1. Introduction

1.1. The Internal Audit & Anti-Fraud Group maintain a suite of anti-fraud policies to support the Council’s zero tolerance approach to fraud, thus maintaining proper arrangements for the Council’s finances.

1.2. To further strengthen their importance as part of robust governance, these policies were approved by Cabinet in January 2012, to be reviewed annually.

1.3. The Policies have been reviewed and this report sets out the latest versions, a summary of the purpose of the reports and a brief summary of changes made.

1.4. The policies apply to the Council, and as part of our strategy on raising fraud awareness will be promoted to and where applicable, applied by the Council’s partners such as Elevate, contractors and schools.

2. Purpose of the Policies

2.1 A brief description of each policy is set out in the table below. The latest version of each policy is set out in the Appendices to this report.

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Policy</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anti-Fraud &amp; Corruption</td>
<td>Sets out the Council’s commitment to</td>
</tr>
<tr>
<td>Strategy &amp; Policy including Fraud Response Plan</td>
<td>reducing opportunities for fraud and corruption across all council services and taking the strongest possible action against those who seek to defraud the Council. Includes guidance on what to do if an employee suspects fraud.</td>
<td></td>
</tr>
<tr>
<td>2 Prosecution Policy</td>
<td>Sets out the Council’s approach to seeking redress/sanction against those who seek to defraud the Council, linking to the Disciplinary rules where the perpetrator is a member of staff</td>
<td></td>
</tr>
<tr>
<td>3 Money Laundering Policy</td>
<td>Sets out the Council’s commitment to ensuring compliance with the requirements of the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 &amp; 2012 and Chartered Institute of Public Finance and Accountancy (CIPFA) guidance for Local Authorities on Money Laundering.</td>
<td></td>
</tr>
<tr>
<td>4 Whistleblowing Policy</td>
<td>In accordance with the Public Disclosure Act 1998 (as amended by the Enterprise and Regulatory Reform Act 2013), sets out how workers can raise serious or sensitive concerns about other members of staff, suppliers, or people who provide services with protection from harassment, victimisation or bullying as a result of them raising concerns.</td>
<td></td>
</tr>
<tr>
<td>5 Regulation of Investigatory Powers Policy</td>
<td>Sets out rules and procedures for undertaking and gaining authorisation for covert surveillance in accordance with the RIPA Act 2000 (as amended by the Protection of Freedoms Act 2012) and compliant with Human Rights &amp; Data Protection Legislation</td>
<td></td>
</tr>
<tr>
<td>6 Bribery Act Policy</td>
<td>Sets out the Council’s commitment to the prevention, deterrence and detection of bribery and to raise awareness with relevant officers linking with the already in place Employee Code of Conduct and rules on accepting gifts and hospitality</td>
<td></td>
</tr>
</tbody>
</table>

3. **Changes to the Policies**

3.1 The following changes have been made to the policies:
- The Whistleblowing policy has been reviewed and amended in light of the provisions of the Enterprise and Regulatory Reform Act 2013 – the notable change being that allegations must be ‘in the public interest’ rather than simply ‘in good faith’;
- The RIPA policy has been updated in response to a recommendation from the Office of Surveillance Commissioners and has been based upon the Thurrock RIPA policy which was noted by the Inspector as being a good example;
- The change in designation of the Divisional Director of Finance to the Chief Finance Officer. Otherwise the policies have been reviewed and deemed fit for purpose.

4. **Awareness Raising**

4.1 Anti-Fraud Policies are available on the Intranet and awareness raised with staff through channels such as the e-bulletin and posters on staff notice boards. More detailed
training/briefings and awareness sessions are targeted at specific groups of staff who need more detailed understanding of the implication of specific policies e.g. RIPA Authorising Officers. The review of the policies will be used as an opportunity to refresh awareness raising with staff.

5. **Financial Implications**
   Implications completed by: (Jonathan Bunt, Chief Finance Officer)

5.1 The Audit & Anti Fraud Teams are fully funded and there are no additional financial implications arising directly from this report. A robust anti-fraud culture, underpinned by appropriate policies prevents financial loss to the Authority.

6. **Legal Implications**
   Implications completed by: (Eldred Taylor-Camara, Legal Group Manager)

6.1 This report provides information to Members for noting and does not require decision. There are no further legal comments to add.

7. **The following people were consulted in the preparation of this report:**
   - Section 151 officer
   - Legal Group Manager
   - Subsidy Grant & Performance Manager – Elevate (HB Fraud)

8. **The following documents were used in the preparation of this report:**
   - PAASC Report 30 January 2013
Internal Audit

Fraud & Corruption
Policy & Strategy
(Incorporating Housing Benefit Fraud)
March 2014

<table>
<thead>
<tr>
<th>Date Last Reviewed:</th>
<th>March 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>PAASC</td>
</tr>
<tr>
<td>Date Approved:</td>
<td>19 March 2014</td>
</tr>
<tr>
<td>Version Number:</td>
<td>1.1</td>
</tr>
<tr>
<td>Review Date:</td>
<td>March 2015</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Group Manager – Internal Audit &amp; Anti-Fraud</td>
</tr>
<tr>
<td>Post Holder:</td>
<td>David Greenfield</td>
</tr>
</tbody>
</table>
The Council’s commitment to the Fraud Corruption Policy

London Borough of Barking & Dagenham, “the Council” carries out its responsibilities and delivers high quality services to the local community. The immense variety of service provision places the Council at risk of loss from fraud and corruption perpetrated both internally and externally. The Council operates a zero tolerance policy to Fraud and Corruption and considers the Fraud and Corruption Policy and Strategy to be an integral part of our approach.

What are the aims and requirements of the Policy?

Where Fraud or Corruption is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Fraud and Corruption Policy and Strategy. It will be investigated fully and the Council will prosecute all offenders where appropriate including, Members, employees, contractors, agency staff, consultants, suppliers and partners.

Who is governed by this Policy?

The Fraud and Corruption Policy and Strategy applies to all staff including and not limited to temporary staff, sessional staff, consultants and contractors. It also covers suppliers and those providing services under a contract with the Council in their own premises, for example, care homes and sheltered accommodation as well as anyone who seeks to commit fraud against the Council.

Executive Summary

The Fraud and Corruption Policy and Strategy makes clear the Council’s commitment to reducing opportunities for fraud and corruption and taking the strongest possible action against those who seek to defraud the Council. There will be no distinction made in investigation and action between cases that generate financial benefits and those that do not.
<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud &amp; Corruption Policy &amp; Strategy</td>
<td>4</td>
</tr>
<tr>
<td>Fraud &amp; Corruption Policy</td>
<td>4</td>
</tr>
<tr>
<td>The anti fraud culture and deterrence</td>
<td>4</td>
</tr>
<tr>
<td>Prevention – Managing the risk of fraud</td>
<td>5</td>
</tr>
<tr>
<td>Detection &amp; Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Fraud &amp; Corruption Strategy</td>
<td>9</td>
</tr>
<tr>
<td>Definitions</td>
<td>12</td>
</tr>
<tr>
<td>Further support, tools and guidance.</td>
<td>13</td>
</tr>
<tr>
<td>Appendix 1 Housing Benefit Policy &amp; Strategy</td>
<td>14</td>
</tr>
<tr>
<td>Appendix 2 Fraud response plan</td>
<td>18</td>
</tr>
</tbody>
</table>
Fraud & Corruption Policy & Strategy

Fraud & Corruption Policy

The council is responsible for the proper administration of its finances. This not only includes direct income and expenditure but also monies that is administered on behalf of the Government, our clients and for which the Council is the responsible accountable body. Anyone can potentially commit fraud, both inside and outside the organisation, and this can be targeted on all of these sources of income and expenditure and our valuable assets.

The Council aims to set high standards of service provision and is committed to upholding the reputation of the Authority and maintaining public confidence in its integrity and expects that Members (Elected councillors) and staff at all levels will adopt the highest standards of propriety and accountability and will lead by example.

The Authority also expects that individuals and organisations that come into contact with the Authority e.g. the public, suppliers and contractors, will act with integrity and without intent or actions involving fraud and corruption.

To achieve its aims and objectives the Council will therefore take a firm stance against any individual, group or organisation committing acts constituting theft, fraud, corruption, financial irregularity or malpractice or other form of wrongdoing, whether it is attempted against, from or within the Council.

In fulfilling its responsibilities to protect the public funds it administers against fraud and corruption the Authority recognises the responsibilities placed upon it by statute and will actively promote this Fraud and Corruption Policy and Strategy which is designed to:

- Promote standards of honest and fair conduct
- Encourage prevention of fraud and corruption
- Maintain strong systems of internal control
- Promote detection
- Pursue a zero-tolerance policy and bring to justice all persons who commit acts of fraud or corruption against the Council
- Recover any losses incurred by the Council

In addition to the following, specific matters in respect of Housing Benefits Fraud are set out in Appendix 1.

The Anti Fraud Culture and Deterrence

The culture of the organisation is one of honesty, openness and opposition to fraud and corruption. Members play a key role in maintaining and promoting this culture. Specifically the Standards Committee is responsible for promoting high standards of conduct by Members, employees, its contractors and partners.

Members have a duty to ensure that Council assets are adequately safeguarded from fraud and abuse and to ensure that the Council’s powers, duties and responsibilities are exercised in an open fair and proper manner to the highest standards of probity.
The Members and employees are an important element in the Council’s stance on fraud and corruption and they are positively encouraged to raise any concerns that they may have on these issues where they are associated with a Council activity.

Members of the public are also able to report concerns to appropriate Council officers or relevant external agencies such as the Police, External Audit, and the Local Government Ombudsman.

The Public Interest Disclosure Act 1998 provides protection for those who voice genuine and legitimate concerns through the proper channels. In this connection the Council has adopted a Whistleblowing Policy to ensure a defined route to bring alleged instances of fraudulent, unlawful or otherwise improper conduct to the Council’s attention. As well as the Whistleblowing Officer, this can involve the Monitoring Officer, Fraud Teams, or the employee’s line manager or Divisional Director or, if more appropriate, an officer external to the individual’s department.

The underlying message is that this Council will not tolerate fraudulent and corrupt activity. A pound lost through fraud and corruption is a pound that is stolen from Barking and Dagenham residents and reduces the amount available to spend on delivering services to residents.

A proactive programme of work will be agreed each year, using a risk-based approach to prioritise areas inherently at risk from fraud, outcomes from which will be publicised as appropriate.

Employees have access to fraud and corruption awareness training. Fraud awareness programmes will be targeted at specific groups of staff in the form of presentations, workshops and newsletters.

Additionally, this strategy and policy will also be available to all employees, contractors and partners and link to associated policies and guidance, for example:

- Employee Code of Conduct
- Disciplinary Rules
- Whistleblowing Policy
- Bribery Policy
- Money Laundering Policy
- Fraud Prosecution Policy

**Prevention – Managing the Risk of Fraud**

Fraud, theft and corruption are costly in terms of financial loss and reputational risk. The risk of loss can be reduced through robust preventive measures. The Council has a number of key processes and procedures which can assist in the prevention of fraud and corruption that include:

- Internal Control systems
- Standing Orders & Financial Regulations
- Employee Code of Conduct
- Disciplinary Rules
- Members Code of Conduct

The Chief Finance Officer has been delegated, through the Council’s Standing Orders and Financial Regulations powers to control and regulate the Council’s finances. These include the promotion of systems and practices to minimise the risk of fraud and corruption. An important part of the control framework is the maintenance of an effective internal and external audit of the Council’s finances that operate to the “best practice “standards defined in the Accounts and Audit Regulations (2011).
Managers

The effective eradication of fraud starts with managers. It is the responsibility of all Council managers to ensure that they manage the risk of fraud within their respective work areas. Managers are expected to be fully conversant with fraud risks (internal and external) relevant to their service areas. Some services will be predominantly at risk of attack from external sources, for example, Council tax, Housing and Renovation grants.

When considering the risk of fraud, managers must take the following steps:

**Identify the risk areas**

Managers must establish which parts of the service are most vulnerable to fraud e.g. letting or managing contracts, handling cash, allocating or distributing grants, ordering equipment, paying invoices, validating documentary evidence in support of claims for benefits etc. Other risks include assessing declared staff interests and considering whether such interests conflict with the Council’s interests or would undermine public confidence in the Council.

**Allocate responsibility for the risk**

Managers must identify who has responsibility for managing each risk and ensure that the officer concerned has adequate training, support and expertise to manage the risk effectively.

**Identify the need for revised controls**

Managers must evaluate the adequacy of existing controls and establish what further controls or changes to existing controls are required to reduce or eliminate the risk of fraud. For this, managers should refer to audit reports, internal investigation findings, value for money review findings, External Audit reports or findings from other external inspections. This will help ensure that there is full compliance with the Regulatory Framework, Standing Orders, local procedures and any relevant legislation.

**Implement the revised controls effectively**

Managers must ensure that the revised controls are cost effective and that written procedures are updated informing staff and customers of any changes that affect them. Staff will need to be trained in the use of revised controls and procedures. Managers must also identify any continued weaknesses and adjust as necessary.

**Evaluate the effectiveness of controls**

After a reasonable period of time managers should assess the effectiveness of the controls and evaluate whether the risk of fraud has been eliminated or reduced.

For advice on managing risk, evaluating possible conflicts of interest, or the development or evaluation of controls contact the Internal Audit or Risk Management Sections.

Any system weaknesses identified as a result of Fraud Investigations will be reported to the relevant service manager as well as the Group Manager (Internal Audit & Anti Fraud) and addressed through an agreed action plan. The relevant Service Manager will be responsible for implementing the action plan. Internal Audit will have a monitoring role, addressing failures to implement recommendations to the relevant Divisional Director in addition to reporting major system failures, remedial action plans and instances of non-compliance to the Public Accounts & Audit Select Committee.
Contractors

It is expected that the Council’s contractors and partners will have adequate controls in place to minimise fraud. We will however, provide fraud awareness training to our community partners as deemed necessary to help them implement robust controls to protect the funds they administer.

Contractors and partners are also expected to have adequate recruitment procedures in place covering requirements under the Immigration and Nationality Act, Criminal Records Bureau checks and stringent vetting in relation to employment history and references. This expectation will form part of all contract terms and conditions.

Employees - Recruitment and Conduct

It is recognised the majority of staff are conscientious and hard working and whose conduct is beyond reproach. However, where it becomes evident fraud and corruption has taken place, action will be taken in accordance with the Council’s Disciplinary Rules. Fraud and corruption are specific instances of gross misconduct and will therefore be treated very seriously and likely to involve criminal or civil proceedings as appropriate.

The Council recognises that a key preventative measure is to take effective steps at the recruitment stage to establish, as far as possible, the previous record of potential employees, in terms of their propriety and integrity. Temporary and agency employees will be treated in the same way.

Staff recruitment is required, therefore, to be in accordance with the Council’s recruitment and selection policies and, in particular, written references regarding known honesty and integrity of potential employees must wherever practicable be obtained before employment offers are made. Criminal records will be checked and disclosed prior to appointment in accordance with the Council’s Policy.

Employees of the Council are expected to follow the Employees’ Code of Conduct and any other Code related to their personal Professional Body.

Employees must comply with their statutory obligations regarding pecuniary interest in Contracts relating to the Council or fees and rewards other than proper remuneration. They are also required to declare any interests which they have that might be seen to conflict with the impartial performance of their duties.

Members (Elected Councillors)

Members are expected to conduct themselves in a way that is beyond reproach, above suspicion and fully accountable by acting in a manner that sets an example to the community they represent and employees who implement their policy objectives.

Malpractice of any sort will not be tolerated and where evidence indicates malpractice has occurred, a report will be made to the relevant Body.

Members are required to operate within:

- The Council Constitution
- Member Code of Conduct
These matters are specifically brought to the attention of Members and include the declaration and registration of potential areas of conflict between Members’ Council duties and responsibilities and any other areas of their personal or professional lives.

The Standards Committee will advise and train Members on matters relating to the Members’ Code of Conduct. The Committee will monitor the operation of that Code.

Detection and Investigation

This section should be read in conjunction with the Fraud Response Plan (Appendix 2).

The array of preventative systems, particularly internal control systems within the Council, has been designed to provide indicators of any fraudulent activity, although generally they should be sufficient in themselves to deter fraud it is often the alertness of employees, Members and the public to indicators of fraud and corruption that enables detection to occur and the appropriate action to take place when there is evidence that fraud or corruption may be in progress.

Employees must report any suspected cases of fraud and corruption to the appropriate manager, or, if necessary, direct to the appropriate Fraud Investigation Team. The Fraud Response Plan appended to this policy provides guidance on what do when an individual suspects fraud and corruption (other than benefit fraud) has or is taking place.

Reporting cases in this way is essential to the Fraud and Corruption Strategy and makes sure that:

- suspected cases of fraud and corruption are investigated properly
- there is a standard process for dealing with all suspected cases of fraud and corruption; and all connected persons and the Council’s interests are protected

The Fraud Investigation Teams are at the forefront of the Council’s fight against fraud and will examine all allegations of theft, fraud and financial malpractice, corruption and behaviour likely to adversely impact on the finances or integrity of the Council, its Members and employees. This extends to allegations against organisations funded by the Council or those with whom the council has a contract and those who receive council services.

It is expected that the Council’s partners will provide full and unrestricted access to their financial records relating to the council finances and the co-operation of their staff with any investigation. In addition, personnel records of any person suspected of involvement in fraud against the council will also be made available to the Fraud Investigation Teams.

The Council will utilise the additional powers of Police to obtain evidence or recovery of funds or where the matter cannot be pursued in-house, for example, serious organised crime and money laundering.

Referral to the Police will be undertaken in consultation with the Chief Finance Officer and in accordance with the Council’s Prosecution Policy. In cases involving Members, the Standards Committee would determine the issue of Police involvement.

Complaints of misconduct under the Members Code of Conduct will be dealt with in accordance with the Standards Committee’s arrangements.

Combining with Others
We will utilise all methods available to detect fraud. Arrangements are in place to actively participate in the Audit Commission’s National Fraud Initiative (NFI). We will also continue to develop and support initiatives that involve the exchange of information and systematic data matching between the Council and other agencies on national and local fraud and corruption activity in relation to Local Authorities.

These agencies include:

- Police
- Department for Works and Pensions
- Her Majesty’s Revenue & Customs
- UK Border Agency
- Pensions Service
- JobCentre Plus

**Sanction and Redress**

The strongest available sanctions will be applied to all who commit fraud against the Council, its clients or the public purse. This may include disciplinary action, prosecution and civil proceedings or a combination of all three.

This also applies to employees who defraud or steal from the Council’s clients. Disciplinary action will also be taken against staff found to have committed fraud against other Local Authorities, or any other agency administering public funds.

Contractors or partner organisations will be expected to take appropriate action against the individual(s) concerned. The ability to request removal of staff will be considered in contract terms.

The decision to recommend any of all of the above sanctions will be made on a case by case basis, having regard to the Disciplinary Rules and Prosecution Policy in place at the time.

Sanctions imposed in relation to cases of fraud involving Members will be imposed by the Standards Committee in accordance with powers bestowed under appropriate Regulations.

**Fraud and Corruption Strategy**

To create a culture and organisational framework - through a series of comprehensive and inter-related procedures and controls - which minimises the risk and impact of fraud or corrupt acts against the Council, whether internally or externally perpetrated.

Where fraud and corruption does occur, to fully investigate all cases and, where proven, take a zero tolerance approach through appropriate use of the full range of available sanctions and penalties. The Strategy is based on the following principles of best practice:

**Acknowledge** - Acknowledging and understanding fraud risks

- Assessing and understanding fraud risks
- Committing support and resource to tackling fraud
- Maintaining a robust anti-fraud response

**Prevent** - Preventing and detecting more fraud

- Making better use of information and technology
- Enhancing fraud controls and processes
• Developing a more effective anti-fraud culture

**Pursue** - Being stronger in punishing fraud and recovering losses

- Prioritising fraud recovery and the use of civil sanctions
- Developing capability and capacity to punish fraudsters
- Collaborating across local authorities and with law enforcement

**Links to Corporate Objectives**

The vision for the Borough is to **Encourage growth and unlock the potential of Barking and Dagenham and its residents**

To achieve the Vision, the Council’s priorities are:

1. Ensure every child is valued so they can succeed
2. Reduce crime and the fear of crime
3. Improve health and wellbeing through all stages of life
4. Create thriving communities by maintaining and investing in new and high quality homes
5. Maximise growth opportunities and increase the household income of Borough residents

This Policy and Strategy ensures resources are correctly applied in the provision of high quality services and initiatives that deliver these Corporate Objectives.

**Resources**

A Corporate Anti Fraud Team will be maintained, to investigate all issues of suspected fraud and irregularity other than housing benefit fraud and to promote the anti-fraud agenda of the Council through proactive and preventative activities.

A Housing Investigation Team will investigate allegations of abuse concerning council housing and seek to recover council properties, for example where it is determined the registered tenant is not in residence as defined by the tenancy agreement, with the aim of delivering housing units back to proper use, and prevent misuse of the Social Housing Stock.

The authority for Fraud Investigators to investigate is enshrined in the Council’s Constitution, Financial Rules.

Internal Audit will, within the context of the Chief Finance Officer statutory powers, have authority for internal audit purposes to:

- Enter at all reasonable times in to any Council premises or onto Council land
- Have access to all records, documents and correspondence relating to operations or transactions of the Council
- Require and receive such explanations as are necessary concerning any matters under examination
- Require any employee of the Council to produce cash, stores or any other property of the Council in her/his custody

A Housing Benefit Team will undertake investigation of referrals of suspected benefits fraud. Visiting Officers will visit benefit customers to check the details of their claim obtaining any necessary supporting documentation in accordance with the DWP Verification Framework.
Housing Benefit Fraud Investigators will be appointed as “Authorised Officers” who have the power of entry and inspection under section 110A of the Social Security Administration Act 1992. “Authorised Officers” must be right and proper persons and be issued with a certificate of appointment which will last for no more than one year at a time.

“Authorised Officers” will use their powers in connection with a claim for Housing Benefit and or Council Tax Benefit to enter business premises of landlords, agents or employers to inspect relevant documents and to interview persons found on the premises.

The “Authorised Officers” will also use their powers to write and request information from prescribed persons or businesses.

Any abuse of these powers will result in the “Authorised Officers” being subjected to disciplinary procedures.

Training

The Council will ensure that all Fraud Investigators are fully trained, appropriately qualified and are continually kept up to date with respective relevant legislative changes.

Publicity

Publicity will be used appropriately to discourage those who might seek to commit fraud both generally and in instances of specific outcomes from individual cases, to highlight the existence and work of the Anti-Fraud Teams and to promote the zero-tolerance approach.

All successful prosecutions for benefit fraud will be reported within internal and external media.

Fraud Reporting

The Council has in place dedicated fraud and whistleblowing telephone hotlines, web forms and email addresses to enable members of the public to report concerns about possible fraudulent activity. All calls will be followed up by appropriate Fraud Investigators and all information supplied will be treated as private and confidential.

Case Management

Fraud Investigation Teams will maintain electronic records (e.g. case management system) to assist with the proper management, monitoring and recording of cases subject to investigation.

Considerations for Anti-Fraud Officers

When investigating fraud, Investigators and Visiting Officers will work to professional standards and in accordance with codes of practice as well as applying the Council's policies on equalities & diversity and customer care. They will at all times apply appropriate procedures to maintain confidentiality. They are expected to comply with the Council's Code of Conduct specific to their activity.

Additionally, they will operate within the guidelines of:
- The Police and Criminal Evidence Act 1984, in undertaking an investigation Council officers will observe the Police and Criminal Evidence Act Codes of Practice. The customer will be advised of their rights and evidence will be obtained and secured in accordance with the Act. These Codes of Practice will
also be observed when taking statements. Officers, when dealing with a suspected fraud, will comply with the requirements of the Human Rights Act. The Council will act in accordance with the current data protection legislation and any advice issued by the Information Commissioner. It is registered with the Commissioner that data may be used for the prevention of crime and the prosecution of offenders. It will use exemptions under the legislation to protect those organisations and individuals who may be asked to supply information to the Council in its investigation of fraud.

Council officers will abide by the requirements of the Regulation of Investigatory Powers Act when conducting surveillance in relation to a suspected fraud.

Whistleblowing Policy & Public Interest Disclosure Act 1998 & Enterprise and Regulatory Reform Act 2013
The Council has set out a policy of whistleblowing in accordance with the Public Interest Disclosure Act. In accordance with this policy Council employees and elected members are expected to inform the Council of any concerns in the public interest about suspected malpractice by colleagues. The Council will follow the procedures set out in the policy when responding to such concerns.

Definitions

What is theft?
Under section 1 of the Theft Act 1968 “A person is guilty of theft if: he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.”

Examples of theft include stealing any property belonging to the council or which has been entrusted to it (i.e. client funds); including cash, equipment, vehicles and data and can also include the stealing of property belonging to our staff or members whilst on council premises.

Under section 24A of the Theft Act 1968, a person is also guilty of theft where ‘they dishonestly retain a wrongful credit’. For example where they do not report and repay an overpayment of salary or advance.

What is fraud?
The Fraud Act 2006 introduced into statute the first legal definition of fraud.

For the purposes of this strategy, fraud is defined as the intentional distortion of records for gain; corruption as the offering or acceptance of inducements designed to influence official action; financial malpractice as theft of funds or assets from the Council or its clients and intentional, unauthorised breaches of financial regulations; and misuse of official position as employees or their friends, relatives or acquaintance benefiting inappropriately from exercise of duty.

Fraudulent acts may arise from:
**Systems Issues** - i.e. where a process /system exists which is prone to abuse by either employees or members of the public e.g. Housing Allocations.

**Financial Issues** - i.e. where individuals or companies have fraudulently obtained money from the Council. Examples include falsification of expense claims, theft of cash and alteration of records to conceal deficiencies, falsification of invoices for payment, failure to account for monies collected.

**Equipment Issues** - i.e. where Council equipment is used for personal reasons, for example personal use of council vehicles.

**Resource Issues** - i.e. where there is a misuse of resources for example theft of building materials or working in a private capacity during contracted hours or whilst sick.

**What is corruption?**

In contrast, corruption has been defined as the offering, giving, soliciting or acceptance of an inducement or reward which may influence the action of any person contrary to the proper conduct of their duties.

Examples of areas where corruption can occur include tendering and awarding of contracts, appointment and reward of external consultants, awarding permissions, planning consents and licenses.

Types of inducement include cash, “free” holidays, “free” professional services and advice, provision of goods or materials, “free” entertainment such as tickets to sporting events.

This area is covered in greater depth by the Bribery Act Policy.

**Further Support, Tools & Guidance**

The latest version of the Fraud & Corruption Policy & Strategy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

[Anti Fraud Information](#)

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

[david.greenfield@lbbd.gov.uk](mailto:david.greenfield@lbbd.gov.uk)
1. STATEMENT OF INTENT

The Council is committed to providing Housing Benefit & Council Tax Benefit to its eligible residents promptly and accurately following the receipt of all necessary supporting information.

It will do all it can to ensure that customers receive the benefits to which they are entitled. It will encourage the take up of benefits by those people who are eligible.

The Council is also aware that some people will attempt to obtain benefit to which they have no entitlement or continue to receive benefit for which they are no longer eligible. It is therefore committed to a robust anti fraud stance in order to protect public funds and to ensure that benefits are delivered only to those who have entitlement to them.

When a fraud has occurred it will consider taking sanctions against the customer dependent upon their personal circumstances and the gravity of the case. Decisions will be taken in accordance with the Council's Prosecution Policy.

2. DUTIES AND CONSIDERATIONS OF BENEFIT OFFICERS

The Council is also committed to prevent benefit fraud by staff therefore all new staff employed in benefits and fraud administration will be rigorously vetted before being offered employment. Any issues that arise subsequently will be dealt with under disciplinary procedures.

The Council requires all officers involved in benefits and fraud administration to report:

- details of any property they are renting to tenants
- any claims for benefit in which they may have an interest

An interest is defined as a claim for benefit where the officer is

- the landlord or agent
- the customer or partner of the customer
- is a dependent or non dependant of the customer

If an officer involved in the administration of benefits or fraud has knowledge of a claim where the customer is a close family member as described by the Housing Benefit and Council Tax Benefit General Regulations, that officer must report the facts.

Interest in a benefit claim must be recorded in the Register of Employee Disclosures and Interests in accordance with agreed procedures. Officers will undertake regular checks on all properties recorded in this register to ensure that no benefit payment has been made in relation to these properties without the prior knowledge of Managers.

Any officer found to be involved in any offence involving any claims for benefit from the Department for Work & Pensions or any local authority will be disciplined under the disciplinary procedures in addition to any prosecution that may occur.

Where any officer investigating a fraud is believed to have abused their powers an investigation will take place with a view to disciplinary action being taken.
Gifts and hospitality offered to employees as a consequence of their role as an employee must be reported to their line manager and recorded in the Register of Gifts and Hospitality in accordance with agreed procedures.

3. DUTIES AND CONSIDERATIONS OF ELECTED MEMBERS

The Council requires all elected members to report details of:

- any property they are renting to tenants
- any claims for benefit in which they may have an interest

An interest is defined as a claim for benefit where the member is:

- the landlord or agent
- the customer or partner of the customer
- is a dependant or non dependant of the customer

Interest in a benefit claim must be recorded in the Council's Register of Interests in accordance with agreed procedures. Officers will undertake regular checks on all properties recorded in this register to ensure that no benefit payment has been made in relation to these properties without the prior knowledge of Managers.

Gifts and hospitality offered to a member as a consequence of their role as an elected member must be recorded in the Register of Gifts and Hospitality in accordance with agreed procedures.

4. DATA MATCHING EXERCISES

The Council will use the Department for Work & Pensions Housing Benefit Matching Service (HBMS) which checks benefit claim data for duplication and inconsistencies with data held by other authorities, the Pensions Service and Jobcentre Plus.

The Council will participate in the National Fraud Initiative (NFI) administered by the Audit Commission which allows comparison of Housing Benefit data against other data sources to identify inconsistencies requiring further investigation.

The Council will also run data matching exercises against its own records but will consult with recognised trade unions prior to data matching payroll data of staff and members.

At all times the Council will act in accordance with its understanding of the law and guidance issued by the Information Commissioner, the Department for Work & Pensions and the External Auditor.

5. VERIFICATION OF HOUSING BENEFIT & COUNCIL TAX BENEFIT CLAIMS

To discourage and prevent fraud from taking place the Council have adopted the Department for Work & Pensions Verification Framework.

The information on the Benefit claim form will be verified by Benefits staff with all supporting documentation photocopied by the relevant officer and endorsed with their name and signature before the original document is returned to the customer.

The DWP Customer Information System (CIS) which is a web enabled application that all Benefit Officers have access to will be used by designated officers to validate information concerning the payment of Income Support or Jobseekers Allowance by that agency.
If fraud is suspected further enquiries will be made which may include contacting third parties and interviewing under caution those suspected in accordance Police and Criminal Evidence Act.

Although all claims for benefit will come under close scrutiny the Council is committed to paying benefit accurately and speedily within recognised time scales. Advice and assistance will be given to customers when applying for benefit to maximise take up.

6. BENEFIT CLAIM FORM

The Council will ensure that its application form for Housing Benefit and Council Tax Support includes questions and instructions in plain language. The form will make clear to the customer that giving false information could result in the customer being prosecuted. It will also state that the Council may cross check information on the form with other Departments within the Council, other agencies, other Councils and the Rent Officer Service.

The Council will put in place systems which will help the customer to make their claim for benefit and remind them of the need to advise the Council promptly of any change in circumstances. This will include those customers whose ethnicity or disability presents particular difficulties.

The Housing Benefit & Council Tax Support claim form will be reviewed and amended regularly to ensure it remains helpful to customers when applying for benefit.

7. OVERPAID BENEFIT TO CUSTOMERS

If benefit has been obtained from the Council where there was no entitlement, for example due to a false claim or a failure to disclose a change in circumstances, the Council will consider the particulars of the individual case. If it is deemed that the customer could reasonably have known they were being overpaid benefit the Council will consider prosecution in accordance with the Prosecution policy.

Where appropriate the Council will consider applying either an administrative penalty equal to 30% of the overpayment or issuing a local authority caution as alternatives to prosecution.

If it is considered not to be in the public interest to apply a relevant sanction the Council will still seek to recover the overpaid benefit in accordance with the Council's overpayment policy.

8. OVERPAID BENEFIT TO LANDLORDS

Payments of benefit are often made directly to landlords on behalf of customers. If a landlord falsifies a claim or assists a customer to falsify a claim they are guilty of an offence and will normally be prosecuted by the Council in accordance with the Prosecution policy.

Landlords who receive benefit directly are obliged to report any change in their tenant’s circumstances. Failure to do so may result in more benefit being paid directly than is actually due.

The Council will make landlords aware of their duty to report a known change of circumstances and that failure to do so is an offence. If the Council believes that an offence has been committed it will consider prosecution and will recover any overpaid benefit either from future direct payments to the landlord or by civil recovery through the Courts.

The Council will expect its Fraud Investigators to use their powers of inspection to obtain information from landlords. These powers will be used reasonably and in compliance with the regulations.
9. "DO NOT REDIRECT MAIL"

The Council will use the "do not redirect mail" service provided by the Post Office to prevent benefit payments being redirected to other addresses.

10. PROACTIVE CAMPAIGNS

The Council will undertake periodic benefit fraud campaigns either alone or in partnership with another authority or organisation.
Appendix 2 Fraud Response Plan

The London Borough of Barking and Dagenham is committed to developing a culture of honesty and zero tolerance to fraud and corruption.

The purpose of this document is to demonstrate and set out the procedures to be followed where theft, fraud or corruption (other than Benefit Fraud) is suspected or detected. It is part of the Council’s overall fraud and corruption policy & strategy. It therefore applies to all Members (elected Councillors) and all personnel whether staff of the London Borough of Barking and Dagenham, consultants, agency staff or contractors.

It also provides a framework for responding that enables evidence to be gathered and collated in a way which facilitates an informed initial decision and ensures that any evidence gathered will have been lawfully obtained and will be admissible if the matter proceeds to criminal or civil action.

This document is not an investigation procedure for staff. If you suspect fraud it is vital that you follow the guidance in this plan and report your suspicions to the Corporate Anti-Fraud Team. Neither does this document provide guidance on fraud prevention. It is quite simply a brief guide on “what to do if you become aware of fraud” and tells you how the Council will respond to suspected or actual occurrences of fraud.

Roles & Responsibilities In Respect Of Fraud and Corruption

All staff and Elected Members have duties under the Council’s Corporate Governance arrangements to prevent and detect occurrences of fraud and have a responsibility to ensure compliance with relevant legislation in discharging these duties.

The Group Manager (Internal Audit & Anti-Fraud) will maintain a log of all reports, detail actions taken and conclusions reached and report periodically to Members of the Public Accounts & Audit Select Committee.

The Group Manager (Internal Audit & Anti-Fraud) will ensure a consistent approach to the conduct of any investigations into matters reported and that proper records of each investigation are kept from the outset, including accurate notes of when, where and from whom evidence was obtained, and by whom.

Where a member of staff is to be investigated, the relevant Chief Officer and Departmental Human Resources Officer will be informed. Normally, the member of staff’s line manager will also be informed unless this is deemed to be inappropriate given the circumstances of the case.

If a suspicion is reported to a manager, s/he must pass that suspicion on to the Corporate Anti-Fraud Team immediately. Any delay could compromise subsequent investigations.

What should staff do if they suspect fraud or corruption?

Employees are often the first to become aware that there is something seriously wrong within the Council.

If you suspect or become aware of fraud or any other illegal act perpetrated by an employee, or other individual(s) against the Council, there are several avenues through which your concerns should be reported.

Initially your concerns should be brought to the attention of your line manager. Alternatively, the matter may be raised with the Corporate Anti-Fraud Team who can advise or discuss the matter informally.
You can also report concerns via the Fraud telephone Hotline and/or dedicated email address.

If you feel unable to express concerns openly and wish to report concerns in confidence, you may do so in accordance with the Council’s Whistleblowing Policy without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

**When you become aware that there may be a problem you should:**

- Make an immediate written note of your concerns, details of any telephone or conversations you have heard or documents you have seen, and note the date, time, and names of the people involved. These notes should be signed, timed and dated. Timeliness is important because the longer you delay writing up the notes, the greater the chances of recollections becoming distorted and the case being weakened.

- Pass any documents that would normally come into your possession immediately to the Corporate Anti-Fraud Team if this can be done without alerting suspicions; this should include any relevant emails.

**You should not:**

- Ignore the concerns or be afraid of raising them. You will not suffer recriminations from your employer as a result of voicing a reasonably held suspicion.

- Approach individuals yourself or convey your suspicions to other staff, except those authorised to deal with the matter. There may be an innocent explanation that resolves your concerns. If you have any doubts about who to consult, speak to the Corporate Anti-Fraud Team first.

- Investigate the matter yourself. There are special rules relating to the gathering of evidence for use in criminal cases. Attempts to gather evidence by persons who are unfamiliar with these rules may jeopardise or undermine the case.

- Discuss it with anyone else after you have reported your suspicions.

**What should a member of the public or a partner organisation do if they suspect fraud or corruption?**

The Council encourages members of the public who suspect fraud and corruption to contact the Group Manager (Internal Audit & Anti-Fraud) in the first instance. Suspicions or identified instances of fraud, corruption or other wrongdoing against the Council can be reported via a confidential hotline number.

**How will allegations of fraud and corruption be dealt with by the Council?**

The Corporate Anti-Fraud Team operates independently of other Council services but will pool resources with other stakeholders such as the Internal Audit, Housing Investigation and Benefit Fraud Teams to provide a joined up approach to prevention, detection, investigation and prosecution of fraud and corruption within the council.

When allegations are received from staff or the public the Corporate Anti-Fraud Team will establish at an early stage the action to be taken by the Council; this may depend on the nature of the
allegation. The matters raised may be investigated internally; however, allegations of wrongdoing involving a criminal act may shape the way the investigation is handled and by whom.

Within ten working days of a concern being received, the responsible officer will write to the complainant:

- Acknowledging that the concern has been received
- Indicating how they propose to deal with the matter
- Giving an estimate of how long it will take to provide a final response; and
- Informing whether or not any further investigations will take place

If it appears that a criminal act has occurred or where there is sufficient evidence of fraud or corruption, the Police will be involved in accordance with the Council’s Prosecution Policy. In most cases, referral to the police will be the normal course of action.

All staff must cooperate fully with police or any other form of external enquiry.

Where the police are unable to progress a criminal prosecution, e.g. because the burden of proof is insufficient to convince the Crown Prosecution Service to proceed, legal opinion will be sought as to the expediency of civil action particularly in relation to recovering losses.

If it appears not to be a criminal matter, an internal investigation will be undertaken to:

- Determine the facts
- Consider if the allegation should be dismissed or
- What action should be taken against any staff found culpable
- Consider what action may be taken to recover any losses to the Council which could include civil action
- Identify whether the Council’s systems, controls or procedures need to be improved

If the outcome of an investigation is that action should be taken against an employee, the Corporate Anti-Fraud Team will advise the appropriate service manager and/or Divisional Director and liaise with the Human Resources section to determine whether disciplinary action is appropriate for:

- misconduct i.e. negligence or error of judgement
- gross misconduct, i.e. dishonesty

A fraud log will be completed detailing every action taken during the investigation, this will include the dates and times that each action undertaken was carried out.

**How we gather and deal with evidence**

The Corporate Anti-Fraud Team will normally manage investigations and will be responsible for gathering evidence and will seek to establish whether there is any physical evidence that fraud has occurred and collect such evidence, recording the time and place that the evidence was obtained.

Where there are reasonable grounds for suspicion, the police will be involved at an early stage however the Group Manager (Internal Audit & Anti-Fraud) may still undertake part or all of the investigation on behalf of the police. All employees MUST co-operate with the investigation process.
If appropriate, and in accordance with Human Resources policies and with their agreement, suspension of officers will be considered to ensure unfettered progress of investigations. It should be noted that suspension is a neutral act and in no way implies guilt of the officer.

Failure to co-operate will itself constitute a disciplinary offence.

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. Wherever possible original documents should be retained, secured and handled as little as possible. Under no circumstances should they be marked in any way. Computer data must also be secured and should not be viewed by anyone who is not appropriately trained.

All evidence will be obtained lawfully, properly recorded and retained securely in accordance with the Police and Criminal Evidence Act 1984 and the Criminal Procedure and Investigations Act 1996.

The outcomes of significant internal investigations will be reported to the Public Accounts & Audit Select Committee.

Conducting interviews

Interviews will be conducted in a fair and proper manner and in accordance with the Council’s Disciplinary Rules.

As much documentary evidence as possible will be gathered before any interviews are conducted. If it is established there are any witnesses to the events the Corporate Anti-Fraud Team will seek to interview witnesses and obtain written statements. File notes of all actions and discussions will be maintained. The veracity of the information provided by witnesses and or other evidence documentary or otherwise will determine whether the employee should be interviewed.

Where there is a possibility of subsequent criminal action, the police will be consulted and interviews may be conducted under caution in compliance with the Police and Criminal Evidence Act 1984 which governs the admissibility of evidence in court proceedings.

Closing the investigation

The investigation will be concluded by deciding whether there is a case to answer and by making recommendations as to appropriate action in a written report to the relevant manager and Divisional Director as well as improvements to systems and procedures.

Management will seek advice from Human Resources to establish the correct procedure to progress the matter through the Council’s disciplinary framework.

For acts of dishonesty, false accounting, gross negligence, deception, or theft, employees can expect to be dismissed. Employees found to have committed fraud against other organisations responsible for the administration of public funds will be considered to have brought this Council into disrepute and can expect to be dismissed.

All matters investigated will be dealt with in accordance with the Council’s Human Resources Disciplinary Rules and Code of Conduct for Employees.
The Fraud Prosecution Policy
(Incorporating Housing Benefit Fraud)
March 2014
The Council's commitment to the Prosecution Policy

The London Borough of Barking & Dagenham is committed to the protection of public funds through its action against fraud and has adopted a zero tolerance approach to fraud and wrong doing perpetrated against it. The Council will seek application of the strongest possible sanctions against those found to have perpetrated fraud against it.

What are the aims and requirements of the legislation?

The aim of this prosecution policy is to deter fraud against the Council including fraudulent benefit claims.

This policy sets out the range of sanctions that may be applied where fraud and wrongdoing is identified and the circumstances relevant to their application.

Who is governed by this Policy?

This policy applies to claimants of Housing Benefit or Council Tax Support, council employees, contractors and members of the public found to have committed fraud and other wrongdoing against the Council.

Disciplinary action will also be taken against Council employees found to have made fraudulent benefit claims.

Executive Summary

The London Borough of Barking & Dagenham is committed to the protection of public funds through its action against fraud. Where a claimant of Housing Benefit or Council Tax Support has been accused of committing a fraud against the Council and the Fraud Investigation Team have enough evidence to sustain prosecution the Council will employ any or all of three sanctions available to it.

Where other types of fraud and wrong doing are identified the Council will employ disciplinary action (in the case of Staff), civil action or criminal sanctions or a combination of all three in parallel.
## Contents

<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Prosecution Policy</td>
<td>4</td>
</tr>
<tr>
<td>General Fraud Sanctions &amp; Redress</td>
<td>5</td>
</tr>
<tr>
<td>Housing Benefit Fraud Sanctions &amp; Redress</td>
<td>6</td>
</tr>
<tr>
<td>Further support, tools and guidance</td>
<td>8</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>9</td>
</tr>
</tbody>
</table>
Fraud Prosecution Policy

The London Borough of Barking and Dagenham is committed to preventing fraud and corruption wherever possible. All allegations of fraud and corruption will be taken seriously.

Where fraud and corruption is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the fraud and corruption strategy. It will be investigated fully and the London Borough of Barking and Dagenham will prosecute all offenders where appropriate including Members, employees, contractors and external partners, in accordance with this policy.

This procedure will be operated in conjunction with the London Borough of Barking and Dagenham’s disciplinary procedures and all employees will be subject to disciplinary action as well as any prosecution process.

Where there is clear evidence that a fraudulent or corrupt act has been committed, the following will be taken into account before a case is considered for prosecution.

- The seriousness of the case
- The level of evidence available
- The level of money or misappropriated assets involved
- Whether the public interest will be served

In assessing a case for prosecution, the following tests will be applied:

- **The Evidential Test:** To ensure sufficiency of evidence to provide a realistic prospect of conviction
- **The Public Interest Test:** To determine whether or not it would be in the public interest to proceed

A prosecution will usually be pursued unless there are public interest factors tending against prosecution which clearly outweigh those tending in favour. To pass the public interest test, Fraud Investigators will balance carefully and fairly the public interest criteria as detailed in ‘The Crown Prosecution Service’s Code for Crown Prosecutors 2010’ against the seriousness of the offence.

The public interest criterion includes:

- The likely sentence (if convicted)
- Whether the offence was committed as a result of genuine mistake or misunderstanding
- Any previous convictions and the conduct of the defendant

The Council will in most instances prosecute where the fraud perpetrated:

- was not a first offence
- was planned
- was undertaken by an officer in a position of authority or trust and he or she took advantage of this, or
- involved more than one person

The full tests the council will apply in considering a case for prosecution are set out in Appendix 1.
Applicable sanctions differ between general fraud and benefit fraud in accordance with legislation, as follows.

With respect to a prima facie case of fraud, an appropriate combination of the following three sanctions may be applied.

- **Disciplinary Action** - Application of this sanction is normally internal disciplinary action but may involve a referral to the relevant professional organisation from which professional disciplinary action could ensue

- **Civil Action** – to recover money, interest and costs where it is cost effective and desirable for the purpose of deterrence, it may be decided that civil redress is the most appropriate course of action. In such instances the council’s legal services team will utilise civil law to recover any losses

- **Criminal Sanction** - fines, imprisonment, and compensation orders

Where it is decided that a criminal prosecution is to be pursued, the Group Manager (Internal Audit & Anti-Fraud) will be consulted and will brief the Chief Finance Officer and Chief Executive as appropriate. However, the option to prosecute may also be determined by the police in some instances.

Managers should not notify the police directly, except in an emergency in order to prevent further loss, or where it is necessary for the police to examine an area before it is disturbed by staff or members of the public.

In instances where an investigation reveals either;

- numerous cases of fraudulent activity
- significant value, or
- breaches of the employee code of conduct and/or disciplinary rules

The option of pursuing a series of sanctions (parallel sanctions) may be chosen.

The individual or parallel sanctions that are to be applied will be the decision of the Corporate Anti-Fraud Team following consultation with the Group Manager (Internal Audit & Anti-Fraud).

In instances where parallel sanctions are applied, for example, internal disciplinary and criminal sanctions, the Corporate Anti-Fraud Team will carry out an investigation with a view to criminal prosecution, whilst simultaneously conducting an internal investigation under the Disciplinary Procedure.

The Corporate Anti-Fraud team will provide sufficient evidence to Human Resources in order that an internal investigation and disciplinary hearing can be taken forward with respect to the evidence given. The advantage of this approach is that all appropriate action is taken at the earliest opportunity.

The Council believes fair and effective prosecution is essential in order to protect public funds and deter fraudulent activity.

Irrespective of the sanctions pursued for general fraud, the council will use all measures available to it to recover any money lost due to fraudulent activity.
In respect to criminal sanctions, this will be sought through the application for a Compensation Order to the Courts. This Order will not only outline the losses sustained by the council through fraud but also the investigation costs.

In respect of Internal Disciplinary, the council has a responsibility following the outcome of its investigation, to initiate an appropriate procedure aimed at recovering all monies identified as being lost or misappropriated through fraud.

The mechanism by which misappropriated monies are to be repaid will normally be established and agreed prior to any sanction being applied, and may be managed through utilisation of procedures such as deduction from salary or debtor invoicing.

Where the above mechanisms fails to recover any monies owed to the council, following advice from Legal Services, the Corporate Anti-Fraud Team will consider the option of civil redress.

Civil redress is available to the council in all instances where initial attempts to recover the loss, such as deduction from salary or debtor invoicing, have failed. In such instances, if considered appropriate, Legal Services will make an application either to the Small Claims or County Court - depending on the value to be recovered.

Other Redress - the council will also seek recovery of losses from pension entitlements where appropriate.

Where other fraudulently obtained assets are found to be held, confiscation orders under Proceeds of Crime legislation will also be considered utilising the police or other Financial Investigator resource.

**Housing Benefit Fraud Sanctions & Redress**

The Council has the power to impose three forms of sanction on those whom it believes have committed benefits offences. Prosecutions will be reserved for those cases which in the opinion of the Council are the most serious. These will be followed by Administrative Penalties and Local Authority Formal Cautions.

**Factors Influencing Sanctions for:**

- Closure of the case with No further Action
- A Formal Caution
- An Administrative Penalty
- Prosecution

**Closure of the Case with No Further Action**

The Authority would consider using its discretion to close the case with no further action being taken by an Investigation Officer, although any overpayment would still be recovered if the circumstances in which the fraud arose are relatively minor, e.g.

- to the best of the council’s knowledge the claimant has never previously offended and
- there was no planning involved in the process and
- there was no other person involved in the fraud and
- the overpayment is low
A Formal Caution

If the circumstances in which the fraud arose are more serious, e.g.
- it is known the claimant had previously offended, but no Formal Caution has been previously recorded or 14 months have elapsed since the last Formal Caution
- Mitigating factors determine the need to consider a Formal Caution Penalty
- there was little or no planning involved in the process
- there were no other persons involved in the fraud
- An admission has been made

the Authority would consider issuing a Formal Caution.

What a Formal Caution is

Unlike the administrative penalty, a caution can only be issued when a customer has admitted an offence. It cannot be issued if the customer refutes or denies the charge. The case should be at prosecution standard if a caution is to be issued. If a caution is refused the Authority will refer to Prosecution Tests and decide upon suitability and cost effectiveness to prosecute.

To reflect the seriousness the Authority places on this course of action, a Caution will be administered by an Officer of no less seniority than a Senior Investigation Officer.

An Administrative Penalty

If the circumstances in which the fraud arose are fairly serious, e.g.
- to the best of the Council’s knowledge the claimant had never previously offended
- the person had not previously been issued with a Formal Caution or Administrative penalty in the last 14 months
- Mitigating factors determine the need to consider an Administrative Penalty
- The Penalty amount does not usually exceed £2000

the Authority would normally consider issuing an Administrative Penalty.

What an Administrative Penalty is

Section 115A of the Social Security Administration Act 1992, as amended by Section 15 of the Social Security Fraud Act 1997, allows an Authority to apply a penalty at a minimum of 50% or £350 whichever is the greater (up to £2000 maximum) of the total overpayment. This applies to offences wholly committed after 8 May 2012. The claimant has 14 days in which to change their decision. If a penalty is not accepted or is withdrawn, the Authority may consider prosecution. The Authority will refer to the prosecution tests and decide upon the suitability and cost effectiveness to prosecute. Consequently, all cases considered for penalties, must be at prosecution standard.

The offer of a penalty should happen at a special interview.

NOTE: Officers involved in the Interview under Caution, will not conduct the Administrative Penalty interview.

Prosecution

If the circumstances in which the fraud arose are very serious, e.g.
- it is known the claimant had previously offended or a Formal Caution/Administrative Penalty has been recorded in the last 14 months
- there was planning involved in the process
- there were other persons involved in the fraud
- the overpayment is of a high amount

the Authority would normally consider referring the case for prosecution.

It may still be appropriate to prosecute someone who has not been paid any benefit but where the attempt to defraud was so serious as to justify a prosecution.

Note, we will allow other local authorities, the DWP and the police to prosecute offences on our behalf, where it is appropriate to do so.

Publicity

Anti-Fraud officers will seek to publicise cases identified for prosecution, with the aim to deter others and thereby to prevent further frauds. The final decision to publicise will rest with the Council’s Press and Publicity Section.

Further Support, Tools & Guidance

The latest version of the Fraud Prosecution Policy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

Anti Fraud Information

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

david.greenfield@lbbd.gov.uk
Tests the council will apply in considering a case for prosecution: to be applied in considering a case for prosecution.

The Evidential Test

In deciding whether to refer a case for prosecution, the following tests will be considered:

- Is there sufficient evidence for a realistic prospect of a prosecution?
- Can the evidence be used in court?
- Could the evidence be excluded by the court e.g. because of the way it was gathered or the rule about hearsay?
- Is the evidence reliable?
- Is its reliability affected by such factors as the defendant’s age, intelligence or level of understanding?
- What explanation has the defendant given? Is the court likely to find it credible in the light of the evidence as a whole?
- Is the witness’s background likely to weaken the prosecution case? e.g. does the witness have any motive that may affect his or her attitude to the case?
- Are there any concerns over the accuracy or credibility of a witness?
- How clear is the evidence?
- Has there been any failure in investigation?
- Has there been any failure in benefit administration including delay?
- Is prosecution in the public interest?

The Public Interest test

In making a decision, the following factors should also be considered:

- Whether a conviction is likely to result in a significant sentence or a nominal penalty
- Whether the offence was committed as a result of genuine mistake or misunderstanding
- Cost effectiveness of taking the case to court
- Any abuse of position or privilege i.e. a member of staff or Councillor
- Whether the claimant is suffering from either significant mental or physical ill health
- Any social factors
- Any voluntary disclosure
- Any previous incidences of fraud
- The evidence shows that the defendant was a ringleader or an organiser of the offence
- There is evidence that the offence was premeditated i.e. the claim was false from inception
- There are grounds for believing that the offence is likely to be continued or repeated, e.g. by a history of recurring conduct
- The offence, although not serious in itself, is widespread in the area where it was committed
# Money Laundering Policy

**March 2014**

<table>
<thead>
<tr>
<th>Date Last Reviewed:</th>
<th>March 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>PAASC</td>
</tr>
<tr>
<td>Date Approved:</td>
<td>19 March 2014</td>
</tr>
<tr>
<td>Version Number:</td>
<td>1.1</td>
</tr>
<tr>
<td>Review Date:</td>
<td>March 2015</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Group Manager – Internal Audit &amp; Anti-Fraud</td>
</tr>
<tr>
<td>Post Holder:</td>
<td>David Greenfield</td>
</tr>
</tbody>
</table>
The Council’s commitment to the Money Laundering Policy

London Borough of Barking & Dagenham, “the Council” takes a zero tolerance approach to fraud and corruption and as such will be taking a proactive approach to the prevention, detection and reporting of suspected money laundering incidents.

What are the aims and requirements of the legislation?

The legislation has the aim to enable suspicious transactions to be recognised and reported to law enforcement agencies to deter and disrupt such practices

Who is governed by this Policy?

The Money Laundering Policy applies to all staff including and not limited to temporary staff, sessional staff and contractors. A failure to comply could be damaging to the finances and reputation of the Council.

Executive Summary

This Money Laundering Policy sets out the Council’s commitment to ensuring compliance with the requirements of the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 & 2012 and Chartered Institute of Public Finance and Accountancy (CIPFA) guidance for Local Authorities on Money Laundering.
<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money Laundering Policy</td>
<td>4</td>
</tr>
<tr>
<td>What is Money Laundering?</td>
<td>4</td>
</tr>
<tr>
<td>What is the legal definition?</td>
<td>4</td>
</tr>
<tr>
<td>What is the legislation?</td>
<td>4</td>
</tr>
<tr>
<td>How can suspicious activity be identified?</td>
<td>5</td>
</tr>
<tr>
<td>What are the areas at risk of Money Laundering?</td>
<td>5</td>
</tr>
<tr>
<td>Reporting of Money Laundering</td>
<td>5</td>
</tr>
<tr>
<td>Further support, tools, training and guidance.</td>
<td>6</td>
</tr>
</tbody>
</table>
Money Laundering Policy

Our policy is to do all we can to prevent wherever possible the Authority and its staff being exposed to money laundering, to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases. It is every member of staff’s responsibility to be vigilant.

What is Money Laundering?

Money Laundering is the term used for a number of offences involving the proceeds of crime. It is the process by which the identity of “dirty” money (i.e. the proceeds of crime and the ownership of those proceeds) is changed so that the proceeds appear to originate from legitimate “clean” sources.

Some areas of the Council’s activities are thought to be particularly vulnerable to attempts to launder money. It can simply involve receiving payment for goods or services with “dirty” money – usually cash. For the purposes of the new legislation it now includes possessing, or in any way dealing with, or concealing, the proceeds of any crime.

What is the legal definition?

Money Laundering is defined as:

- concealing, disguising, converting, transferring or removing criminal property from England, Wales, Scotland or Northern Ireland
- being involved in an arrangement which a person knows or suspects it facilitates the acquisition, retention, use or control of criminal property
- acquiring, using or possessing criminal property
- when a person knows or suspects that money laundering activity is taking place (or has taken place), or becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, they must disclose this as soon as practicable or risk prosecution

What is the legislation?

The Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007 & 2012 places specific obligations on persons who are involved in “relevant business”. Offences under the Proceeds of Crime Act and Money Laundering Regulations can attract penalties of unlimited fines and up to 14 years imprisonment.

How can suspicious activity be identified?

Employees dealing with transactions which involve income for goods and services (or other income), particularly where large refunds may be made or large amounts of cash are received, will need to consider issues such as:
For new customers:

- is checking their identity proving difficult?
- is the individual reluctant to provide details?
- is there a genuine reason for using the services provided?
- is the customer attempting to introduce intermediaries to either protect their identity or hide their involvement?
- is the customer requesting a large cash transaction?
- is the source of the cash known and reasonable?

For regular and established customers:

- is the transaction reasonable in the context of the service provider’s normal business?
- is the size or frequency of the transaction consistent with the normal activities of the customer?
- has the pattern of the transaction changed since the business relationship was established?

**What are the areas at risk of Money Laundering?**

Some areas of the Council’s activities are thought to be particularly vulnerable to attempts to launder money. Where a need is identified by the risk assessment, advice will be provided to line managers to enable them to provide more targeted training. This may be provided using in-house resources, or through courses and seminars run by external agencies.

Possible examples relating to the Council include:

- Conveyancing, including Housing Right-to-Buy transactions
- Housing Benefit fraud
- Payments in excess of £10,000 e.g. business rates, business rents, hall hire etc.
- Refunds of large overpayments to accounts e.g. as above, plus: Council Tax, hire fees etc.
- Suspiciously low tenders

Generally, for the types of transactions the Council is involved with which are at risk in relation to Money Laundering, for example the sale of a capital asset, the risk is mitigated because these transactions will be with large, well known companies who will be represented by their solicitors who have their own professional duties regarding the Money Laundering Regulations. Conversely, where we have similar transactions with un-represented individuals or bodies this is an area of greater risk and our response will need to reflect this.

**Reporting of Money Laundering concerns**

The Council has nominated the Chief Finance Officer as the main point of contact for money laundering issues and to act as the nominated Money Laundering Reporting Officer. Staff should report any suspicions to the Chief Finance Officer immediately as they arise.

Suspicious may be reported informally by telephone or email and the responsible officer will seek to establish the facts of the case and determine whether a formal referral to the National Criminal Intelligence Service (NCIS) is appropriate.
The Money Laundering Reporting Officer, or their delegated officer, will consult with staff as appropriate in order to investigate the matter.

**Further Support, Tools, Training & Guidance**

- The latest version of the Money Laundering Policy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

  **Anti Fraud Information**

  If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

  david.greenfield@lbld.gov.uk
Internal Audit

Whistleblowing Policy

March 2014

Date Last reviewed: March 2014
Approved by: PAASC
Date Approved: 19/3/14
Version Number: 1.1
Review Date: March 2015
Document Owner: Group Manager – Internal Audit & Anti-Fraud
Post Holder: David Greenfield
The council’s commitment to the Whistleblowing Policy

This Whistleblowing Policy sets out the Council’s commitment to ensuring compliance with the requirements of the Public Interest Disclosure Act 1998 as amended by the Enterprise and Regulatory Reform Act 2013. The council has designated the Monitoring Officer as Whistleblowing Officer.

What are the aims and requirements of this policy?

The Council wishes to encourage and enable employees and persons providing services on behalf of or to the council to raise serious concerns within the Council rather than overlooking the issue or ‘blowing the whistle’ outside.

For that reason, this policy has been put in place to make sure that if you want to come forward and raise any concern within the remit of this policy, you can do so with confidence and without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

Who is governed by this policy?

The whistleblowing policy applies to all staff (including those designated as casual, temporary, agency, authorised volunteers or work experience), and those contractors working for the Council on Council premises, for example, agency staff, builders, drivers. It also covers suppliers and those providing services under a contract with the Council, for example, care homes and sheltered accommodation.

To ensure your concern is treated as whistleblowing, you must identify yourself and the policy is in place to encourage this. We will consider anonymous allegations but it is less likely that we will conduct an investigation and achieve a successful outcome.

Executive Summary

Sometimes employees and those who contract with the council are the first to spot that something is wrong and putting the council and/or its residents at risk, but are reluctant to act for fear of not being taken seriously, that their concerns may not be justified or that they may be victimised for speaking out.

Legislation is in place to protect those that raise legitimate concerns in the public interest and in the right way.

This policy sets out the concerns that are dealt with under the whistleblowing procedure, the way in which you may raise concerns and how the Council will respond to those concerns.
What is whistleblowing? ................................................................. 43
Who is covered by this policy? .......................................................... 43
What types of action are covered by the policy? ..................................... 43
What is not covered by the policy? ....................................................... 44
Protecting you .................................................................................. 44
How to raise a concern ....................................................................... 45
How we respond to your concerns ...................................................... 46
Untrue Allegations ........................................................................... 46
It is our policy is to promote a culture of openness and a shared sense of integrity throughout the Council by inviting employees to act responsibly in order to uphold the reputation of the Council and maintain public confidence.

What is whistleblowing?

Whistleblowing is the reporting of suspected or ongoing wrongdoing at work.

We are committed to being open, honest and accountable. For this reason, concerns about malpractice and impropriety are taken very seriously. We want you to be able to raise any concerns that the interests of others and the Council (and therefore residents of Barking and Dagenham) are at risk, within the Council rather than overlooking the issue or ‘blowing the whistle’ outside.

This is because members of staff may be the first to spot anything that is seriously wrong within the council, however, they might not say anything because they think this would be disloyal, or they might be worried that their suspicions are not justified. They may also be worried that they or someone else may be victimised.

That is why we have produced this whistleblowing policy to help staff, including agency workers and contractors to contact us with concerns. This policy has been put in place to make sure that if you want to come forward and raise any concern which you feel relate to illegal, improper or unethical conduct, you can do so with confidence and without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

Who is covered by this policy?

The whistleblowing policy applies to all staff (including those designated as casual, temporary, agency, authorised volunteers or work experience), and those contractors working for the Council on Council premises, for example, agency staff, builders, drivers. It also covers suppliers and those providing services under a contract with the Council, for example, care homes and sheltered accommodation.

To ensure your concern is treated as whistleblowing, you must identify yourself and the policy is in place to encourage this. We will consider anonymous allegations but it is less likely that we will conduct an investigation and achieve a successful outcome.

What types of action are covered by the policy?

The policy is intended to deal with serious or sensitive concerns about wrongdoings that are in the public interest – referred to as public interest disclosures.

When you raise a concern under the whistleblowing policy it must be in the reasonable belief that it is in the public interest to do so. We may ask you to sign a declaration to ensure you understand this principle.

Examples of concerns that may be in the public interest are suspected or ongoing actions that fall into the following categories – the list of actions under each category is not exhaustive.

Criminal Offences
- Misuse of Council funds
- Other fraud or corruption
- Bribery
- An unlawful act
- A person abusing their position for any unauthorised use or for personal gain
- Improper or unauthorised use of Council money

**Failure to comply with legal obligations**
- A person deliberately not keeping to a Council policy, official code of practice or any law or regulation
- A person being discriminated against because of their race, colour, religion, ethnic or national origin, disability, age, sex, sexuality, class or home life

**Actions which endanger the health or safety of any individual**
- Service users, children or students, particularly children and adults in our care being mistreated or abused
- Any other danger to health and safety

**Actions which cause damage to the environment**
- The environment being damaged (for example, by pollution)

**Actions which are intended to conceal any of the above**
- Other wrongdoing including instances where attempts have been made to conceal or cover up wrongdoing

Your concern may be about members of staff, people who work directly for the Council, suppliers, or people who provide services to the public for us.

**What is not covered by the policy?**

You cannot use this policy to deal with serious or sensitive matters that are covered by other procedures, for example:

- Staff complaints about their contract of employment. These complaints are dealt with through our Grievance or Managing Performance at Work procedures.
- Customers’ complaints about our services. These complaints are dealt with through our Corporate Complaints Procedure.
- Allegations against councillors. Such allegations should be sent in writing to: The Monitoring Officer, London Borough of Barking and Dagenham, Civic Centre, Dagenham, Essex, RM10 7BN. Write "Private and Confidential" on your envelope.

A complaint form and other information is available online at: [http://www.lbbd.gov.uk/CouncilandDemocracy/Complaints/Pages/ComplaintsMembers.aspx](http://www.lbbd.gov.uk/CouncilandDemocracy/Complaints/Pages/ComplaintsMembers.aspx)

Also, you cannot use this policy to raise issues that have already been settled through other procedures, for example, matters previously resolved under the Council’s Disciplinary Rules procedures.

**Protecting you**

If your allegation is true, you have nothing to fear. But we understand that deciding to blow the whistle is not easy.

When you make a protected disclosure you have the right not to be dismissed, victimised or subjected to any other detriment because you have made a disclosure. Therefore, we will not tolerate any harassment or victimisation of a whistleblower and will treat such actions as a serious disciplinary offence which will be dealt with under the council Disciplinary Procedure.
We will do our best to protect your identity and keep your concerns confidential if this is what you want.

There may be occasions when you will need to provide statements of evidence in order for us to conclude the investigation. In this case we will not reveal your name or position without your permission or unless we have to do so by law, for example, if the evidence is required in Court then your anonymity may be subject to the decision of the Courts.

If you work for the Council, you should also know that any allegation you make will not influence, or be influenced by, any unrelated disciplinary action against you or any redundancy procedures that may affect you.

How to raise a concern

If you work for the Council, you should first raise your concern with your immediate supervisor or Group Manager (but obviously this will depend on the seriousness and sensitivity of the matter, and who is suspected of the wrongdoing).

Alternatively you may also raise concerns with your Divisional or Corporate Director.

Concerns that involve financial malpractice should always be raised with the Corporate Anti Fraud Team.

If you prefer, or you do not work for the Council, you can contact the Corporate Anti Fraud Team direct in any of the following ways:

- By writing to the Corporate Anti Fraud Team at:
  Whistleblowing, London Borough of Barking and Dagenham, Ground Floor, Civic Centre Annexe, Dagenham, Essex. RM10 7BN.

  (Write 'Private and Confidential' on your envelope)

- By phoning the Whistleblowing line on 020 8227 2541. You can leave a confidential voice-mail message 24 hours a day.

- By sending an e-mail to: whistle-blowing@lbld.gov.uk

To maintain confidentiality you are advised not to copy other people into your message to the whistleblowing mailbox

If for whatever reason you feel your concerns cannot be reported by way of the above reporting options, your concerns can be directed to the council Whistleblowing Officer:

  Monitoring Officer, Legal and Democratic Services, London Borough of Barking and Dagenham, First Floor, Civic Centre Annexe, Dagenham, Essex. RM10 7BN.

  (Write 'Private and Confidential' on your envelope)

If you are putting your concerns in writing it is best to give as much information as possible - including any relevant names, dates, places and so on.

You should also provide:

- The reason why you are concerned about a situation
- Background information
What you personally witnessed or extent to which you have experienced the problem. If possible you should provide documentary evidence.

The earlier you raise a concern, the easier it will be to take effective action.

You are strongly encouraged to raise your concerns in one of the ways set out above, but if you feel you are unable to raise the matter internally, or feel unsatisfied with any action we take, you could contact

- our external auditor;
- your local Citizens’ Advice Bureau
- relevant professional bodies or regulatory organisations
- a relevant voluntary organisation; or
- the police

You can get independent advice or support from an organisation called Public Concern at Work. Their contact details are:
Public Concern at Work
3rd Floor, Bank Chambers
6 - 10 Borough High Street
London SE1 9QQ
Phone: 020 7404 6609
E-mail: whistle@pcaw.co.uk

How we respond to your concerns

Within 10 working days of you raising a concern, the Whistleblowing Officer or designated investigator will:

- acknowledge that we have received your concern
- explain how we will handle the matter; and
- tell you what support is available to you

It is difficult to set further timescales as they depend on the nature of the allegation and the type of investigation we need to carry out.

The way we deal with the concern will depend on what it involves. If we need to take urgent action, we will do this before carrying out any investigation.

We will first make enquiries to decide whether we should carry out an investigation and, if so, how we should go about it. Throughout all our enquiries and any investigation, our main concern will be to put the interests of the public first.

Untrue Allegations

If you make an allegation which you believe is true, but it is not confirmed by our investigation, we will not take any action against you.

However, if the investigatory process finds you have made an allegation which you know is untrue; we will take appropriate disciplinary or legal action against you.
The latest version of the Whistleblowing Policy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

**Anti Fraud Information**

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

[david.greenfield@lbld.gov.uk](mailto:david.greenfield@lbld.gov.uk)
Internal Audit

The Regulation of Investigatory Powers (RIPA) Policy

March 2014

Date Last Reviewed: March 2014
Approved by: PAASC
Date Approved: 19 March 2014
Version Number: 1.1
Review Date: March 2015
Document Owner: Group Manager – Internal Audit & Anti-Fraud
Post Holder: David Greenfield
Purpose

(For text in **bold**, see glossary of terms – Appendix 1)

The RIPA Policy covers the proper conduct of crime prevention activities that involve use of covert directed surveillance, covert human intelligence sources or the accessing of communications data. Application of the policy ensures that the Council is operating in accordance with the RIPA Act 2000 (the 2000 Act) as amended by the Protection of Freedoms Act 2012 (the 2012 Act). This policy sets out the Council’s approach, in particular, it details the checks and balances in place to ensure that any use of covert techniques is lawful, necessary and proportionate.

Staff found to have breached the Acts or the Council’s Code of Practice are deemed to have breached the Council’s Employee Code of Conduct and will be liable to disciplinary action.

Related Documents

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA) and the Data Protection Act (DPA).

Investigations should be conducted in accordance with the Council’s Anti-Fraud & Corruption Strategy & Policy.

Who is Governed by this Policy

The RIPA Policy covers all council staff and those working on behalf of the Council who are engaged in prevention and detection activities which involve the use of surveillance or covert human intelligence sources.

Executive Summary

Regulation of a Local Authority’s use of surveillance, use of covert human intelligence sources and accessing of communications data is set out in the RIPA Act 2000.

Local Authorities’ abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of serious crime or disorder. Local Authorities are not able to use intrusive surveillance. Powers relating to directed surveillance were amended by the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS)(Amendment) Order 2012 to limit usage to the purpose of preventing or detecting a criminal offence where the potential punishment is a maximum term of at least 6 months of imprisonment or involving potential offences involving underage sales of tobacco and alcohol.

The RIPA (Communications Data) order came into force in 2004. It allows Local Authorities to acquire communications data, namely service data and subscriber details for limited purposes. This order was updated by the Regulation of Investigatory Powers Communications Data) Order 2010.

The Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

The purpose of Part II of the Act is to protect the privacy rights of anyone in a Council’s area, but only to the extent that those rights are protected by the HRA. A public authority, such as the Council, has the ability to infringe those rights provided that it does so in accordance with the rules, which are contained within Part II of the Act. Should the public authority not follow the rules, the authority loses the impunity otherwise available to it. This impunity may be a defence to a claim for
damages or a complaint to supervisory bodies, or as an answer to a challenge to the admissibility of evidence in a trial.

Further, a Local Authority may only engage the Act when performing its ‘core functions’. For example, a Local Authority may rely on the Act when conducting a criminal investigation as this would be considered a ‘core function’, whereas the disciplining of an employee would be considered a ‘non-core’ or ‘ordinary’ function.

In line with the Code of Practice issued by Central Government associated with the 2012 Act, LBBD will only use covert surveillance under RIPA powers where it is proportionate and necessary to do so, and only in the investigation of serious criminal offences.
# Contents

<table>
<thead>
<tr>
<th>Introduction</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed Surveillance</td>
<td>1</td>
</tr>
<tr>
<td>Covert Human Intelligence Sources</td>
<td>3</td>
</tr>
<tr>
<td>The Authorisation Process</td>
<td>4</td>
</tr>
<tr>
<td>Magistrate Authorisation</td>
<td>5</td>
</tr>
<tr>
<td>Authorisation periods</td>
<td>7</td>
</tr>
<tr>
<td>Urgency</td>
<td>7</td>
</tr>
<tr>
<td>Telecommunications Data - NAFN</td>
<td>8</td>
</tr>
<tr>
<td>Handling of material and use of material as evidence</td>
<td>8</td>
</tr>
<tr>
<td>Training</td>
<td>9</td>
</tr>
<tr>
<td>Surveillance Equipment</td>
<td>9</td>
</tr>
<tr>
<td>RIPA Record Quality Reviews</td>
<td>9</td>
</tr>
<tr>
<td>The Inspection Process</td>
<td>9</td>
</tr>
<tr>
<td>Resources</td>
<td>9</td>
</tr>
</tbody>
</table>

**Appendix 1 – Glossary of terms**
**Appendix 2 – Human Rights Act**
**Appendix 3 – Data Protection Act**
**Appendix 4 – Key RIPA Officers**
**Appendix 5 – RIPA Forms**
**Appendix 6 – The Central Register**
**Appendix 7 – Best practice for photographic and video evidence**
**Appendix 8 – RIPA Authorising Officer’s Aide-Memoire**
Introduction

‘It is essential that the Chief Executive, or Head of Paid Service, together with the Directors and the Heads of Units should have an awareness of the basic requirements of RIPA and also an understanding of how it might apply to the work of individual council departments. Without this knowledge at senior level, it is unlikely that any authority will be able to develop satisfactory systems to deal with the legislation. Those who need to use or conduct directed surveillance or CHIS on a regular basis will require more detailed specialised training’ (Office of Surveillance Commissioners).

Directed Surveillance

The use of directed surveillance or a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be considered to be a tool of last resort, to be used only when all other less intrusive means have been used or considered.

The Council will conduct its directed surveillance operations in strict compliance with the DPA principles and limit them to the exceptions permitted by the HRA and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The Senior Responsible Officer (SRO) (Appendix 4) will be able to give advice and guidance on this legislation. The SRO will appoint a RIPA Coordinating Officer (RCO). The RCO will be responsible for the maintenance of a central register that will be available for inspection by the Office of the Surveillance Commissioners (OSC). The format of the central register is set out in Appendix 6.

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted. Best practice for compliance with evidential rules relating to photographs and video/CCTV footage is contained in Appendix 7. Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used.

The general usage of the council’s CCTV system is not affected by this policy. However, if cameras are specifically targeted for the purpose of directed surveillance, a RIPA authorisation must be obtained.

Wherever knowledge of confidential information is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Chief Executive, who is the Head of Paid Service (or in his absence whoever deputises for him).

Directed surveillance that is carried out in relation to a legal consultation on certain premises will be treated as intrusive surveillance, regardless of whether legal privilege applies or not. These premises include prisons, police stations, courts, tribunals and the premises of a professional legal advisor. Local Authorities are not able to use intrusive surveillance. Operations will only be authorised when there is sufficient documented evidence that the alleged crime or disorder exists and when directed surveillance is considered to be a necessary and proportionate step to take in order to secure further evidence.

Low level surveillance, such as ‘drive-bys’ or everyday activity observed by officers in the course of their normal duties in public places, does not need RIPA authority. If surveillance activity is
conducted in immediate response to an unforeseen activity, RIPA authorisation is not required. However, if repeated visits are made for a specific purpose, authorisation may be required. In cases of doubt, legal advice should be taken.

When vehicles are being used for directed surveillance purposes, drivers must at all times comply with relevant traffic legislation.

**Necessary**

A person granting an authorisation for directed surveillance must consider *why* it is necessary to use covert surveillance in the investigation *and* believe that the activities to be authorised are necessary on one or more statutory grounds.

**Proportionate**

The authoriser must also believe the proposed activities are proportionate to what is being sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

**Crime Threshold**

The Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012 imposes a ‘Crime Threshold’ whereby only crimes which are either punishable by a maximum term of at least 6 months’ imprisonment (whether on summary conviction or indictment) or are related to the underage sale of alcohol or tobacco can be investigated under RIPA.

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold came into effect on 1 November 2012.

A Local Authority *cannot* authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
Thus LBBD will continue to authorise use of directed surveillance in more serious cases as long as
the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a
Magistrate has been granted.

LBBD will also continue to authorise the use of directed surveillance for the purpose of preventing or
detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the
necessity and proportionality test is met and prior approval from a Magistrate has been granted.

A local authority may not authorise the use of directed surveillance under RIPA to investigate
disorder that does not involve criminal offences

An Authorising Officer’s Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when
considering applications for directed surveillance.

Covert Human Intelligence Sources

A person who reports suspicion of an offence is not a Covert Human Intelligence Source (CHIS),
nor do they become a CHIS if they are asked if they can provide additional information, e.g. details
of the suspect’s vehicle or the time that they leave for work. It is only if they establish or maintain a
personal covert relationship with another person for the purpose of covertly obtaining or disclosing
information that they become a CHIS.

The Council does not at present utilise CHIS. Any consideration of such use can only be
considered with prior discussion with the Chief Finance Officer and/or Head of Legal.

For some test purchases it will be necessary to use a CHIS who is, or appears to be, under the age
of 16 (a juvenile). Written parental consent for the use of a juvenile CHIS must be obtained prior to
authorisation, and the duration of such an authorisation is 1 month instead of the usual 12 months.
The Authorising Officer must be the Chief Executive or Deputy. NOTE: A juvenile CHIS may not be
used to obtain information about their parent or guardian.

Officers considering the use of a CHIS under the age of 18, and those authorising such activity must
be aware of the additional safeguards identified in The Regulation of Investigatory Powers

A vulnerable individual should only be authorised to act as a CHIS in the most exceptional
circumstances. A vulnerable individual is a person who is or may be in need of community care
services by reason of mental or other disability, age or illness, and who may not be able to take care
of themself. The Authorising Officer in such cases must be the Chief Executive, who is the Head of
Paid Service, or in their absence whoever deputises for them.

Any deployment of a CHIS should take into account the safety and welfare of that CHIS. Before
authorising the use or conduct of a CHIS, the authorising officer should ensure that an appropriate
bespoke risk assessment is carried out to determine the risk to the CHIS of any assignment and the
likely consequences should the role of the CHIS become known. This risk assessment must be
specific to the case in question. The ongoing security and welfare of the CHIS, after the cancellation
of the authorisation, should also be considered at the outset.

A CHIS handler is responsible for bringing to the attention of a CHIS controller any concerns about
the personal circumstances of the CHIS, insofar as they might affect the validity of the risk
assessment, the conduct of the CHIS, and the safety and welfare of the CHIS.
The process for applications and authorisations have similarities to those for directed surveillance, but there are also significant differences, namely that the following arrangements must be in place at all times in relation to the use of a CHIS:

1. There will be an appropriate officer of the Council who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and

2. There will be a second appropriate officer of the use made of the CHIS, and who will have responsibility for maintaining a record of this use. These records must also include information prescribed by the Regulation of Investigatory Powers (Source Records) Regulations 2000. Any records that disclose the identity of the CHIS must not be available to anyone who does not have a need to access these records.

The Authorisation Process

The processes for applications and authorisations for directed surveillance and CHIS are similar, but note the differences set out in the CHIS section above. Directed Surveillance & CHIS applications are made using forms in Appendix 5.

The authorisation process involves the following steps:

**Investigation Officer**

1. The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment.

2. A risk assessment will be conducted by the Investigation Officer within 7 days of the proposed start date. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns and insurance issues. Particular care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance.

3. The Investigation Officer will submit the application form to an authorising officer (see Appendix 4) for approval.

4. All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

**Authorising Officer (AO)**

5. The AO will obtain a unique reference number (URN) from the central register before authorising an application.

6. The AO considers the application and if it is considered complete the application is signed off. An Authorising Officer’s Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when considering applications for directed surveillance.

7. If there are any deficiencies in the application further information may be sought from the Investigation Officer, prior to sign off.

8. Once final approval has been received the Investigation Officer will retain a copy and will create an appropriate diary method to ensure that any additional documents are submitted in good time.
Application to Magistrates Court
9. The countersigned application form will form the basis of the application to the Magistrates Court (see further below)

Authorised Activity
10. Authorisation takes effect from the date and time of the approval from the Magistrates Court.
11. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the DVLA.
12. Consideration should be given to notifying the relevant police force intelligence units of the operation.
13. Before directed surveillance activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point.
14. Evidential notes should be made by all officers engaged in the operation. These documents will be kept in accordance with the appropriate retention guidelines.
15. Where a contractor or external agency is employed to undertake any investigation on behalf of the Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

Conclusion of Activities
16. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form (Appendix 5).
17. Originals of the complete application, renewal & cancellation forms will be retained with the central register.

Magistrate Authorisation
Under sections 37 and 38 of the Protection of Freedoms Act 2012 a local authority who wishes to authorise the use of directed surveillance, acquisition of Communications Data (CD) and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above. The current process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will therefore remain the same.

The appropriate officer from LBBBD will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. For CD requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The
necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

The original RIPA authorisation should be shown to the JP but also be retained by LBBD so that it is available for inspection by the Commissioners’ officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may also wish to take a copy.

Importantly, the appropriate officer will also need to provide the JP with a partially completed judicial application form.

Although the officer is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

The order section of the form will be completed by the JP and will be the official record of the JP’s decision. The officer from LBBD will need to obtain judicial approval for all initial RIPA authorisations and renewals and will need to retain a copy of the judicial application form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

The authorisation will take effect from the date and time of the JP granting approval and LBBD may proceed to use the techniques approved in that case.

It will be important for each officer seeking authorisation to establish contact with HMCTS administration at the magistrates’ court. HMCTS administration will be the first point of contact for the officer when seeking a JP approval. LBBD will need to inform HMCTS administration as soon as possible to request a hearing for this stage of the authorisation.

On the rare occasions where out of hours access to a JP is required then it will be for the officer to make local arrangements with the relevant HMCTS legal staff. In these cases we will need to provide two partially completed judicial application forms so that one can be retained by the JP. They should provide the court with a copy of the signed judicial application form the next working day.

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority’s responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

The hearing is a ‘legal proceeding’ and therefore our officers will be sworn in and present evidence or provide information as required by the JP.

The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application form. He/she may have questions to clarify points or require additional reassurance on particular matters.

The attending officer will need to be able to answer the JP’s questions on the policy and practice of conducting covert operations and the detail of the case itself. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and
supporting papers that the authorising officer has considered and which are provided to the JP to make the case.

It is not LBBD’s policy that legally trained personnel are required to make the case to the JP. The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

If more information is required to determine whether the authorisation has met the tests then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

The JP will record his/her decision on the order section of the judicial application form. HMCTS administration will retain a copy of the local authority RIPA authorisation and the judicial application form. This information will be retained securely. Magistrates’ courts are not public authorities for the purposes of the Freedom of Information Act 2000.

LBBD will need to provide a copy of the order to the communications SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested until the JP has signed the order approving the grant.

**Authorisation periods**

The authorisation will take effect from the date and time of the JP granting approval and LBBD may proceed to use the techniques approved in that case.

A written authorisation (unless renewed or cancelled) will cease to have effect after 3 months. Urgent oral or written authorisations, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Renewals should not normally be granted more than seven days before the original expiry date. If the circumstances described in the application alter, the applicant must submit a review document before activity continues.

As soon as the operation has obtained the information needed to prove, or disprove, the allegation, the applicant must submit a cancellation document and the authorised activity must cease.

CHIS authorisations will (unless renewed or cancelled) cease to have effect 12 months from the day on which authorisation took effect, except in the case of juvenile CHIS which will cease to have effect after 1 month. Urgent oral authorisations or authorisations will unless renewed, cease to have effect after 72 hours.

**Urgency**

The law has been changed so that urgent cases can no longer be authorised orally. Approval for directed surveillance in an emergency must now be obtained in written form. Oral approvals are no longer permitted. In cases where emergency approval is required an Authorising Officer (AO) must be visited by the applicant with two completed RIPA application forms. The AO will then assess the proportionality, necessity and legality of the application. If the application is approved then the applicant must then contact the out-of-hours HMCTS representative to seek approval from a Magistrate. The applicant must then take two signed RIPA application forms and the judicial approval form to the Magistrate for the hearing to take place.
As with a standard application the test of necessity, proportionality and the crime threshold must be satisfied. A case is not normally to be regarded as urgent unless the delay would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation. Examples of situations where emergency authorisation may be sought would be where there is intelligence to suggest that there is a substantial risk that evidence may be lost, a person suspected of a crime is likely to abscond, further offences are likely to take place and/or assets are being dissipated in a criminal investigation and money laundering offences may be occurring. An authorisation is not considered urgent if the need for authorisation has been neglected or the urgency is due to the authorising officer or applicant’s own doing.

**Telecommunications Data - NAFN**

The RIPA (Communications Data) Order 2003 allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does NOT allow Local Authorities to intercept record or otherwise monitor communications data.

Applications to use this legalisation must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-fraud Network) for this purpose.

Officers may make the application by accessing the NAFN website. The application will first be vetted by NAFN for consistency, before being forwarded by NAFN to the Council’s Designated Persons for the purposes of approving the online application. The Council will ensure that Designated Persons receive appropriate training when becoming a Designated Person.

The Council’s Designated Persons are presently the relevant Head of Service, and the Head of Audit. NAFN will inform the Designated Person once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Person will then access the restricted area of the NAFN website using a special code, in order to review and approve the application. When approving the application, the Designated Person must be satisfied that the acquiring of the information is necessary and proportionate. Approvals are documented by the Designated Person completing the online document and resubmitting it by following the steps outlined on the site by NAFN. This online documentation is retained by NAFN who are inspected and audited by the Interception of Communications Commissioner Office.

When submitting an online application, the officer must also inform the relevant Designated Person, in order that they are aware that the NAFN application is pending.

**Handling of material and use of material as evidence**

Material obtained from properly authorised directed surveillance or a CHIS may be used in other investigations. Arrangements in place for the handling, storage and destruction of material obtained through the use of directed surveillance, a CHIS or the obtaining or disclosure of communications data must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.
Training

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data along with Authorising Officers, the Senior Responsible Officer and the RIPA Coordinating Officer must be suitably qualified or trained.

The Senior Responsible Officer in conjunction with the RIPA Coordinating Officer is responsible for arranging suitable training for those conducting surveillance activity or using a CHIS.

All training will take place at reasonable intervals as determined by the Senior Responsible Officer, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

Surveillance Equipment

All mobile surveillance equipment should be securely held and suitability for use discussed with the Security & Investigations or Corporate Anti-Fraud Teams.

RIPA Record Quality Reviews

To ensure directed surveillance authorisations are being conducted in accordance with Council policy, a system of internal quality assurance has been put in place. At quarterly periods throughout the year, authorised application forms will be passed to the Chief Executive for review. PAASC will receive quarterly summaries on the Council’s use of RIPA.

The Inspection Process

The Office of Surveillance Commissioners (OSC) will make periodic inspections during which the inspector will interview a sample of key personnel, examine RIPA and CHIS applications and authorisations, the central register and policy documents. The inspector will also make an evaluation of processes and procedures.

Resources

Links to the latest Codes of Practice can be found on the Council’s Intranet site:

Further information can also be found on the Office of Surveillance Commissioners & Home Office websites:
http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

Relevant Acts:
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

david.greenfield@lbbd.gov.uk
GLOSSARY OF TERMS
(For full definitions, refer to the Act)

Central Register
The primary record of RIPA & CHIS applications, reviews, renewals, and cancellations and where original documents are stored.

Collateral intrusion
The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.

Communications Data
Information on the communication’s origin, destination, route, time, date, size, duration, or type of underlying service but not the content.

Confidential information
This covers confidential journalistic material, matters subject to legal privilege, and information relating to a person (living or dead) relating to their physical or mental health; spiritual counselling or which has been acquired or created in the course of a trade/profession/occupation or for the purposes of any paid/unpaid office.

Covert Human Intelligence Source
A person who establishes or maintains a personal or other relationship for the covert purpose of using such a relationship to obtain information or to provide access to any information to another person or covertly discloses information.

Covert relationship
A relationship in which one side is unaware of the purpose for which the relationship is being conducted by the other.

Directed Surveillance
Surveillance carried out in relation to a specific operation which is likely to result in obtaining private information about a person in a way that they are unaware that it is happening.

Intrusive Surveillance
Surveillance which takes place on any residential premises or in any private vehicle. A Local Authority cannot use intrusive surveillance.

Legal Consultation
A consultation between a professional legal adviser and his client or any person representing his client, or a consultation between a professional legal adviser or his client or representative and a medical practitioner made in relation to current or future legal proceedings.

Residential premises
Any premises occupied by any person as residential or living accommodation,
excluding common areas to such premises, e.g. stairwells and communal entrance halls.

**RIPA Co-Ordinating Officer (RCO)**
The RCO has the day to day responsibility to maintain a central and up-to-date record of all authorisations (Central Register) and arrange appropriate training.

**Senior Responsible Officer (SRO)**
The SRO is responsible for the integrity of the processes in order for the Council to ensure compliance when using Directed Surveillance or CHIS.

**Service data**
Data held by a communications service provider relating to a customer’s use of their service, including dates of provision of service; records of activity such as calls made, recorded delivery records and top-ups for pre-paid mobile phones.

**Surveillance device**
Anything designed or adapted for surveillance purposes.
The Human Rights Act 1998

Articles of the Human Rights Act relevant to RIPA:
- Article 6 – Right to a Fair Trial
- Article 8 – Right to Privacy

If it is proposed that directed surveillance evidence is to be used in a prosecution, or other form of sanction, the subject of the surveillance should be informed during an interview under caution.
The eight principles of the Act relating to the acquisition of personal data need to be observed when using RIPA. To ensure compliance, the information must:

- Be fairly and lawfully obtained and processed
- Be processed for specified purposes only
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than is necessary
- Be processed in accordance with an individuals rights
- Be secure
- Not be transferred to non European Economic Area countries without adequate protection.
Key RIPA Officers

Authorisation of RIPA applications where there is a likelihood of obtaining Confidential Information can only be given by the Chief Executive or deputy.

Only the Chief Executive, as Head of Paid Service or their deputy, can authorise the use of a vulnerable person or a juvenile to be used as a Covert Human Intelligence Source.

The Senior Responsible Officer & Co-ordinating Officer for RIPA and those officers authorised to sign applications, reviews, renewals and cancellations of Directed Covert Surveillance of Covert Human Intelligence Sources can be found at: http://lbld/resources/authorising-officers.htm
Appendix 5

RIPA Forms

Can be accessed here:

A central register will be maintained by the RIPA Co-ordinating Officer. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations.

Each operation will be given a unique reference number (URN) from which the year of the operation may be readily identified.

The register will also contain the following information:

- The name of the applicant
- The name of the subject of the surveillance or CHIS activity (for internal enquiries a pseudonym may be used)
- The date and time that the activity was authorised
- The date and time of any reviews that are to be conducted
- The date and time of any renewals of authorisations
- The date and time of the cancellations of any authorisations

Kept in conjunction with the register will be details of the training and updates delivered to authorising officers, a list of authorising officers, a copy of the RIPA policy and copies of all relevant legislation.

The original of all documents will also be held with the register, which will be available for inspection by the Office of the Surveillance Commissioners.

The register will form the basis of statistical returns of RIPA usage by the Council which are periodically compiled.
Appendix 7

Best practice regarding photographic and video evidence

Photographic or video evidence can be used to support the verbal evidence of what the officer conducting surveillance actually saw. There will also be occasions when video footage may be obtained without an officer being present at the scene. However it is obtained, it must be properly documented and retained in order to ensure evidential continuity. All such material will be disclosable in the event that a prosecution ensues.

Considerations should be given as to how the evidence will eventually be produced. This may require photographs to be developed by an outside laboratory. Arrangements should be made in advance to ensure continuity of evidence at all stages of its production. A new film, tape or memory card should be used for each operation.

If video footage is to be used, start it with a verbal introduction to include day, date, time and place and names of officers present. Try to include footage of the location, e.g. street name or other landmark so as to place the subject of the surveillance.

A record should be maintained to include the following points:
- Details of the equipment used
- Name of the officer who inserted the film, tape or memory card into the camera
- Details of anyone else to whom the camera may have been passed
- Name of officer removing film, tape or memory card
- Statement to cover the collection, storage and movement of the film, tape or memory card
- Statement from the person who developed or created the material to be used as evidence

As soon as possible the original recording should be copied and the master retained securely as an exhibit. If the master is a tape, the record protect tab should be removed once the tape has been copied. Do not edit anything from the master. If using tapes, only copy on a machine that is known to be working properly. Failure to do so may result in damage to the master.

Stills may be taken from video. They are a useful addition to the video evidence.
## Authorising Officer's Aide-Memoire

### Has the applicant satisfactorily demonstrated proportionality?

<table>
<thead>
<tr>
<th>Has the applicant satisfactorily demonstrated proportionality?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Court will ask itself should (not could) we have decided this was proportionate.</td>
</tr>
<tr>
<td>Is there a less intrusive means of obtaining the <strong>same</strong> information?</td>
</tr>
<tr>
<td>What is the risk – to the authority (loss), to the community of allowing the offence to go un-investigated? What is the potential risk to the subject?</td>
</tr>
<tr>
<td>What is the least intrusive way of conducting the surveillance?</td>
</tr>
<tr>
<td>Has the applicant asked for too much? Can it safely be limited?</td>
</tr>
<tr>
<td>Remember – Don’t use a sledge-hammer to crack a nut!</td>
</tr>
<tr>
<td><strong>YOUR COMMENTS</strong></td>
</tr>
</tbody>
</table>

### Has the applicant satisfactorily demonstrated necessity?

<table>
<thead>
<tr>
<th>Has the applicant satisfactorily demonstrated necessity?</th>
</tr>
</thead>
<tbody>
<tr>
<td>What crime is alleged to be being committed? Has the applicant described it in full?</td>
</tr>
<tr>
<td>Is surveillance necessary for what we are seeking to achieve?</td>
</tr>
<tr>
<td>Does the activity need to be covert, or could the objectives be achieved overtly?</td>
</tr>
<tr>
<td><strong>YOUR COMMENTS</strong></td>
</tr>
</tbody>
</table>

### What evidence does applicant expect to gather?

<table>
<thead>
<tr>
<th>What evidence does applicant expect to gather?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has applicant described (a) what evidence he/she hopes to gain, and (b) the value of that evidence in relation to <strong>THIS</strong> enquiry?</td>
</tr>
<tr>
<td><strong>YOUR COMMENTS</strong></td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is there any likelihood of obtaining confidential information during this operation? If “Yes” operation must be authorized by the Chief Executive.</td>
</tr>
<tr>
<td>Have any necessary risk assessments been conducted before requesting authorization? Details what assessment (if any) was needed in this particular cases. In the case of a CHIS authorization an appropriate bespoke risk assessment must be completed.</td>
</tr>
<tr>
<td>When applying for CHIS authorization, have officers been identified to:</td>
</tr>
<tr>
<td>a) have day to day responsibility for the CHIS (a handler)</td>
</tr>
<tr>
<td>b) have general oversight of the use of the CHIS (a controller)</td>
</tr>
<tr>
<td>c) be responsible for retaining relevant CHIS records, including true identity, and the use made of the CHIS.</td>
</tr>
<tr>
<td>Have all conditions necessary for authorization been met to your satisfaction? GIVE DETAILS</td>
</tr>
<tr>
<td>Do you consider that it is necessary to place limits on the operation? IF YES, GIVE DETAILS (eg no. of officers, time, date etc) and REASONS</td>
</tr>
</tbody>
</table>

Remember to diarise any review dates and any subsequent action necessary by you and/or applicant. Return copy of completed application to applicant and submit original to Audit & Anti-Fraud Group. Retain copy.
Internal Audit

The Bribery Act Policy
March 2014

Date Last Reviewed: March 2014
Approved by: PAASC
Date Approved: 19 March 2014
Version Number: 1.1
Review Date: March 2014
Document Owner: Group Manager – Internal Audit & Anti-Fraud
Post Holder: David Greenfield
The Council’s commitment to the Bribery Act Policy

The council will not condone acts of bribery in any form whether it is in the form of money, gifts or a favour, offered or given to a person in a position of trust to influence that person's views or conduct.

What are the aims and requirements of the legislation?

Where Bribery is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Bribery Act policy. It will be investigated fully and the London Borough of Barking and Dagenham will prosecute all offenders where appropriate including, Members, employees, contractors and external partners.

Who is governed by this Policy?

The Bribery Act policy covers everyone working for us, or on our behalf, including all permanent employees, temporary agency staff, contractors, members of the council (including independent members), volunteers and consultants.

Executive Summary

The Bribery Act Policy sets out the Council’s commitment to ensuring compliance with the requirements of the Bribery Act.
<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Bribery Act</td>
<td>4</td>
</tr>
<tr>
<td>What are adequate procedures?</td>
<td>5</td>
</tr>
<tr>
<td>What are the six principles</td>
<td>5</td>
</tr>
<tr>
<td>Golden Rules</td>
<td>6</td>
</tr>
<tr>
<td>Employee Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>Reporting a concern.</td>
<td>7</td>
</tr>
<tr>
<td>Further support, tools and guidance</td>
<td>8</td>
</tr>
</tbody>
</table>
The Bribery Act Policy

The Bribery Act 2010 makes it an offence to offer, promise or give a bribe (section 1). It also makes it an offence to ask for, 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 getting or keeping business or an advantage in carrying out business. There is also a new corporate offence under section 7 that we will commit if we fail to prevent bribery that is intended to get or keep business or an advantage in business for our organisation. We are no longer able to claim we were not aware of bribery and may be responsible as an organisation, but we will have a defence if we can show we had adequate procedures in place designed to prevent bribery by our staff or by people associated with our organisation. (See ‘What are adequate procedures?’ below for an explanation).

Bribery Act policy statement

Bribery is a criminal offence. We do not offer bribes to anyone for any purpose, and we do not accept bribes.

Using another person or organisation to give bribes to others is a criminal offence. We do not offer bribes indirectly or otherwise engage in bribery.

We are committed to preventing and detecting bribery. We take a zero-tolerance stance towards bribery and aim to ensure this Bribery Act policy is observed throughout the Council.

We will deal with allegations of bribery involving employees under our disciplinary procedure as “gross misconduct”. It is normal practice to dismiss employees without notice in cases where gross misconduct is considered to have taken place.

The aim of this policy

This policy provides a framework to allow those affected by it to understand and put into place arrangements to prevent bribery. It will work with related policies and other documents to identify and report when this policy is breached.

The policy aims to ensure that everyone:

- acts honestly at all times and protects the council’s resources they are responsible for; and
- keeps to the spirit, as well as the letter, of the laws and regulations that cover our work

Scope of this policy

This policy applies to all of our activities. All levels of the council are responsible for controlling the risk of bribery. We will aim to encourage schools, suppliers and other organisations we work with to adopt policies that are consistent with the principles set out in this policy.
The Bribery Act policy applies to and covers everyone working for us, or on our behalf, including all permanent employees, temporary agency staff, contractors, members of the council (including independent members), volunteers and consultants.

This means that everyone at all levels of the council has a responsibility to control the risk of bribery occurring.

**What are “adequate procedures”**

In order for this council to show that we take the Bribery Act seriously, we need to show we have adequate procedures in place designed to prevent bribery. Whether our procedures are adequate will be for the courts to decide. Our procedures need to be in proportion to the level of risk of bribery in our organisation. Individual organisations can refer to six principles to decide whether their procedures are in proportion to the level of risk. These principles are not prescriptive. These principles are intended to be flexible, allowing for the different circumstances of organisations. Small organisations will, for example, face different challenges to those faced by large multi-national organisations. The detail of how an organisation applies these principles will be different depending on the organisation, but the outcome should always be effective Bribery Act procedures.

**What are the six principles?**

1. **Proportionate procedures**

   An organisation’s procedures to prevent bribery by the people associated with it should be in proportion to the risks of bribery it faces and to the nature, scale and complexity of the organisation’s activities. They should include interrogation of data for the purpose of discovering evidence and ensuring personal data is protected. The procedures should also be clear, practical, accessible and effectively put into place and enforced.

2. **Commitment at the top levels of our organisation**

   Our Cabinet and Corporate Management Team are committed to preventing bribery by the people associated with us. They help create a culture in our organisation where bribery is never acceptable.

3. **Risk assessment**

   We regularly assess how and to what extent we will be exposed to potential risks of bribery. We keep a record of the assessments, which include financial risks and also other risks such as damage to our reputation.

4. **Due diligence**
We apply due diligence procedures in relation to people who provide services for or on behalf of our organisation to reduce the risks of bribery. This would include carrying out checks on such organisations or companies and ensuring that they have similar anti bribery processes in place.

5. Communication (including training)

We aim to make sure that our policies and procedures to prevent bribery are understood throughout our organisation. We do this through communication inside and outside of our organisation, including training.

6. Monitoring and review

We monitor and review the procedures designed to prevent bribery and make improvements where they are needed. The Monitoring Officer and Group Manager (Internal Audit & Anti-Fraud) will oversee this.

We are committed to putting these principles into place.

We can also be fined, and if we are found guilty of an offence under section 7, can be fined an unlimited amount.

Facilitation payments

Facilitation payments are unofficial payments made to public officials in order to get them to take certain actions or take actions more quickly. Facilitation payments are illegal under the Bribery Act, and we will not tolerate them.

Gifts and hospitality

This policy is in line with our gifts and hospitality policy (this can be read at http://lbhd/hr/ongoing-process-of-managing-people/gifts-and-hospitality.htm). The gifts and hospitality policy makes it clear that if members of the council or staff are offered gifts in their council role, they should not accept anything with more than a token value (examples of things that are of token value include bottles of wine, boxes of chocolates, flowers, pens, calendars and diaries).

Public contracts and failure to prevent bribery

Under the Public Contracts Regulations 2006, a company is automatically and permanently barred from competing for public contracts if it has been convicted of a corruption offence. There are no plans to amend the 2006 regulations to include the crime of failing to prevent bribery. Organisations that are convicted of failing to prevent bribery are not automatically barred from competing for public contracts. However, we can exclude organisations convicted of this offence from competing for contracts with us. We will include standard clauses in our commercial contracts forbidding bribery and corruption.

Golden Rules
We will not tolerate bribery

Those covered by the policy must not:

• give, promise to give, or offer a payment, a gift or hospitality with the expectation or hope that they will receive a business advantage, or to reward a business advantage that they have already been given
• give, promise to give, or offer a payment, a gift or hospitality to a government official or representative to speed up a routine procedure
• accept a payment from another person or organisation if they know or suspect that it is offered with the expectation that it will give them a business advantage
• accept a gift or hospitality from another person or organisation if they know or suspect that it is offered or provided with an expectation that they will provide a business advantage in return
• take action against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy; or
• take part in activities that break this policy

Our commitment to action

We are committed to:

• setting out a clear Bribery Act policy and keeping it up to date
• making all employees aware of their responsibility to keep to this policy at all times;
• training all employees so that they can recognise and avoid the use of bribery
• encouraging our employees to be aware and to report any suspicions of bribery
• providing our employees with suitable ways of telling us about their suspicions and making sure we treat sensitive information appropriately
• investigating alleged bribery and helping the police and other authorities in any prosecution that happens because of the alleged bribery
• taking firm action against any people involved in bribery
• providing information to all employees to help them tell us when someone has broken or is suspected of breaking this policy; and
• including appropriate clauses in contracts to prevent bribery

Employee Responsibilities

All the people who work for us or are under our control are responsible for preventing, detecting and reporting bribery and other forms of corruption. All staff must avoid activities that break this policy and must:

• make sure they read, understand and keep to this policy; and
• tell us as soon as possible if they believe or suspect that someone has broken this policy, or may break this policy in the future
Anyone covered by the policy found to break it will face disciplinary action, could be dismissed for gross misconduct and/or may also face civil and criminal prosecution.

**Reporting a concern**

We all have a responsibility to help detect, prevent and report instances of bribery. If anyone has a concern about suspected bribery or corruption, they should speak up – their information and support will help. The sooner they act, the sooner the situation can be dealt with.

There are several ways of informing about any concerns. For example, talking to a line manager first, or the contacts listed in the Whistleblowing Policy if this is more appropriate.

Those reporting concerns do not have to give us their name. Upon receiving a report about an incident of bribery, corruption or wrong doing, action will be taken as soon as possible to assess the situation. There are clear procedures for investigating fraud and misconduct and these will be followed in any investigation of this kind. This will be easier and quicker if those reporting concerns decide to give their name. In some circumstances, we will have to consider reporting the matter to the Serious Fraud Office.

Staff that refuse to accept or offer a bribe, or those who report concerns or wrongdoing can understandably be worried about what might happen as a result. To encourage openness and anyone who reports a genuine concern in the public interest will be supported under this policy, even if they turn out to be mistaken. There is a commitment to making sure nobody is treated badly because they have refused to take part in bribery or corruption, or because they have reported a concern.

If there are any questions about these procedures, the Monitoring Officer can be contacted, on 0208 227 2114 or the Group Manager (Internal Audit & Anti-Fraud), on 0208 227 2896.

**Other relevant policies**

- Fraud Prosecution Policy
- Money Laundering Policy
- Whistleblowing Policy
- Employee Code of Conduct
- Rules in respect of Gifts and Hospitality
- Disciplinary Procedure and Disciplinary Rules
The latest version of the Bribery Act Policy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

Anti Fraud Information

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

david.greenfield@lbbd.gov.uk