actionable breach of confidence.

7.4 Many people making a disclosure to the Council will wish to protect their identity and the Council will always seek to protect the identity of individuals during the course of progressing an investigation. If the Council receives a request for information identifying a whistleblower, the Council will contact the whistleblower to seek their views beforehand and will, wherever possible, seek to comply with those views.

7.5 The principle of maintaining confidentiality should also be applied to the identity of any individual who may be the subject of a disclosure.

7.6 The Council will ensure that our handling of concerns meets the requirement of the General Data Protection Regulations and Data Protection Act 2018 and the Freedom of Information Act 2000.

8.0 THE RESPONSIBLE OFFICER

8.1 Internal Audit will maintain a central record of all whistleblowing referrals made under this policy and monitor the outcome of these cases. All records will be held securely and confidentially.

8.2 As such, details of any allegation should be reported to Internal Audit by the receiving manager on receipt. Internal Audit will log and allocate each case a reference number whether or not Internal Audit are involved in the investigation work. The outcome of the investigation should be notified to Internal Audit by the Investigating Officer.

8.3 The records held by Internal Audit will be used to analyse the impact and effectiveness of the arrangements in place in statistical terms and records held in HR sections may be subject to review. The detailed case records form part of the process of reporting back to Members on the effectiveness and outcomes of the Policy and form the record of actions taken in the case of any matters raised under the Public Interest Disclosure Act. The information will be referred to for monitoring purposes and periodic assurance reports provided to the Audit Committee by the Head of Financial Management as part of this process.

8.4 A whistleblowing record sheet (Appendix B) should be used to record a summary for each case. A copy should be sent to Internal Audit and one retained with the investigation paperwork on completion.

8.5 The Chief Executive has overall responsibility for the maintenance and operation of this policy, and monitoring the effectiveness of the

Council's Whistleblowing Policy and Process. The Standards Committee has an overview of the Whistleblowing Policy.

9.0 TRAINING AND AWARENESS

9.1 Chief Officers and Heads of Service are responsible for ensuring that their employees are aware of the whistleblowing policy and process and that any training needs are addressed which may arise from the application of the policy. Raising awareness of the Council's Whistleblowing Policy should form part of the induction training for all employees and should be addressed as refresher training for all employees.

9.2 Employees have a responsibility to ensure that they are aware of and understand the Council's policy in relation to Whistleblowing.

10.0 REVIEW

10.1 This policy will be subject to annual review in consultation with the appropriate trades unions. A summary of concerns raised under this policy will be prepared on an annual basis and shared with the trades unions during the review.

Appendix A

SEVEN NOLAN PRINCIPLES

The following are the Seven Nolan Principles underpinning standards for Public Life:

The principles of public life apply to anyone who works as a public office-holder. This includes all those who are elected or appointed to public office, nationally and locally, and all people appointed to work in the civil service, local government, the police, courts and probation services and in the health, education, social and care services. All public office-holders are both servants of the public and stewards of public services. The principles also have application to all those in other sectors delivering public services.

1. Selflessness: Holders of public office should act solely in terms of the public interest.
2. Integrity: Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.
3. Objectivity: Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.
4. Accountability: Holders of public office are accountable to the public for their decisions and actions and must admit themselves to the scrutiny necessary to ensure this.
5. Openness: Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.
6. Honesty: Holders of public office should be truthful.
7. Leadership: Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

**Source: The Committees website is at
<http://www.public-standards.gov.uk/>**

Appendix B

CONFIDENTIAL

BURY COUNCIL

WHISTLEBLOWING CASE RECORD

The date the concern/allegation / disclosure was received in the Council Department involved How the report was received (verbal or written)	
Details of who the concerns were raised with? Name and job role	
Name and job role of employee making complaint / allegation (unless anonymity was requested)	
Was confidentiality requested / explained or promised?	

A summary of the concern / allegation raised:	
Details of any feedback given and any response from the employee	
Matter reported to Head of Internal Audit (Yes / No) Date referred:	
Has formal acknowledgment been provided to employee in line with the policy? (Acknowledgement of receipt within 10 working days).	

Chief Officer and Officer(s) handling the investigation (Names)	
Summary outcome of the investigation (Proved / not proved, action plans and recommendations)	
Date notification of outcome given to employee	
Papers retained (location), responsible officer and review date.	

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 3 – HOUSING BENEFIT/COUNCIL TAX BENEFIT – FRAUD PROSECUTION POLICY

1.0 INTRODUCTION

In order to provide an effective counter fraud deterrent the Council must apply appropriate sanctions to those people found to have committed an offence. There are three sanctions that the Council can apply: Prosecution, Administrative Penalty and Simple Caution.

PROSECUTION

- 1.1** The Council has the right to prosecute or appear in any legal proceedings under section 222 of the Local Government Act 1972.
- 1.2** The Council to prosecute fraudulent HB/CTB claimants or offer any other form of sanction as deemed appropriate is a matter delegated to the Executive Director of Resources & Regulation.
- 1.3** The prosecutions will be brought on behalf of the Council in the name of the Council Solicitor, on the instructions of the Executive Director of Resources & Regulation. The Council Solicitor is obliged to consider and review the decision to prosecute in accordance with the criteria set down in the Code of Conduct for Crown Prosecutors. The Law Society Practice Rules require observance of this Code by all prosecutors.
- 1.4** Referrals may also be made in certain circumstances to the Department for Work and Pensions who may take the Council's case into account whilst taking a prosecution for other fraudulently claimed benefits, or to the police, as appropriate.

ADMINISTRATIVE PENALTY

- 1.5** An Administrative Penalty is a fine set at 30% of the amount of benefit overpaid. This option is a viable alternative to prosecution if the amount involved is low, the period of the offence is short, there appears to have been no attempt to defraud the system, or the person's health is an issue.

CAUTION

- 1.6** Cautions serve as a 'half way house' in cases where the offence is too serious to drop but where there are other considerations

indicating that a prosecution may not be appropriate. These could be sympathetic considerations or a first time offence.

2.0 SPECIFIC PRINCIPLES

- 2.1** In all cases of fraud the Council will actively consider Prosecution, Administrative Penalty or a Formal Caution. In coming to a decision between the three options the Council will have regard to the sums involved, and where the penalty or caution is refused, proceed to prosecution having regard to the issues outlined in the following section.
- 2.2** In all cases a report will be prepared by the Investigations Officer for consideration by the Collections & Investigations Manager who will in turn sanction and progress the appropriate course of action. Once a case is considered appropriate for the application of a sanction, a decision will be taken whether to prosecute, levy an Administrative Penalty or apply a Caution, having regard to the sums involved and the individual circumstances of the person involved.
- 2.3** In deciding whether a case is suitable for the application of a sanction the Council will take a number of issues into account, and these are outlined in section 3.

3.0 ISSUES TO BE TAKEN INTO ACCOUNT

In this section appropriate Officers shall mean the Collections & Investigations Manager, Investigations Officer, Council Solicitor or other Officer involved in a decision to apply a sanction as the appropriate method of disposal following an investigation.

3.1 *When considering a case for the application of a sanction or closure of a case, appropriate Officers shall have regard to the following: -*

(i) Strength of the evidence obtained

Evidence may be defined as something that tends to prove a fact. Substantive evidence is essential for a successful conviction e.g. an employer may be required to produce wage records in court. In any case the Council Solicitor would review the evidence when asked to prosecute on behalf of the Council.

(ii) Failure in investigation

This will include cases where all the correct legal requirements have not been followed.

3.2 *Once the issues shown at 3.1 have been considered, the appropriate Officers will then have regard to all or some of the following issues, which are not necessarily in hierarchical order:-*

(i) The amount of money obtained and the duration of

the offence

It is not normally practical to prosecute where the amount of the overpayment is less than the cost of proceedings; however Formal Cautions or Administrative Penalties remain an option. However, the amount of the overpayment may be disregarded in the case of a persistent offender or any other case where prosecution may be warranted. For example, where prosecution may have a significant deterrent effect, or where the type of fraud is prevalent in this area.

(ii) The offender's physical or mental well-being

Sanctions should not be pursued where it is considered that personal or mental health problems have contributed to the reasons for committing the offence. Detrimental effects to the person's health as a result of sanction proceedings must also be considered. Obvious examples include heart disease, nerves (including threat/suspicion of suicide), individuals with perceived or known low mentality or any case where it appears that health would be affected detrimentally.

(iii) Voluntary disclosure

Voluntary disclosure only occurs when a claimant, of his or her own free will, reveals a fraud of which Bury Council was unaware. Disclosure will not be deemed to be voluntary when, for example, the issue of a benefit review form has solicited or prompted the disclosure in some way.

(iv) Any previous incidence of fraud

Where fraud has been established in the past, including cases where a sanction may or may not have been applied.

(v) Failure in benefits administration, including unreasonable delay

It is recognised that under the Social Security Administration Act 1992 that making a false claim is an offence irrespective of whether benefit is obtained. Where in the view of appropriate Officers some failure in benefits administration has allowed a fraud to succeed e.g. where benefit is paid on incomplete information, where if the information had been complete and verified, the benefit may not have been paid.

(vi) Social factors

Where, for example, in the view of appropriate Officers of the Council, the suspect may have committed the fraudulent action by a particularly stressful domestic situation, having regard to par 6.2 of the Code of Conduct for Crown Prosecutors (as referred to at 1.3 to this Policy) which states that "often the prosecution should go ahead and those factors be put to the court for consideration when sentence is being passed".

3.3 A case will not be deemed unsuitable for the application of a sanction simply because those involved have, or are in a position to repay, the amount owing.

4.0 *FUTURE ARRANGEMENTS*

4.1 Fraud investigation will change significantly from April 2015 when housing benefit fraud investigation will be transferred to a new national Single Fraud Investigation Service (SFIS) under the Department for Work and Pensions. Council tax support fraud investigation will continue in the form of corporate fraud and arrangements to take this forward are currently being worked on.

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 4 – STANDARDS OF CONDUCT – (LOCAL GOVERNMENT ACT 2000 PART III)

CODES OF CONDUCT

The Council is determined to provide excellent local government for the people of the Borough.

It promotes and maintains high standards of conduct by Members and Co-opted Members and has adopted a Code of Conduct for Members, in line with its obligations under section 27(2) of the Localism Act 2011. The Council also has a Protocol for Member and Officer Relations.

Additionally, local government employees are expected to give the highest possible standard of service to the public, and where it is part of their duties, to provide appropriate advice to Councillors and fellow employees with impartiality. Employees will be expected, through agreed procedures and without fear of recrimination, to bring to the attention of their immediate supervisor any deficiency in the provision of service. As such a Code of Conduct for Employees has also been established.

The Employees Code of Conduct sets out provisions relating to the disclosure of information, personal interests, equality issues, the need for political neutrality, relationships with Councillors & contractors, gifts and hospitality.

Copies of each Code of Conduct can be found on pages 227 to 247 of the Council Constitution, a copy of which can be found on the Bury Council website at:

<https://www.bury.gov.uk/index.aspx?articleid=10492>

Both sets of Codes of Conduct enhance Part III of the Local Government Act 2000 which established arrangements governing the standards of conduct of Members.

The Council adopted a Code of Conduct for Councillors and Other Voting Representatives in April 2002 (revised July 2012). Local Authorities must publish their Codes of Conduct and make them available for public inspection.

The Code of Conduct is based on the general principles of selflessness, honesty & integrity, objectivity, accountability, openness, personal judgement, respect for others, duty to uphold the law, stewardship and leadership.

Any newly elected Members to a Council will be required to declare that they will follow the Council's Code of Conduct when making their declaration of acceptance of office under Section 83 of the Local Government Act 1972.

The Code also sets out provisions relating to disclosure of pecuniary interests relating to the business of the Council, which if not notified and declared may attract criminal penalties.

Part III of the Act also requires each Local Authority to establish its own Standards Committee which will be responsible for promoting and maintaining high standards of conduct by Members and Co-opted Members of the Council. The membership of the Standards Committee must include two Members of the Council and at least one person who is not a Member or an Officer of the Council.

Disciplinary Procedures

Allegations that a Member has failed, or may have failed, to comply with the Council's Code of Conduct, will be the subject of referral to the Monitoring Officer, who will consult with the Council's Independent Person and decide what action to take.

The Monitoring Officer will also be responsible for ensuring that a Register of Interests of Members is maintained.

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 5 – GUIDANCE FOR MEMBERS AND OFFICERS ON HOW TO REPORT SUSPECTED FRAUD AND CORRUPTION WITHIN OUTSIDE BODIES

INTRODUCTION

Membership of outside bodies has become a regular feature of the duties performed by both Councillors and Officers in Local Government service including voluntary organisations, Local Government Associations and companies.

THE ROLES AND RESPONSIBILITIES OF MEMBERS AND OFFICERS

In carrying out their roles Councillors and Officers will act both as individuals and as representatives of the Council. This means:-

- Acting according to the rules, Constitution and framework set by the outside body
- Making independent and personal judgements in line with their duty of care to the outside body
- Reporting back as necessary to the Council or relevant Committee
- Behaving ethically and following as far as applicable the Code of Conduct for Councillors, Independent and Other Voting Representatives
- Taking an active and informed role in the management of the outside bodies affairs
- Not representing the political party to which the Councillor owes their political loyalty
- To take part in the outside body's discussions and decisions
- Not to look at things simply from the Council's perspective
- To take an active part in meetings and events organised by groups.

In performing these duties and roles, Members may become suspicious or suspect fraud and/or corruption. Dependent on the nature of the outside organisation, Members could find themselves liable if they do fail to report or act upon any suspicions of fraud or corruption.

By and large it will not be the responsibility of the Council to investigate any accusations of fraud and corruption. For the vast majority of organisations with which the Council works, there are regulatory and inspectorate bodies to whom such reports should be made.

Before deciding to formally report any suspicions of impropriety, Members and Officers must seek the advice of the Monitoring Officer (the Assistant Director - Legal and Democratic Services), who will then advise on the most appropriate action to take, and will, on behalf of the Member, inform the relevant regulatory or inspectorate body for the organisation concerned.

METROPOLITAN BOROUGH OF BURY ANTI-FRAUD AND CORRUPTION STRATEGY

PART 6 – LOCAL CODE OF CORPORATE GOVERNANCE

1.0 BACKGROUND

- 1.1** Bury Council recognises that it is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively. In discharging this accountability Members and Officers will be responsible for putting in place proper arrangements for the governance of the Council's affairs and the stewardship of the resources at its disposal.
- 1.2** Effective local government relies on public confidence in elected Councillors and appointed Officers. Good governance strengthens credibility and confidence in public services. The function of governance is to ensure that authorities, other local government organisations or connected partnerships fulfil their purpose and achieve their intended outcomes for citizens and service users and operate in an effective, efficient, economic and ethical manner.
- 1.3** This concept should guide all governance activity. Good governance leads to good management, good performance, good stewardship of public money, good public engagement and, ultimately, good outcomes for citizens and service users.

2.0 THE GOVERNANCE FRAMEWORK

- 2.1** CIPFA/SOLACE (Society of Local Authority Chief Executive's) recognised that local government has been subject to change and reform since the publication of its 2001 document *Corporate Governance in Local Government: A Keystone for Community Governance* and so a revised framework was published in 2007 entitled *Delivering Good Governance in Local Government: Framework*. The revised Framework built upon recent governance work in both the public and private sectors and in particular *The Good Governance Standard for Public Services* drawn up by the Independent Commission on Good Governance in Public Services established by CIPFA and the Office for Public Management (OPM) in partnership with the Joseph Rowntree Foundation.
- 2.2** The Framework emphasises the importance of good governance to the wider outcomes of good management, good performance, and good public engagement. It puts high standards of conduct and leadership at the heart of good governance, placing responsibility on Members and Officers to

demonstrate leadership by behaving in ways that exemplify high standards of conduct, and so set the tone for the rest of the organisation.

2.3 The Framework also defines the principles that should underpin the governance of each local authority but it is not a prescription for a single model of governance. Whatever form of executive arrangements are in place, authorities are urged to test their structures against the principles contained in the Framework by:

- Reviewing their existing governance arrangements against this Framework.
- Developing and maintaining an up-to-date local code of governance, including arrangements for ensuring its ongoing application and effectiveness.
- Preparing a governance statement in order to report publicly on the extent to which they comply with their own code on an annual basis including how they have monitored the effectiveness of their governance arrangements in the year, and on any planned changes in the coming period.

3.0 THE LOCAL CODE OF CORPORATE GOVERNANCE

3.1 A key change from the original Code is the requirement to produce an Annual Governance Statement which will replace the existing Statement of Internal Control.

3.2 The Code has been written and structured in such a way as to feed directly into the Governance Statement i.e. the Code says what we will do, and the Governance Statement will say how we have done it.

3.3 In 2010 CIPFA published an Application Note to the Framework which extended the contents of the Annual Governance Statement to include a specific statement on whether the Council's financial management arrangements conform to the governance requirements and where they do not, to explain why and how they deliver the same impact.

3.4 The Code is structured around 6 core principles:-

- Focussing on the purpose of the Council and on outcomes for the community including citizens and service users and creating and implementing a vision for the local area.
- Members and Officers working together to achieve a common purpose with clearly defined functions and roles.
- Promoting the values of the Council and demonstrating the values of good governance through behaviour.
- Taking informed and transparent decisions which are subject to effective scrutiny and managing risk.

- Developing the capacity and capability of Members to be effective and ensuring that Officers – including the statutory Officers – also have the capability and capacity to deliver effectively.
- Engaging with local people and other stakeholders to ensure robust local public accountability.

4.0 MONITORING AND REPORTING

- 4.1** The Council will undertake regular, at least annual, reviews of its governance arrangements to ensure continuing compliance with best practice as set out in the CIPFA/SOLACE Framework. These reviews are to be reported to the Audit Committee.
- 4.2** The Council will prepare an Annual Governance Statement to be submitted to the Audit Committee and the Council for consideration.
- 4.3** The Council recognises that the Governance Statement should cover all significant corporate systems, processes and controls, spanning the whole range of the Council's activities, including in particular those that are designed to ensure that:
- The Council's practices are implemented in practice;
 - High-quality services are delivered efficiently and effectively;
 - The Council's values and ethical standards are met;
 - Laws and regulations are complied with;
 - Required processes are adhered to;
 - Performance statements and other published information are accurate and reliable;
 - Human, financial and other resources are managed efficiently and effectively.

5.0 RESPONSIBILITIES

5.1 The Monitoring Officer / Assistant Director - Legal and Democratic Services will be responsible for:

- overseeing the implementation and monitoring of the Code;
- Reviewing the operation of the Code;
- Reporting annually to the Standards Committee on compliance with the Code and any changes that may be necessary to maintain it and ensure its effectiveness in practice;

- Preparing an annual Monitoring Officer's Report, which will also form part of the assurance required to be demonstrated in the Annual Governance Statement.

5.2 The Executive Director of Resources & Regulation will be responsible for:

- Reviewing the Code annually, to provide assurance on the adequacy and effectiveness of the Code and the extent of compliance with it. Details of the extent to which the Council is complying with the Code will be included within the Annual Governance Statement.

5.3 The Assistant Director of Resources & Regulation (Finance & Efficiency) will be responsible for:

- Co-ordinating, throughout the year, the Council's internal control assurances, including reporting regularly to Strategic Leadership Team and Audit Committee.
- Co-ordinating the production of an Annual Governance Statement, in accordance with the Accounts and Audit Regulations 2011, which will represent the overall levels of assurance within the Council on behalf of all Members and Officers.

5.4 The Head of Financial Management will be responsible for:

- Reporting annually to the Audit Committee on audit activities during the year, with particular emphasis on the systems of internal control and the arrangements for corporate governance, providing some of the assurance required in the Corporate Governance Statement.

BURY COUNCIL

ANTI-MONEY LAUNDERING GUIDANCE

MARCH 2015

ANTI-MONEY LAUNDERING GUIDANCE

1 Money laundering
2 Anti-money laundering legislation
3 Council's relevant business for the purposes of the legislation
4 Possible signs of money laundering activities
5 Customer Due Diligence
6 Record keeping procedures
7 Internal reporting procedures
8 Educating and Training staff
9 Legal Professional Privilege
10 Data Protection
11 Freedom of Information
Appendix A – Useful websites and documents
Appendix B – External customers
Appendix C – Offences and Penalties
Appendix D – Forms

The purpose of this guidance is to:-

- Outline the legal and regulatory framework of anti-money laundering and counter-terrorist financing obligations.
- Outline good practice on implementing the legal requirements.
- Outline good practice in developing systems and controls to prevent Council Officers being used to facilitate money laundering and terrorist financing.

- Provide direction on applying the risk based approach to compliance effectively in accordance with the practice note issued by the Law Society in September 2007.

LEGAL REQUIREMENTS

1. MONEY LAUNDERING

- 1.1. Money laundering is the method by which cash or funds obtained illegally are passed or “laundered” through financial systems to disguise their criminal origin. The “laundered” funds can then be used for legitimate transactions that do not arouse suspicion. It is a favoured method of organised criminals and terrorists.
- 1.2. In order to make money laundering more difficult the Government has passed laws requiring particular persons, including persons in certain companies and other bodies, to notify the National Criminal Intelligence Service on becoming aware of money laundering activities or suspecting that money laundering activities are taking place. Failure to report such activities can result in criminal prosecution and severe penalties.
- 1.3. Appendix A contains details of the websites of organisations that have published guidance on the anti-money laundering legislation and other useful documents.

2. ANTI-MONEY LAUNDERING LEGISLATION

- 2.1. The legislation is contained in –
 - The Proceeds of Crime Act 2002;
 - The Terrorism Act 2000
 - The Money Laundering Regulations 2007 (SI 2007/2157)
- 2.1.1 The Regulations apply to persons acting in the course of businesses carried on in the UK in various areas but pertinent to the Council are:-

Auditors, Insolvency Practitioners, External Accountants and Tax Advisors.

Independent Legal Professionals (this does not include solicitors employed by a public authority or working in-house except where working within the Regulated Sector e.g. buying and selling of real property or business entities, managing of client money, securities or other assets, opening or management of bank savings or securities accounts, organisation of contributions necessary for the creation, operation or management of companies, creation, operation or management of trusts, companies or similar structures).

- 2.2. Part 7 of the 2002 Act makes it an offence for a person –
- 2.2.1. to conceal, disguise, convert or transfer “criminal property” or remove it from the UK;
 - 2.2.2. to enter into, or become concerned in, arrangements which he or she knows or suspects will facilitate the acquisition, use, retention or control of criminal property;
 - 2.2.3. to acquire, use or possess criminal property;
 - 2.2.4. to fail in the case of the regulated sector to disclose knowledge or suspicion of money laundering to the nominated Officer (“the Money Laundering Officer”) – see paragraph 7 (internal reporting procedures) or the failure by him or her to disclose such knowledge or suspicion to the Serious Organised Crime Agency (SOCA);
 - 2.2.5. to tip off or make a disclosure which is likely to prejudice an investigation.
- 2.3. Property is treated as “criminal property” if it is obtained or known to have been obtained as a result of committing an act that would be a crime under UK law, no matter how small the crime.
- 2.4. A summary of offences and penalties can be found in Appendix C to this report.
- 2.5. The offences that council Officers must be particularly aware of are:-
- 2.5.1. the offence of entering into, or becoming concerned in, arrangements which the Officer knows or suspects will facilitate the acquisition, use, retention or control of criminal property; and
 - 2.5.2. the offence of tipping-off a person known or suspected to be money laundering or making a disclosure which is likely to prejudice an investigation.
- 2.6. The Council are responsible for disclosing actual or suspected money laundering activity to SOCA in respect of certain business activities within the regulated sector.
- 2.7. The business activities that apply to the Council are the provision by way of business of accountancy services, audit services and legal services.
- 2.8. Failure to comply with the 2007 Regulations is a criminal offence rendering the Council, as a corporate body, liable to prosecution. Where the offence is shown to have been committed with the consent or connivance of a senior Officer or has been committed

due to neglect on his/her part, that Officer is also liable to prosecution as well.

- 2.9. The 2007 Regulations require businesses in the regulated sector to introduce certain procedures to prevent money laundering.
- 2.10. The Money Laundering Regulations 2007 permit a risk based approach to compliance with obligations.
- 2.11. This approach does not apply to reporting suspicious activity because Police and Criminal Evidence Act and the Terrorism Act lay down specific legal requirements not to engage in certain activities and to make reports of suspicious activities once a suspicion is held.
- 2.12. The risk based approach applies to ongoing monitoring of clients and retainers which enables you to identify suspicions. The Council is required to put appropriate procedures in place in respect of:
 - establishing in certain cases the identity of external customers;
 - keeping records;
 - reporting suspicions of money laundering to SOCA;
 - educating and training staff.

3. COUNCIL'S RELEVANT BUSINESS FOR THE PURPOSES OF THE LEGISLATION

- 3.1. The provision by way of business advice about the tax affairs of another person by a body corporate.
- 3.2. The provision by way of business of accountancy services by a body corporate.
- 3.3. The provision by way of business of audit services.
- 3.4. The provision by way of business of legal services by a body corporatewhich involves participation in a financial or real property transaction (whether by assisting in the planning or execution of any such transaction or otherwise by acting for, or on behalf of, a client in any such transaction).
- 3.5. The provision by way of business of services in relation to the formation, operation or management of a company or a trust.
- 3.6. Whilst it is mainly accountancy, audit and legal services which will be formally subject to the requirements of the regulations, all members of staff are required to comply with this guidance in terms of reporting concerns regarding money laundering so that inadvertent offences can be avoided. The client identification

procedure is only required to be followed by those engaging in relevant business as set out above.

4.0 POSSIBLE SIGNS OF MONEY LAUNDERING ACTIVITIES

4.1 It is impossible to give a definitive list of money laundering activity but the following are types of risk factors which may, either alone or cumulatively with other factors, suggest the possibility of such activity.

- A new client.
- A secretive client e.g. refuses to provide requested information without a reasonable explanation.
- Concerns about the honesty, integrity, identity or location of a client.
- Illogical third party transactions – unnecessary routing or receipt of funds from third parties or through third party accounts.
- Involvement of an unconnected third party without logical reason or explanation.
- Payments of a substantial sum in cash (over £5,000).
- Overpayments by a client.
- Absence of an obvious legitimate source of the funds.
- Movement of funds overseas, particularly to a high risk country or tax haven.
- Where, without reasonable explanation, the size, nature and frequency of transactions or instructions (or the size, location or type of client) is out of line with normal expectations.
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational.
- The cancellation or reversal of an earlier transaction.
- Requests for release of client account details other than in the normal course of business.
- Extensive use of corporate structures and trust in circumstances where the client's needs are inconsistent with the use of such structures.
- Poor business records or internal accounting controls.

- A previous transaction for the same client which has been, or should have been, reported.
- Unusual property investment transactions if there is no apparent investment purpose or rationale.
- Instructions to receive and pay out money where there is no linked substantive property transaction involved.
- Property transactions, funds received for deposits or prior to completion from an unexpected source or where instructions are given for settlement funds to be paid to an unexpected destination.

5. CUSTOMER DUE DILIGENCE

5.1 Customer Due Diligence (CDD) is required by the Money Laundering Regulations 2007 because you can better identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you. You must conduct CDD on those clients who retain you for the regulated services (see paragraph 2.1.1).

5.2 The Money Laundering Regulations 2007 require you conduct CDD when:

- Establishing a business relationship
- Carrying out an occasional transaction
- You suspect money laundering or terrorist financing
- You doubt the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.

5.3 Council Officers in other departments who require accountancy, audit or legal services are internal customers and not subject to the anti-money laundering provisions.

5.4 External customers to whom the Council may provide accountancy, audit or legal services include –

- 5.4.1 any person or body for which the Council has power, in exercise of its power to trade, to carry out or provide any services or work or provide any facilities or supplies under statutory powers, including under the well-being power;
- 5.4.2 the bodies or organisations designated as “public bodies” for the purposes of the Local Authorities (Goods and Services) Act 1970.

- 5.5. Where CDD is required satisfactory evidence of the identity of an external customer must be obtained as a pre-requisite to providing the particular service.
- 5.6 Satisfactory evidence of identity is evidence which is reasonably capable of establishing (and does in fact establish to the satisfaction of the person obtaining it) that the external customer is the person he or she claims to be.
- 5.7 As the potential for money laundering is greater when the external customer is not physically present, staff should be extra vigilant when conducting checks to establish satisfactory evidence of identity.
- 5.8 Where the external customer is acting or appears to be acting on behalf of another person, for example as an agent or nominee of that person, reasonable measures must be taken to establish the identity of that other person.
- 5.9 In the absence of satisfactory evidence of identity, the Council's business relationship or one-off transaction with the external customer must not proceed any further.
- 5.10 Some examples of suitable forms of evidence to establish an external customer's identity are given in Appendix B.
- 5.11 Simplified CDD applies to UK public authorities so that it is sufficient to establish that the entity exists, but where there is a heightened risk of corruption or misappropriation of Government monies, greater monitoring should be considered.

6. RECORD-KEEPING PROCEDURES

- 6.1 Where CDD is required the Council must retain copies of a number of records
- 6.2 The retained records are –

Evidence of identity

- 6.2.1 a copy of the evidence of identity obtained from the external customer; or
- 6.2.2 information where a copy of the evidence of identity may be obtained; or
- 6.2.3 information enabling the evidence of identity to be re-obtained but only where it is not reasonably practicable for the Council to comply with paragraph 6.2.1 or 6.2.2;

Details of transactions

- 6.2.4 a record containing details relating to all transactions carried out by the Council where –
 - 6.2.4.1 money laundering is suspected, or
 - 6.2.4.2 accountancy services, audit services or legal services are provided by the Council by way of business to an external customer.

Retention of records

- 6.3 The records mentioned in paragraph 6.2 must be retained by the Council –
 - 6.3.1 in the case of records retained under paragraphs 6.2.1 – 6.2.3 (evidence of identity), for at least 5 years, commencing with the date on which the relationship ends where the Council has formed a business relationship with the external customer; or
 - 6.3.2 in the case of a one-off transaction or a series of such transactions, for at least 5 years commencing with the date of the completion of all activities taking place in the course of that transaction (or, as the case may be, the last of the transactions); or
 - 6.3.3 in the case of records retained under paragraph 6.2.4 (money laundering suspected or professional services provided by way of business), for at least 5 years commencing with the date on which all activities taking place in the course of the transaction in question were completed.

7. INTERNAL REPORTING PROCEDURES

- 7.1 The 2002 Act and the 2007 Regulations require the Council to nominate a person to receive reports of money laundering (called “the nominated Officer” in the legislation but “the Money Laundering Officer or MLO” in this document).
- 7.2 The MLO is the Head of Financial Management, Resources and Regulation Department, whose contact details can be found in the internal telephone directory.
- 7.3 The MLO’s deputy, who will act on his behalf in his absence, is the Internal Audit Manager.
- 7.4 Any member of staff who knows or suspects, or has reasonable grounds for knowing or suspecting, that a customer is engaged in money laundering must immediately report that fact in writing to the MLO.
- 7.5 The MLO must consider any internal report in the light of any relevant information available to the Council, and decide whether

the information shows or gives reasonable grounds for suspecting that a customer is engaged in money laundering.

- 7.6 Where the MLO decides that the information shows or gives reasonable grounds for suspecting that a customer is engaged in money laundering, he must submit an external report to SOCA.
- 7.7 The Regulations require any person who knows or suspects that an external customer is engaged in money laundering to report that fact to the MLO. Failure to report knowledge or suspicion of money laundering is itself an offence and may itself result in the prosecution of that person.
- 7.8 If you know or suspect that an external customer is involved in money laundering you must immediately contact the MLO. The MLO will then complete a Suspicious Activity Report (SAR) as soon as they are notified of a suspicion or knowledge of terrorist financing or money laundering. The SAR is to be submitted to SOCA. Where you know that a Law Enforcement Agency already has an interest in the matter, the MLO may complete an LIVR (Limited Intelligence Value Report).
- 7.9 Guidance and report forms can be found on the SOCA website.
- 7.10 If the MLO decides that a report should be submitted to SOCA the processing of the external customer's transaction must not proceed without the MLO and SOCA sanction.
- 7.11 To avoid an allegation of tipping-off the external customer, you must follow the instructions of the MLO and SOCA and not communicate further with the external customer without their permission and in accordance with their instructions.
- 7.12 Continuing to communicate with the external customer or processing the external customer's transaction without the SOCA's sanction may result in the prosecution of that person for tipping-off the external customer.
- 7.13 The MLO himself may commit an offence if he knows or suspects, or has reasonable grounds for knowing or suspecting, that an external customer is engaged in money laundering on the basis of information or other matters that have come to him or her as a result of an internal report and fails to report this to the SOCA as soon as it is practicable to do so.

8. EDUCATING AND TRAINING STAFF

- 8.1 The MLO will –
 - 8.1.1 arrange appropriate training for relevant current and new members of staff in line with their responsibilities, so that they are able to recognise and deal with transactions which may be related to money laundering; and

- 8.1.2 ensure that relevant employees are aware of this guidance and the Council's money laundering procedures.
- 8.2 Training will be ongoing to ensure that staff are kept up to date and in the form of guidance notes, face-to-face training, e-learning or otherwise.
- 8.3 Records will be kept of the staff undergoing training and the date and nature of the training.

9. LEGAL PROFESSIONAL PRIVILEGE

- 9.1 Solicitors and all other legal staff and legal services' support staff have a duty of confidentiality to keep information concerning the Council's affairs confidential.
- 9.2 Such information attracts legal professional privilege. There are two categories of legal professional privilege: legal advice privilege and litigation privilege.

Legal advice privilege

- 9.3 Legal advice privilege applies to the imparting of confidential information by Members of the Council or other council staff to solicitors and other legal services' staff for the purpose of obtaining legal advice in relation to the business of the Council, and to communications from legal services' staff imparting legal advice to Members of the Council or other council staff.
- 9.4 Only those communications that –
 - 9.4.1 directly seek or provide legal advice, or
 - 9.4.2 contain information passed by legal services' staff to Members of the Council or other council staff for the purpose of keeping each other informed so that advice (including advice as to a proposed or suggested course of action in the relevant legal context) may be sought or given as required, or
 - 9.4.3 attract legal advice privilege.
- 9.5 But legal advice privilege does not attach to documents prepared for the purpose or forming part of a criminal act, or to communications seeking legal advice for the purpose of furthering a criminal act, even if the legal adviser is not aware of the true purpose of preparing the documents or seeking the legal advice.
- 9.6 Consequently, documents and communications known to have been made for the purpose of furthering money laundering do not attract legal advice privilege.

- 9.7 However, if money laundering were simply suspected, legal advice privilege would not apply if the suspicions proved to be correct. But if the suspicions proved to be unfounded, documents and communications attracting legal advice privilege would remain privileged.
- 9.8 The 2002 Act anticipates this possibility and provides for an “authorised disclosure” of privileged documents and communications without breaching either a solicitor or other legal services’ staff duty of confidentiality or professional restrictions to treat certain documents and communications as legally privileged.
- 9.9 The 2002 Act also authorises the disclosure of privileged documents and communications where the solicitor is not involved in a transaction but knows or suspects that the transaction involves money laundering. A disclosure in those circumstances is a “protected disclosure” and the solicitor does not breach his duty of confidentiality and professional obligations by reporting the matter to the MLO.
- 9.10 Legal advice privilege continues to apply however in all other circumstances to documents or communications disclosed to the MLO on the basis of an authorised or protected disclosure.

Litigation privilege

- 9.11 Litigation privilege applies to the imparting of confidential information, in the context of legal proceedings, to council solicitors and other council legal services’ staff by –
- 9.11.1 Members of the Council and other council staff, and
- 9.11.2 the solicitors or other legal advisers of the other party or parties to the proceedings,
- (in contemplation of the proceedings, during the course of the proceedings or during the course of negotiations leading to a settlement of the proceedings).
- 9.12 Litigation privilege continues to apply in the circumstances outlined in paragraph 9.11 even though the solicitor or legal adviser knows or suspects that money laundering is taking place, except where –
- 9.12.1 the solicitor or legal adviser is taking part in money laundering activities;
- 9.12.2 the solicitor or legal adviser provides the legal advice for money laundering purposes; or

- 9.12.3 the solicitor or legal adviser knows that the customer is seeking legal advice for money laundering purposes.
- 9.13 A solicitor or legal adviser is in contempt of court if he discloses information to SOCA that is protected by litigation privilege and also in breach of the rules of professional misconduct.
- 9.14 Confidential information imparted to the legal adviser outside the context of litigation (for example the conveyance of a property as a consequence of litigation) does not attract litigation privilege and is therefore not exempt from disclosure to SOCA in appropriate circumstances.

10. DATA PROTECTION

- 10.1 Under the Data Protection Act 1998 an external customer may request in writing –
 - 10.1.1 a copy of all the personal data of which that person is the data subject and any information available to the Council on the source of that data; and
 - 10.1.2 information on the processing of any personal data of his by the Council, a description of that data, the purpose for which the data are being processed and to whom the personal data has or may be disclosed.
- 10.2 The Council must respond to a request for information promptly and in any event not more than 40 days from the date on which the request is received.
- 10.3 The 1998 Act contains certain exemptions from the right of access to personal data. One such exemption is where the right of access would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- 10.4 The exemption from the right of access to personal data will apply where the disclosure of personal data would result in the commission of the tipping-off offence under the 2002 Act.
- 10.5 The exemption is not automatic and each case should be considered on its merits to ensure that the exemption applies.
- 10.6 The Council's Data Protection Policy can be viewed on the Intranet in the A-Z Directory and guidance on the application of the policy and the Data Protection Act 1998 can be obtained from the Council's Data Protection Co-ordinator.

11. FREEDOM OF INFORMATION

- 11.1 The Freedom of Information Act 2000 gives members of the public a general right of access to all types of recorded information held

by public authorities, which includes the Council. The general right of access is however subject to exemptions.

- 11.2 The relevant exemptions are contained in section 23 (information supplied by, or relating to, bodies dealing with security matters) and section 31 (law enforcement).
- 11.3 Section 23 (1) and (3) (k) provides that information held by a public authority (the Council) which relates to the SOCA is exempt from disclosure.
- 11.4 Section 31(1) (a) is a similar exemption on disclosure to the exemption in the Data Protection Act 1998. It provides that information is exempt from disclosure if its disclosure under the 2000 Act would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

APPENDIX A

The Law Society Anti Money Laundering Practice Note. Legal Policy 3 September 2007.

USEFUL WEBSITES

The Joint Money Laundering Steering Group www.jmlsg.org.uk

The Serious Organised Crime Agency www.soca.gov.uk

The Law Society – www.lawsociety.org.uk

The Financial Services Authority – www.fsa.gov.uk/

APPENDIX B

EXTERNAL CUSTOMERS

1. ASSESSING THE RISK

Low risk

- 1.1. The risk of an external customer using council financial systems for money laundering purposes is relatively low where –
 - 1.1.1. the external customer is subject to a high degree of regulatory control;
 - 1.1.2. the external customer is subject to statutory or regulatory public disclosure requirements;
 - 1.1.3. the external customer is a government department or agency;
 - 1.1.4. the external customer is introduced by intermediaries who are themselves subject to UK, EU or equivalent anti-money laundering regulations, and who the member of staff concerned is reasonably confident comply with the regulations.

Higher risk

- 1.2. The risk of an external customer using council financial systems for money laundering purposes may be higher where –
 - 1.2.1. the business transaction with the external customer would involve complex ownership structures, as this may make it easier to conceal underlying beneficiaries, especially where there is no legitimate commercial rationale;
 - 1.2.2. the external customer is in a public position and/or location which carries a higher exposure to the possibility of corruption;
 - 1.2.3. the external customer is represented by or involved with an intermediary, who is not subject to UK, EU or comparable anti-money laundering regulations;
 - 1.2.4. the origin of the external customer's finances and sources of funds cannot easily be verified or where the audit trail has been deliberately broken and/or unnecessarily layered.

Higher risk or lower risk?

- 1.3. The risk of an external customer using council financial systems for money laundering purposes may be higher or lower where –

- 1.3.1. the external customer is a non-profit organisation and whether or not the customer is registered with a supervisory body, for example the Charity Commission;
- 1.3.2. the external customer is known to other parts of the Council – depending on the extent of this knowledge and linked accounts;
- 1.3.3. the nature of the external customer's structure (trust, etc.);
- 1.3.4. the breadth, complexity and/or geographical spread of ownership of the external customer's structure;
- 1.3.5. the external customer is unable to meet the verification requirement outlined in paragraph 3 or 4, as the case may be.

2. DUE DILIGENCE AND KNOWING THE CUSTOMER

- 2.1. In order to know the external customer, steps should be taken in each case –
 - 2.1.1. to establish who exactly the external customer for business is, and who needs to be identified;
 - 2.1.2. to establish the external customer's identity;
 - 2.1.3. to verify the external customer's identity.
- 2.2. In addition to the steps mentioned in paragraph 2.1, additional steps should be taken where appropriate –
 - 2.2.1. to establish the external customer's circumstances and business, including, where appropriate, the external customer's source of funds, and the purpose of specific transactions and the expected nature and level of those transactions;
 - 2.2.2. to update information held on the external customer to ensure the information held is valid;
 - 2.2.3. to review information held on the external customer to ensure it is current and valid;
 - 2.2.4. to monitor the external customer's business activity and business transactions to ensure that the Council is not being used as a vehicle for money laundering.

3. CUSTOMER IDENTIFICATION: INDIVIDUAL EXTERNAL CUSTOMERS

Individual external customers

- 3.1. In relation to individual external customers, standard identification should comprise –
- 3.1.1. the external customer's full name;
 - 3.1.2. the external customer's current address;
 - 3.1.3. the external customer's previous address if the customer has changed address in the last three months;
 - 3.1.4. the external customer's date of birth;
 - 3.1.5. the external customer's nationality;
 - 3.1.6. the external customer's country of residence;
 - 3.1.7. the external customer's employment and financial circumstances.
- 3.2. Specific aspects of the information provided by the external customer under paragraph 3.1 should be verified, either from a document or documents produced by the external customer, or electronically by the member of staff concerned, or by a combination of both.
- 3.3. Verification of an external customer's identity should be based on original documents not copies.

Documents providing evidence of identity

- 3.4. The following principal documents may be used to provide evidence of identity –
- 3.4.1. Government issued, with a photograph –
 - Unexpired photocard driving licence.
 - National Identity card.
 - 3.4.2. Government issued without a photograph –
 - Unexpired (old style) driving licence.
 - Recent evidence of entitlement to a state or local authority funded benefit, tax credit, pension, educational or other grant.
 - 3.4.3. Issued by a judicial authority –
 - Instrument of a court appointment (such as liquidator or grant of probate).

- 3.4.4. Issued by public sector bodies or authorities –
- Current council tax demand letter or utility bill or statement
- 3.4.5. Issued by other regulated bodies under the anti-money laundering regulations –
- Current bank statements or credit/debit card issued by a regulated financial sector firm in the UK, EU or comparable jurisdiction.
 - Satisfactory reference on, or confirmation of identity of, the external customer received from a regulated financial sector firm in the UK, EU or comparable jurisdiction in response to a direct enquiry.
- 3.4.6. Other –
- UK Citizencard.
- 3.5. Where the external customer is unable to supply satisfactory evidence of identity through no fault of their own, for instance external customers who are vulnerable adults, external customers dependent on the care of others or external customers who are minors, confirmation in writing from a person in a position of responsibility that the external customer is who they say they are may be accepted as evidence of identity (Persons in a position of responsibility include solicitors, doctors, ministers of religion, teachers, and social workers, local Councillors with knowledge of the client).
- 3.6. External customers who are not normally resident in the UK but are seeking council services should generally be able to produce national identity cards, passports or residence permits issued by the Home Office or national driving licences.

4. PARTNERSHIPS AND UK LLPs ETC

- 4.1 A partnership is not a separate legal entity, so you must obtain information on the constituent individuals.
- 4.2 Where a partnership is made up of regulated professionals, it will be sufficient to confirm the firm's existence and the trading address from a reputable professional directory or search facility with the relevant professional body. Otherwise you should obtain evidence on the identity of at least the partner instructing you and one other partner, and evidence of the firm's trading address.
- 4.3 For a UK LLP, obtain information in accordance with the requirements for companies as outlined below.

5. CUSTOMER IDENTIFICATION: COMPANIES AND OTHER ENTITIES

General

- 5.1 The following standard identification should be obtained in relation to the business concerned –
- 5.2 the full name of the business;
- 5.3 the type of legal entity, for example, private company, public company, trust;
- 5.4 the location of the business, the operating address and/or registered address;
- 5.5 the country of incorporation;
- 5.6 the registered number (or equivalent), for example the company's registration number or charity registered number;
- 5.7 the regulatory body for the business (if any);
- 5.8 where appropriate, the names of all directors (or equivalent); and
- 5.9 where appropriate the names of the principal beneficial owners (i.e. those with a 25% or over beneficial interest in the business.
- 5.10 The registered details of the business should be verified by –
 - 5.10.1 a search of the relevant company or regulatory register (or equivalent);
 - 5.10.2 confirmation of the listing of the business on a regulated market; or
 - 5.10.3 a copy of the formation document for the business, its certificate of incorporation or equivalent.

Publicly quoted companies

- 5.11 Where the external customer for business is –
 - 5.11.1 a publicly quoted company, subject to public disclosure rules,
 - 5.11.2 a majority-owned and consolidated subsidiary of such a publicly quoted company, or
 - 5.11.3 subject to the licensing and prudential regulatory regime of a statutory regulator,

(no further steps need be taken to verify identity over and above the standard identification requirement, and the usual commercial checks and due diligence).

Private companies

- 5.12 Where private companies are well known, reputable organisations, with long histories in their industries, and with substantial public information about them, the standard identification requirement will be sufficient to meet anti-money laundering obligations.
- 5.13 The names of all directors (or equivalent) should be obtained and, following the assessment of the money laundering risk presented by the company, the decision taken as to whether it is appropriate to verify the identity of one or more directors.
- 5.14 Certificate of incorporation, filed audited accounts, details from the relevant company register.
- 5.15 Where the principal owner of a private company is another corporate entity or trust, the identity of the beneficial owners should be established, unless that corporate entity is publicly quoted. The identity of the beneficial owners who exercise effective control should then be verified.

Trusts

- 5.16 Trusts come in a variety of forms ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability to small local trusts funded by individual donations from a local community serving the local need.
- 5.17 The following information should be obtained for each trust –
- Full name.
 - Nature of trust (discretionary, bare, etc.).
 - Donor of the funds.
 - Nature of business or activity.
 - Location of business or activity (operating address).
 - Country of establishment.
 - Names of all trustees.
 - Name of any protector or controller.
 - Names or classes of beneficiaries.
- 5.18 The identity of the trust should be verified either by searching the appropriate register maintained in the country of establishment, or by obtaining a copy of the instrument establishing the trust. Following an assessment of the money laundering risk presented by the trust, verification of the identity of one or more trustees may be appropriate.

- 5.19 Where a trust is itself subject to the anti-money laundering regulations, or a publicly quoted company, the standard identification requirement should be sufficient to meet anti-money laundering obligations.
- 5.20 Following an assessment of the money laundering risk presented by the trust, evidence of the identity of additional trustees may be appropriate.

Charities

- 5.21 Charities can take a number of legal forms. Some may be companies limited by guarantee, and should be treated as private companies. Other charities may take the form of trusts.
- 5.22 Details of all registered charities in England and Wales are kept by the Charity Commission in a Central Register of Charities. The registered name of a charity, its registration number and the address of the Charity Commission's correspondent for the charity concerned can be accessed on the Commission's website or a check can be made to the Commission's enquiry line.
- 5.23 Churches are in general exempted by law from registering as charities and may not therefore have a registered number. Their identity can be verified by reference to the appropriate headquarters or regional organisation of the denomination.

Partnerships and unincorporated businesses

- 5.24 The identification procedure for partnerships and unincorporated businesses is the one for companies and other entities.
- 5.25 Where partnerships or unincorporated businesses are well known, reputable organisations, with long histories in their industries, and with substantial public information about them, the standard identification requirement should be sufficient to meet anti-money laundering obligations.
- 5.26 The money laundering risk of smaller, less transparent partnerships or unincorporated businesses should be considered and where appropriate the identity of the principal beneficial owners, shareholders and/or controllers should be established and any articles of association or constitution.

Clubs and societies

- 5.27 The standard identification requirement may be used for clubs and societies that serve a limited social or regional purpose. Following an assessment of the money laundering risk presented by the club or society, it may be appropriate to verify the identity of additional trustees (or equivalent).

APPENDIX C

Below is a summary of offences and the relevant penalties if you do not comply with anti-money laundering and counter-terrorist finance obligations. In addition to being a principal offender, you could also be charged with offences of conspiracy, attempt, counselling, aiding, abetting or procuring a principal offence, depending on the circumstances.

Police and Criminal Evidence Act:

Section	Description	Penalty
327	Conceals, disguises, converts, transfers or removes criminal property	On summary conviction – up to six months imprisonment or a fine or both
328	Arrangements regarding criminal property	As above
329	Acquires, uses or has possession of criminal property	On indictment – up to 14 years imprisonment or a fine or both
330	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – regulated sector	On summary conviction – up to six months imprisonment or a fine or both
331	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – nominated Officer in the regulated sector	On indictment – up to five years imprisonment or a fine or both
333	Tipping off	On summary conviction – up to six months imprisonment or a fine or both
342	Prejudices an investigation	On indictment – up to five years imprisonment or a fine or both

Terrorism Act:

Section	Description	Penalty
15	Fundraising	On summary conviction –

		up to six months imprisonment or a fine or both
16	Use and possession	As above
17	Funding arrangements	As above
18	Money laundering	On indictment – up to 14 years imprisonment or a fine or both
19	Failure to disclose	As above
21A	Failure to disclose – regulated sector	As above

Regulations:

Regulation 45 lists a number of sections, the breach of which is an offence.

Section	Description	Penalty
7 (1)	Applying Customer Due Diligence (CDD) to new customers	On summary conviction – a fine
7 (2)	Applying CDD to existing customers	As above
7 (3)	Determining extent of CDD on a risk-sensitive basis and being able to demonstrate this to the Solicitors Regulation Authority (SRA)	On indictment – up to 2 years imprisonment or a fine or both
8 (1)	Conducting ongoing monitoring	As above
8 (3)	Determining extent of ongoing monitoring on a risk-sensitive basis and being able to demonstrate this to the SRA	As above
9 (2)	Verification prior to the establishment of a business relationship or carrying out of an occasional transaction	As above
10 (1)	Relates to casinos	As above
11 (1)(a)	Not use a bank account without CDD	As above

11 (1)(b)	Not establish a business relationship or carry out an occasional transaction if no CDD	As above
11 (1)(c)	Terminate existing relationship or occasional transaction if no CDD	As above
14 (1)	Conduct enhanced due diligence	As above
15 (1)	Relates to financial and credit institutions	As above
19 (1)	Keep your own records	As above
19 (4)	Keep records others have relied on	As above
19 (5)	Be prepared to provide records others have relied on	As above
19 (6)	Ensure those you rely on are willing to provide records	As above
20 (10)	Establish policies and procedures	As above
20 (4)	Relates to financial and credit institutions	As above
21	Train relevant employees	As above
26	Does not relate to solicitors	As above
Directions under 18	Not to act where Treasury makes a direction	As above

APPENDIX D

FORMS

Form 1 – Individual external customer		
IDENTITY		
Full name of external customer's business		
Current address		
Previous address if external customer has changed address in last 3 months		
Date of birth		
Nationality		
Country of residence		
VERIFICATION OF IDENTITY		
Record reference numbers of documents where appropriate		
The external customer provided the following as evidence of identity		✓ if copy attached
The following		✓ if copy

additional evidence of identity was supplied or obtained		attached
RISK ASSESSMENT NOTE This is low/medium/high risk client with no/with beneficial owners providing low/medium/high risk instructions, standard or enhanced CDD material obtained [and low/medium/high level ongoing monitoring is to occur.]		
RECORDS In relation to an external customer, the following records must be kept for at least 5 years, commencing with the date on which the business relationship ends or, in the case of a one-off transaction or a series of such transactions, commencing with the date of the completion of all activities taking place in the course of the transaction (or, as the case may be, the last of the transactions) – • a copy of the evidence of identity, or • information where a copy of the evidence of identity may be obtained, or • information enabling the evidence of identity to be re-obtained if it is not reasonably practicable to keep a copy or specify where a copy of the evidence of identity may be obtained. Where money laundering is suspected, or the Council provides accountancy services, audit services or legal services by way of business to an external		

customer, for at least 5 years commencing with the date on which all activities taking place in the course of the transaction in question were completed, a record must be kept containing details of all of the transactions with the external customer.

Signed:	
Name:	
Position:	
Date:	

Form 2 – Companies and other entities		
IDENTITY		
Full name of external customer		
Type of legal entity (corporate, trust, etc.)		
Location of business (full operating address)		
Country of incorporation		
Registered number, if any (or appropriate)		
Regulatory body		
Names of directors (or equivalent)		
Names of principal beneficial owners (over 25%)		
VERIFICATION OF IDENTITY		
The external customer provided the following as evidence of identity		✓ if copy attached
The following additional evidence of		✓ if copy

identity was supplied or obtained		attached
RISK ASSESSMENT NOTE This is low/medium/high risk client with no/with beneficial owners providing low/medium/high risk instructions, standard or enhanced CDD material obtained [and low/medium/high level ongoing monitoring is to occur.]		
RECORDS In relation to an external customer, the following records must be kept for at least 5 years, commencing with the date on which the business relationship ends or, in the case of a one-off transaction or a series of such transactions, commencing with the date of the completion of all activities taking place in the course of the transaction (or, as the case may be, the last of the transactions) – 27 • a copy of the evidence of identity, or • information where a copy of the evidence of identity may be obtained, or • information enabling the evidence of identity to be re-obtained if it is not reasonably practicable to keep a copy or specify where a copy of the evidence of identity may be obtained. Where money laundering is suspected, or the Council provides accountancy services, audit services or legal services by way of business to an external customer, for at least 5 years commencing with the date on which all activities taking place in the course of the transaction in question were completed, a record must be kept containing details of all of the transactions with the external customer.		

Signed:	
Name:	
Position:	
Date:	

BURY COUNCIL

ANTI-BRIBERY POLICY

MARCH 2015

ANTI-BRIBERY POLICY

1. Policy Statement - Anti Bribery

Bribery is a criminal offence. Bury Council is wholly committed to preventing bribery and corruption in all our dealings and relationships, and upholding all relevant laws, including the Bribery Act 2010. We do not, and will not, pay bribes or offer improper inducements to anyone for any purpose, nor do we or will we, accept bribes or improper inducements.

To use a third party as a conduit to channel bribes to others is a criminal offence. We do not, and will not, engage indirectly in or otherwise encourage bribery.

We are committed to the prevention, deterrence and detection of bribery. We have zero-tolerance towards bribery. We aim to maintain anti-bribery compliance "business as usual", rather than as a one-off exercise.

2. Objective of this policy

This policy provides a coherent and consistent framework to enable the Council's employees to understand and implement arrangements enabling compliance. In conjunction with related policies and key documents it will also enable employees to identify and effectively report a potential breach.

We require that all personnel, including those permanently employed, temporary agency staff and contractors:

- Act honestly and with integrity at all times and to safeguard the Council's resources for which they are responsible.
- Comply with the spirit, as well as the letter, of the laws and regulations of all jurisdictions in which the Council operates, in respect of the lawful and responsible conduct of activities.

3. Scope of this policy

This policy applies to all of the Council's activities. For partners, joint ventures and suppliers, we will seek to promote the adoption of policies consistent with the principles set out in this policy.

Within the Council, the responsibility to control the risk of bribery occurring resides at all levels of the Council, in all business units and corporate functions.

Part 8 – Anti-Bribery Policy

This policy covers all personnel, including all levels and grades, those permanently employed, temporary agency staff, contractors, non-executives, agents, Members (including independent Members and Co-optees), volunteers and consultants.

4. Bury Council's commitment to action

Bury Council commits to:

- Set out a clear anti-bribery policy and keeping it up to date.
- Making all employees aware of their responsibilities to adhere strictly to this policy at all times.
- Training all employees so that they can recognise and avoid the use of bribery by themselves and others.
- Encouraging its employees to be vigilant and to report any suspicions of bribery, providing them with suitable channels of communication and ensuring sensitive information is treated appropriately.
- Rigorously investigating instances of alleged bribery and assisting police and other appropriate authorities in any resultant prosecution.
- Taking firm and vigorous action against any individual(s) involved in bribery.
- Provide information to all employees to report breaches and suspected breaches of this policy.
- Include appropriate clauses in contracts to prevent bribery.

5. Bribery

Is an inducement or reward offered, promised or provided to gain personal, commercial, regulatory or contractual advantage and can take various forms such as

- bribery of another individual or organisation;
- accepting a bribe from an individual or organisation.

Bribes may not always be monetary and may include gifts or hospitality.

The Bribery Act

There are four key offences under the Act:

- bribery of another person (section 1)

- accepting a bribe (section 2)
- bribing a foreign official (section 6)
- failing to prevent bribery (section 7)

The Bribery Act 2010

(http://www.opsi.gov.uk/acts/acts2010/ukpga_20100023_en_1) makes it an offence to offer, promise or give a bribe (Section 1). It also makes it an offence to request, agree to receive, or accept a bribe (Section 2). Section 6 of the Act creates a separate offence of bribing a foreign public official with the intention of obtaining or retaining business or an advantage in the conduct of business.

There is also a corporate offence under Section 7 of the Act of failure by the Council to prevent bribery that is intended to obtain or retain business, or an advantage in the conduct of business, for the Council. The Council will have a defence to this corporate offence if it can show that it had in place adequate procedures designed to prevent bribery by or of persons associated with the Council.

6. What are "adequate procedures"?

Whether the procedures are adequate will ultimately be a matter for the courts to decide on a case-by-case basis. Adequate procedures need to be applied proportionately, based on the level of risk of bribery in the organisation. It is for individual organisations to determine proportionate procedures in the recommended areas of six principles. These principles are not prescriptive. They are intended to be flexible and outcome focussed, allowing for the different circumstances of organisations. Small organisations will, for example, face different challenges to those faced by large multi-national enterprises. The detail of how organisations apply these principles will vary, but the outcome should always be robust and effective anti-bribery procedures.

Proportionate procedures

An organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the organisation's activities. They are also clear, practical, accessible, effectively implemented and enforced.

Top level commitment

The top-level management are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable.

Risk Assessment

Part 8 – Anti-Bribery Policy

The organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented. It includes financial risks but also other risks such as reputational damage.

Due diligence

The organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks.

Communication (including training)

The organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training that is proportionate to the risks it faces.

Monitoring and review

The organisation monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

Bury Council is committed to the proportional implementation of these principles.

7. Penalties

An individual guilty of an offence under sections 1, 2 or 6 is liable:

- On conviction in a magistrates court, to imprisonment for a maximum term of 12 months, or to a fine not exceeding £5,000, or to both.
- On conviction in a crown court, to imprisonment for a maximum term of ten years, or to an unlimited fine, or both.

Organisations are liable for these fines and if guilty of an offence under section 7 of the Act are liable to an unlimited fine.

8. Bribery is not tolerated

It is unacceptable to:

- Give, promise to give, or offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.

- Give, promise to give, or offer a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure.
- Accept payment from a third party that you know or suspect is offered with the expectation that it will obtain a business advantage for them.
- Accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by us in return.
- Retaliate against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy.
- Engage in activity in breach of this policy.

9. Facilitation payments

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

10. Gifts and hospitality

This policy is not meant to change the requirements of our gifts and hospitality policy. This makes it clear that:

- Employees should tactfully refuse any gift offered to them by any persons who have, or may seek to have dealings with the Council. The same principal applies in reverse.
- Nominal gifts and hospitality of token value are acceptable.
- Where it is not possible to return a gift, it should be passed to the Mayor's Secretary to support the Mayor's charity.
- If a gift is accepted it must be recorded on the online form on the intranet.

11. Public contracts and failure to prevent bribery

Under the Public Contracts Regulations 2006 (which gives effect to EU law in the UK), a company is automatically and perpetually debarred from competing for public contracts where it is convicted of a corruption offence. There are no plans to amend the 2006 Regulations for this to include the crime of failure to prevent bribery. Organisations that are convicted of failing to prevent bribery are not automatically barred from participating in tenders for public contracts. The Council has the discretion to exclude organisations convicted of this offence.

Whilst the 2006 Regulations are still current, the 2014 EU Procurement Directives will bring with them various improved safeguards from corruption:

- Specific safeguards against conflicts of interest, similar to common existing UK practice where declarations are signed by procurement staff to confirm they have no outside interests with bidders etc.
- Similar provision against illicit behaviour by candidates and tenderers, such as attempts to improperly influence the decision-making process or collusion.
- Safeguards against undue preference in favour of participants who have advised the contracting authority or been involved in the preparation of the procedure.
- Self-cleaning measures, for suppliers who have cleaned up their bad practices.

12. Staff responsibilities

The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for the Council or under its control. All staff are required to avoid activity that breaches this policy.

You must:

- Ensure that you read, understand and comply with this policy.
- Raise concerns as soon as possible if you believe or suspect that a conflict with this policy has occurred, or may occur in the future.
- Avoid any activity that breaches this Policy or could be seen as a breach of this Policy;
- Seek advice **before** accepting gifts or hospitality;

Employees **must not**:

- Give or promise to give, or offer a payment, gift or hospitality with the expectation or hope that a personal, commercial, regulatory or contractual advantage will be received, or to reward any such advantage already given;
- Give or promise to give, or offer a payment, gift or hospitality to a government official, agent or representative to facilitate or speed up a procedure;

- Accept payment from a third party that you know or suspect is offered with the expectation that it will obtain a business advantage for them;
- Accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by the Council in return;
- Retaliate against, threaten or victimise anyone who has refused to be involved in bribery or corrupt practices, or who has raised concerns under this policy.

The list above is not exhaustive but is intended to provide examples of conduct likely to breach this policy.

If employees have any doubt at all about circumstances that they find themselves in, advice should be sought from their line manager **before** it becomes an issue to be dealt with.

As well as the possibility of civil and criminal prosecution, staff breaching this policy will face disciplinary action, which could result in dismissal for gross misconduct.

13. Raising a Concern

Bury Council is committed to ensuring that all of us have a safe, reliable, and confidential way of reporting any suspicious activity. We want each and every member of staff to know how they can raise concerns.

We all have a responsibility to help detect, prevent and report instances of bribery. If you have a concern regarding a suspected instance of bribery or corruption, please speak up – your information and assistance will help. The sooner you act, the sooner it can be resolved.

There are multiple channels to help you raise concerns. Please refer to the Whistleblowing Policy in part 2 and determine your favoured course of action. Preferably the disclosure will be made and resolved internally (e.g. to your head of department/another Senior Officer/Trade Union). Secondly, where internal disclosure proves inappropriate, concerns can be raised with the regulator (e.g. external auditor). Raising concerns in these ways may be more likely to be considered reasonable than making disclosures publicly (e.g. to the media).

Concerns can be anonymous. In the event that an incident of bribery, corruption, or wrongdoing is reported, we will act as soon as possible to evaluate the situation. We have clearly defined procedures for investigating fraud, misconduct and non-compliance issues and these will be followed in any investigation of this kind. This is easier and quicker if concerns raised are not anonymous.

Staff who refuse to accept or offer a bribe, or those who raise concerns or report wrongdoing can understandably be worried about the repercussions. We aim to encourage openness and will support anyone who raises a genuine concern in good faith under this policy, even if they turn out to be mistaken.

We are committed to ensuring nobody suffers detrimental treatment through refusing to take part in bribery or corruption, or because of reporting a concern in good faith.

If you have any questions about these procedures, please contact:

Jayne Hammond – Assistant Director of Legal and Democratic Services – 0161-253-5237

Andrew Baldwin – Head of Financial Management – 0161-253-5034