AUDIT AND STANDARDS COMMITTEE

27 June 2018

Title: Review of Key Counter Fraud Policies & Strategy	
Report of: Corporate Investigation Manager (Assurance & Counter Fraud)	
Open	**For Discussion**
Wards Affected: None	**Key Decision:** No
Report Author: Kevin Key	**Contact Details:** Tel: 020 8227 2850 E-mail: kevin.key@lbbd.gov.uk
Accountable Director: Claire Symonds, Chief Operating Officer	
Summary: To ensure proper arrangements to administer the Council's financial affairs, the Council has adopted key policies and a strategy to combat fraud and irregularity. These polices were approved by Cabinet and to further strengthen their importance, as part of robust governance, recommended for review annually. Accordingly, they are presented to the relevant assurance groups to note and comment upon.	
Recommendation(s): Members are asked to note the Council's updated Counter Fraud Policies and Strategy	
Reason(s) The Council's vision and priorities are underpinned by the theme 'a well-run organisation' as set out in the corporate plan. The work of audit & counter fraud supports this theme to ensure the Council meets both its legal responsibilities and the needs of the community.	

1. Introduction

1.1. The Assurance & Counter Fraud Group maintains a suite of counter fraud policies and a strategy to support the Council's strong stance against fraud, thus maintaining proper arrangements for the Council's finances.

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

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

1.4. They apply to the Council, and as part of 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/Strategy

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

Appendix	Document	Brief Description
A	Counter Fraud Strategy	Sets out the Council's commitment to reducing opportunities for fraud and corruption across all council services and taking the strongest possible action against those who seek to defraud the Council.
B	Counter Fraud Policy including Fraud Response Plan	Sets out how the Council responds to fraud and the changing risk profile of fraud and Includes guidance on what to do if an employee suspects fraud.
C	Prosecution Policy	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
D	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.
E	Whistleblowing Policy	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.
F	Regulation of Investigatory Powers Policy	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 & Data Protection Legislation
G	Bribery Act Policy	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
H	Proceeds Of Crime Act Policy & Procedures	Sets out how the Council will use the Proceeds of Crime Act 2002 as a primary tool in its efforts to disrupt individual and organised crime and ensure those convicted of an offence are stripped of the benefits of their criminal lifestyle.

3. Summary of Changes

3.1 The following changes have been made:

- Updates to reflect officer designation changes where appropriate
- Updates to Council's Authorised Applicants for Regulation of Investigatory Powers (RIPA) Act investigations
- Minor spelling and grammatical changes throughout
- Addition of information in relation to impending General Data Protection Regulation (GDPR) legislation

Otherwise these documents have been reviewed and deemed fit for purpose.

4. Awareness Raising

4.1 Counter Fraud Policies and the Strategy will be made available on the Intranet. Awareness raising, training and briefings will be targeted at specific groups of staff - identified from an ongoing project to refresh of the Council's fraud risk assessment - through channels such as face to face, e-bulletins/e-learning and posters on staff notice boards.

5. Financial Implications

Implications completed by: Katherine Heffernan, Group Manager - Finance

5.1 The maintenance and regular review of appropriate anti fraud and related policies is a key part of the Council's overall approach to robust control and strong financial management. The Council has an Audit and Assurance service which is fully funded and the application of the policies can be delivered from existing resources.

6. Legal Implications

Implications completed by: Dr Paul Feild, Senior Governance Solicitor

6.1 The Accounts and Audit (England) Regulations 2015 section require that: a relevant authority must ensure that it has a sound system of internal control which—facilitates the effective exercise of its functions and the achievement of its aims and objectives; ensures that the financial and operational management of the authority is effective; and includes effective arrangements for the management of risk.

6.2 Furthermore the Director of Finance has a statutory duty, under Section 151 of the Local Government Act 1972 and Section 73 of the Local Government Act 1985, to ensure that there are proper arrangements in place to administer the Council's financial affairs.

6.3 The Policies set out in this report address the need to counter fraud, money laundering, bribery and the proceeds of crime. The policies guide on the investigatory and prosecution process.

6.4 In formulating the policies it addresses the issue of corruption and bribery. Corruption is the abuse of entrusted power for private gain. The Bribery Act 2010 defines bribery as “the inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages whether monetary or otherwise”.

6.5 The Local Government Act 1972 provides the Council with the ability to investigate and prosecute offences committed against it. We will enhance our provision further by making best use of existing legislation, for example the Proceeds of Crime Act 2002, to ensure that funds are recovered, where possible by the Council.

7. The following people were consulted in the preparation of this report:

- Group Manager - Finance
- Senior Governance Solicitor

APPENDIX A

Assurance & Counter Fraud

Counter Fraud Strategy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	*Draft for approval*
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

COUNTER FRAUD STRATEGY

June 2018

Contents

Counter Fraud Objective 2

Resources & Skills 3

Responsibility 3

Liaison 4

"Taking Action" and Supporting Policies 5

Review & Assessment/Quality Assurance 7

Counter Fraud Objective

To create a culture and organisational framework - through a series of comprehensive and inter-related procedures and controls - which maximises the deterrence of fraud, minimises the incidence & impact of fraud against the Council, and ensures, through professional investigation, effective outcomes including sanctions and redress against those who defraud the Council.

The Strategy is based on the following principles:

Acknowledge responsibility The Council has acknowledged its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.
Identify risks The Council uses fraud risk identification to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the Council and its service users.
Develop a strategy This document sets out the Council approach to managing fraud risks and defining responsibilities for action.
Provide resources As set out in this document, the Council has appropriate resources to support the counter fraud strategy.
Take action The Council has in place a suite of policies to support the counter fraud strategy and take action to deter, prevent, detect and investigate fraud.

Links to Corporate Objectives
The vision for the Borough is **One borough; one community; London's growth opportunity**

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

- Encouraging civic pride
- Enabling social responsibility
- Growing the borough

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

Resources & Skills

The Assurance & Counter Fraud Group will investigate all issues of suspected fraud and irregularity and promote the counter fraud agenda of the Council through proactive and preventative activities.

Housing Investigators will investigate allegations concerning council housing with the aim of delivering housing units back to proper use, and preventing misuse of the council housing stock. Housing Investigators are appointed as “Authorised Officers”, and thus can exercise powers, under Section 4 of the Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014.

All investigators are professionally qualified and undertake appropriate continuous professional development.

The Assurance & Counter Fraud Group has access to a qualified Accredited Financial Investigator to enable the option of redress under the Proceeds of Crime Act (POCA). Any monies recovered will be used to further promote counter fraud across the council.

The authority for Assurance & Counter Fraud Group Investigators to investigate is enshrined in the Council’s Constitution; Financial Rules including the authority to have access to all records, and to all council premises.

Monies obtained under the POCA incentivisation scheme will be invested into counter fraud activities.

Responsibility

Assurance & Counter Fraud Group
The Assurance & Counter Fraud Group will champion the Council’s tough stance against fraud and promote a counter fraud culture across the council, its Members, staff, contractors, partner agencies and service users. Investigators will work to professional standards and in accordance with relevant codes of practice as well as applying the Council’s policies on equalities & diversity and customer care. Investigators will at all times maintain confidentiality, comply with the employee code of conduct and operate within the guidelines of all relevant legislation.

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.

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, Disclosure & Barring checks, and stringent vetting in relation to employment history and references. This expectation will form part of all contract terms and conditions.

Employees
It is recognised most staff are conscientious and hardworking and whose conduct is beyond reproach. 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.

Often, employees are the first to spot that something is wrong and putting the council and/or its residents at risk. In accordance with the Code of Conduct, employees should bring to the attention of the appropriate manager, any impropriety, fraud or breach of procedure. If they 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, they should report their concerns through the channels set out in the Council's Whistleblowing Policy.

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.

Members may become aware of potential fraud through their casework with constituents and their day to day duties as Councilors. Any such issues or concerns should be reported to the Assurance & Counter Fraud Group at the earliest opportunity.

Liaison

The Assurance & Counter Fraud Group will utilise all methods available to detect fraud. Arrangements are in place to actively participate in the 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 Visas & Immigration
- Pensions Service

In addition, we will work with colleagues in other Local Authorities and utilise counter fraud networks such as LBFIG, LAG and CIPFA Counter Fraud Centre.

Taking Action and Supporting Polices

Deterrence

The Council will publicise its counter fraud measures using appropriate means to promote the deterrent message, for example the effectiveness of controls including the governance framework, arrangements that are in place to detect fraud, the professionalism of those who investigate fraud, the Council's success in applying proportionate sanctions and the prompt, effective recovery of losses.

Prevention

The Assurance & Counter Fraud Group works with Internal Audit to support management in assessing compliance with the Council's policies and ensuring that adequate levels of internal check are included in operational procedures. The Assurance & Counter Fraud Group will advise on counter fraud measures in new systems and promote awareness on the importance of considering fraud risks as part of good governance arrangements. Awareness will be maintained on the changing risk profile of potential fraud and national developments to tackle new areas.

Detection

In addition to maintaining channels for the public and officers to report fraud, the Assurance & Counter Fraud Group will proactively use all legal and cost effective means to detect fraud, including working with other organisations and participating in national data matching schemes.

Investigation

All allegations of fraud will be professionally investigated in accordance with the Fraud Response Plan and in adherence to all relevant legislation. Outcomes from investigations will make recommendations for further actions as appropriate - to include disciplinary action, police action, civil recovery - as well as to make any

necessary changes to systems and procedures to ensure that similar frauds will not recur.

Recovery and Sanctions

Where the Council identifies fraud then it will seek to recover losses wherever appropriate and prosecute or apply other sanctions to perpetrators, such as those contained within the Prosecution Policy. Where fraud by employees is indicated, then action will be taken in accordance with the Council's disciplinary procedures. This may be in addition to any civil recovery action or sanctions.

Redress

Redress in the form of compensation or confiscation under proceeds of crime legislation will be sought wherever appropriate in accordance with the Prosecution Policy. Our aim is to ensure that those who seek to defraud the Council do not profit from their criminal activity.

Policies

All Counter Fraud work will be undertaken in accordance with relevant policies as follows:

Policy	Brief Description
Counter Fraud Policy including Fraud Response Plan	Sets out the Council's commitment to 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.
Prosecution Policy	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
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.
Whistleblowing Policy	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.
Regulation of Investigatory Powers Policy	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 & Data Protection Legislation
Bribery Act Policy	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
Proceeds of Crime Act 2002 Policy	Sets out the Council's approach to applying procedures under proceeds of crime legislation to instigate financial redress against those who defraud the Council

These policies will be reviewed at least annually

Review & Assessment/Quality Assurance

The strategy will be reviewed annually. The outcomes from counter fraud work will be periodically reported to Members of the Public Accounts & Audit Select Committee and outcomes assessed to evaluate success of the strategy.
Periodically, the Assurance & Counter Fraud Group procedures will be assessed against best practice as set out in CIPFA's "Managing the Risk of Fraud and Corruption".

APPENDIX B

Assurance & Counter Fraud

Counter Fraud Policy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	*Draft for Approval*
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

The Council's commitment to the Counter Fraud 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 perpetrated both internally and externally. The Council takes a tough stance against Fraud and considers this Policy and the associated strategy to be an integral part of our approach.

What are the aims and requirements of the Policy?

Where Fraud is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Counter Fraud Policy. 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 Counter Fraud Policy 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 Counter Fraud Policy makes clear the Council's commitment to reducing opportunities for fraud and taking the strongest possible action against those who seek to defraud the Council.
All references to fraud in this document include any other type of fraud related offence – fraud, theft, corruption, bribery. See definitions at the end of this document.

Contents

Title	Page No.
Counter Fraud Policy	1
The Counter fraud culture and deterrence	1
Prevention – Managing the risk of fraud	3
Detection & Investigation	6
Recovery, Sanction and Redress	7
Definitions	7
Further support, tools and guidance.	9
Appendix 1 Fraud response plan	10

Counter Fraud Policy

Counter Fraud 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 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.

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 the Authority recognises the responsibilities placed upon it by statute and will actively promote this Policy which is designed to:

- Promote standards of honest and fair conduct
- Encourage prevention of fraud
- Maintain strong systems of internal control
- Promote detection
- Take a tough stance against fraud and bring to justice all persons who commit acts of fraud against the Council
- Recover any losses incurred by the Council

The Counter Fraud Culture and Deterrence

The culture of the organisation is one of honesty, openness and opposition to fraud. 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. With this in mind, 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 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 activity. A pound lost through fraud is a pound that is stolen from Barking and Dagenham residents and reduces the amount available to spend on delivering services to residents.

An ongoing proactive programme of work will be undertaken 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 counter fraud awareness materials. Fraud awareness programmes will be targeted at specific groups of staff in the form of presentations, workshops and newsletters.

Additionally, this 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
- Counter Fraud Strategy

Prevention – Managing the Risk of Fraud

Fraud is 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 that include:

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

The Chief Operating 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. 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 (2015).

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) and maintain robust controls within their service areas to mitigate these. Some services will be predominantly at risk of attack from external sources, for example, Council tax and Housing.

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 controls

Managers must evaluate the adequacy of existing controls and establish what further controls or changes are required to reduce or eliminate the risk of fraud. In addition, managers should utilise internal audit reports, internal investigation findings, value for money review findings, external audit reports or findings from other external inspections to 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.

Advice on managing risk, evaluating possible conflicts of interest, or the development or evaluation of controls can be obtained from 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 & 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 Senior Manager in addition to reporting major system failures, remedial action plans and instances of non-compliance to the Audit & Standards Committee.

Contractors

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

Contractors and partners are also expected to have adequate recruitment procedures in place covering requirements under the Immigration and Nationality Act, disclosure & barring 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 hardworking and whose conduct is beyond reproach. However, where it becomes evident fraud has taken place, action will be taken in accordance with the Council's Disciplinary Rules. Fraud is a specific instance 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 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 1).

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 that enables detection to occur and the appropriate action to take place when there is evidence that fraud may be in progress.

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

Reporting cases in this way is essential to the Counter Fraud Policy and makes sure that:

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

The Counter Fraud Team is 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 Counter Fraud Team.

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 Operating Officer & Investment 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.

Recovery, 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. Where appropriate to do so, recovery of losses/compensation will be sought and confiscation of proceeds of crime pursued in accordance with relevant legislation.

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 or all of the above sanctions and redress will be made on a case by case basis, having regard to the Disciplinary Rules and Prosecution Policy.

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.

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.

Fraud is defined as the intention to make a gain for oneself or another or to cause loss to another/expose another to a risk of loss by dishonestly making a false representation, dishonestly failing to disclose to another person information which he/she is under a legal duty to disclose or occupies a position in which he is expected to safeguard or not to act against the financial interests of another person and dishonestly abuses that position.

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?

Corruption is defined as the abuse of a position of trust to gain an undue advantage for oneself or another.

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.

What is Bribery?

Bribery is defined as a financial or other advantage that is offered or requested with the intention of inducing or rewarding the improper performance of a relevant function or activity, or with the knowledge or belief that the acceptance of such an advantage would constitute the improper performance of such an activity.

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 Counter Fraud Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages.

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:

caft@lbbd.gov.uk

Appendix 1 Fraud Response Plan

The London Borough of Barking and Dagenham is committed to developing a culture of honesty and a tough stance against fraud.

The purpose of this document is to demonstrate and set out the procedures to be followed where theft, fraud or corruption is suspected or detected. It is part of the Council's overall Counter Fraud Policy. 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 Assurance & Counter Fraud Group. 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

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 Assurance & Counter Fraud Group will maintain a log of all reports, detail actions taken and conclusions reached and report periodically to Members of the Audit & Standards Committee.

The Assurance & Counter Fraud Group 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 Assurance & Counter Fraud Group immediately. Any delay could compromise subsequent investigations.

What should staff do if they suspect fraud?

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 Assurance & Counter Fraud Group Officers 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 Assurance & Counter Fraud Group Officers if this can be done without alerting suspicions; this should include any relevant e mails

You should not:

- Ignore the concerns or be afraid of raising them. You will not suffer recriminations from your employer because 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 Assurance & Counter Fraud Group Officers 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?

The Council encourages members of the public who suspect fraud to contact the Assurance & Counter Fraud Group in the first instance. Suspicions or identified instances of fraud or other wrongdoing against the Council can be reported via a confidential hotline number.

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

The Assurance & Counter Fraud Group operates independently of other Council services but will pool resources with other stakeholders such as Internal Audit to provide a joined-up approach to prevention, detection, investigation and prosecution of fraud within the council.

When allegations are received from staff or the public the Assurance & Counter Fraud Group Officers 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. Details of the investigation and outcomes will not be divulged due to privacy and data protection concerns.

If it appears that a criminal act has occurred or where there is sufficient evidence of fraud, 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 Assurance & Counter Fraud Group Officers will advise the appropriate service manager and/or 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 Assurance & Counter Fraud Group 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 Assurance & Counter Fraud Group Officers 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. All relevant legislation will be adhered to.

The outcomes of significant internal investigations will be reported to the Audit & Standards 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 Assurance & Counter Fraud Group Officers 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 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.

APPENDIX C

Assurance & Counter Fraud

The Fraud Prosecution Policy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	*draft*
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

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 tough stance 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 policy?

The aim of this prosecution policy is to deter fraud against the Council.

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 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 committed fraud against other local authorities or any other agency administering public funds.

Executive Summary

The London Borough of Barking & Dagenham is committed to the protection of public funds through its action against fraud.

In order to reinforce the deterrence message, where fraud and wrong doing is 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, in accordance with this policy.

All references to fraud in this document include any other type of fraud related offence – fraud, theft, corruption and bribery as defined in the Counter Fraud policy.

Contents

Title	Page No.
Fraud Prosecution Policy	1
Fraud Sanctions & Redress	2
Publicity	4
Further support, tools and guidance	4
Appendix 1	5

Fraud Prosecution Policy

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

Where fraud is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Counter Fraud 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, the Assurance & Counter Fraud Group 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.

Fraud Sanctions & Redress

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 with or without police involvement

Where it is decided that a criminal prosecution is to be pursued, the Counter Fraud Team will brief the Chief Operating Officer, Chief Executive, Director or other Officer's 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 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 Assurance & Counter Fraud Group following consultation with the Corporate Investigation Manager and Legal Services.

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

The Assurance & Counter Fraud Group 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 redress, 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 fail to recover any monies owed to the council, following advice from Legal Services, the Assurance & Council Fraud Group 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, confiscation orders under Proceeds of Crime legislation will also be considered utilising Accredited Financial Investigator resources.

Publicity

Assurance & Counter Fraud Group officers will seek to publicise successfully prosecuted cases, with the aim to deter others and thereby to prevent further frauds. The final decision to publicise will rest with the Council's Media & Public Relations Team.

Further Support, Tools & Guidance

The latest version of the Fraud Prosecution Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages

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:

caft@lbbd.gov.uk

Appendix 1

Tests the council will apply 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 administration including delay?

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

APPENDIX D

Assurance & Counter Fraud

Money Laundering Policy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	*draft*
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

The Council's commitment to the Money Laundering Policy

London Borough of Barking & Dagenham, "the Council" takes a tough stance to fraud perpetrated against it 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 policy?

The policy 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.

Contents

Title	Page No.
Money Laundering Policy	1
What is Money Laundering?	1
What is the legal definition?	1
What is the legislation?	1
How can suspicious activity be identified?	2
What are the areas at risk of Money Laundering?	2
Reporting of Money Laundering	3
Further support, tools, training and guidance.	3

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
- 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

Staff should report any suspicions to the Finance Director, Corporate Investigations Manager or Financial Investigator immediately as they arise.

Suspicions may be reported informally by telephone or email and the responsible officer will seek to establish the facts of the case, investigate the matter fully and determine whether a formal referral to the National Crime Agency (NCA) is appropriate.

Further Support, Tools, Training & Guidance

The latest version of the Money Laundering Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages

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:

caft@lbbd.gov.uk

APPENDIX E

Assurance & Counter Fraud

Whistleblowing Policy

June 2018

Date Last reviewed:	June 2017
Approved by:	PAASC
Date Approved:	Draft for approval
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Director of Finance

The councils 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, contractors, consultants, authorised volunteers or work experience. It also covers those working for suppliers/providing services under a contract with the Council where this or an equivalent whistleblowing policy is in force.

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.

Contents

What is whistleblowing? 3
Who is covered by this policy? 3
What types of action are covered by the policy? 3
What is not covered by the policy? 4
Protecting you 5
How to raise a concern 5
How we respond to your concerns 7
Untrue Allegations 7
Further Support, Tools & Guidance 7

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, contractors, consultants, authorised volunteers or work experience. It also covers those working for suppliers/providing services under a contract with the Council where this or an equivalent whistleblowing policy is in force.

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, 5th Floor Roycraft House, 15 Linton Road, Barking, IG11 8HE. Write "Private and Confidential" on your envelope.

  A complaint form and other information is available on line at:

https://www.lbbd.gov.uk/council/councillors-and-committees/councillors/complaints-about-councillors/how-to-complain-about-a-councillor/

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 Director.

Note whistle blowing concerns that relate to professionals who:

- Behaved in a way that has harmed a child, or may have harmed a child;
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Will need to be referred to the Local Authority Designated Officer (LADO) in Children Services: lado@lbbd.gov.uk who will determine if a specific child protection investigation is required.

Concerns that involve financial malpractice should always be raised with the Assurance & Counter Fraud Group Officers.

If you prefer, or you do not work for the Council, you can contact the Assurance & Counter Fraud Group direct in any of the following ways:

- By writing to the Assurance & Counter Fraud Group at:

  London Borough of Barking and Dagenham, 2nd Floor Town Hall, Town Hall Square, 1 Clockhouse Avenue, Barking, IG11 7LU.

  (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@lbbd.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's Whistleblowing Officer. The council has designated the Monitoring Officer as the Whistleblowing Officer and can be contacted at:

Monitoring Officer, Law & Governance, London Borough of Barking and Dagenham, Fifth Floor, Roycraft House, 15 Linton Road, Barking, IG11 8HE.

(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, the National Audit Office or any of the prescribed persons/organisations a list of which, and the issues they are able to deal with, is available on the Department for Business, Innovation & Skills website at www.gov.uk.

You can get independent advice or support from an organisation called Public Concern at Work. Their contact details are:

Public Concern at Work
CAN Mezzanine
7 - 14 Great Dover Street
London SE1 4YR

Phone: 020 7404 6609
E-mail: whistle@pcaw.org.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.

Further Support, Tools & Guidance

The latest version of the Whistleblowing Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages

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:

caft@lbbd.gov.uk

Assurance & Counter Fraud

The Regulation of Investigatory Powers Act (RIPA) Policy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	For approval by PAASC
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

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) as well as the General Data Protection Regulation **(**GDPR) that will be introduced on 25 May 2018.

Investigations should be conducted in accordance with the Council's Counter Fraud Strategy & Counter Fraud 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, accessing communications data or use of 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 as amended by the Protection of Freedoms Act 2012

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 Human Rights Act. 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

Page Number

Introduction 4

Directed Surveillance 4

Covert Human Intelligence Sources 7

The Authorisation Process 9

Judicial Authorisation 10

Authorisation periods 13

Telecommunications Data - NAFN 13

Handling of material and use of material as evidence 13

Training 13

Surveillance Equipment 13

RIPA Record Quality Reviews 13

The Inspection Process 13

Resources 14

Appendix 1 – Glossary of terms
Appendix 2 – Human Rights Act
Appendix 3 – Data Protection Act/General Data Protection Regulation
Appendix 4 – Key RIPA Officers
Appendix 5 – Judicial Oversight – LBBD Council's Authorised Applicants
Appendix 6 – RIPA Forms:
Application form for Directed Surveillance
Renewal form for Directed Surveillance
Review form for Directed Surveillance
Cancellation form for Directed Surveillance
Appendix 7 – The Central Register
Appendix 8 – Best practice for photographic and video evidence
Appendix 9 – Authorising Officer's Aide-Memoire
Appendix 10 – Open Source
Appendix 11 – Flow Chart for RIPA

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 Monitoring Officer** (RMO). The RMO will be responsible for the maintenance of a **central register** that will be available for inspection by the Investigatory Powers Commissioner's Office (IPCO). 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.

This policy does not affect the general usage of the council's CCTV system. However, if cameras are specifically targeted for 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 them).

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 a necessary and proportionate step to take to secure further evidence.

Low level surveillance, such as 'drive-bys' or everyday activity observed by officers during 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 always 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 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 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 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 Operating officer and/or Director of Law & Governance.

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 (Juveniles) Order 2000 and its Code of Practice.

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 themselves. 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 consider 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, as far 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 always 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 must 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. 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 pass the application through to one of their services "gatekeepers" for review.

4. The gatekeeper, having reviewed the application, will forward the request to the RIPA Monitoring Officer or another officer within the Assurance & Counter Fraud Group. The application will be logged on the central register and assigned a unique reference number. The RIPA Monitoring Officer will then submit the application form to an authorising officer (see Appendix 4) for approval.

5. 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)

6. The AO considers the application and if it is considered complete the application is signed off and returned to the Monitoring Officer who will log the outcome within the central register. This process, along with the initial application and dealings with the Monitoring Officer, can be completed through email.

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

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

9. 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

10. The countersigned application form will form the basis of the application to the Magistrates Court (see further below)

Authorised Activity

11. Authorisation takes effect from the date and time of the approval from the Magistrates Court.

12. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the DVLA.

13. Consideration should be given to notifying the relevant police force intelligence units of the operation.

14. 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.

15. Evidential notes should be made by all officers engaged in the operation. These documents will be kept in accordance with the appropriate retention guidelines.

16. 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

17. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form (Appendix 5).

18. Originals of the complete application, any review or renewal & the cancellation forms will be retained with the central register. Should the forms have been completed electronically, the Monitoring Officer will retain all correspondence.

Judiciary 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) or the 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 the 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 LBBD 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 Communications Data 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/her 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 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 the HM Courts & Tribunals Service (HMCTS) administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking a Judiciary 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 specific points.

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 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 one month. Urgent oral authorisations or authorisations will unless renewed, cease to have effect after 72 hours.

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 Operational Director, Enforcement Services Division and the Director of Public Health. 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, 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 Monitoring Officer must be suitably qualified or trained.

The Senior Responsible Officer in conjunction with the RIPA Monitoring 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.

Surveillance Equipment

All mobile surveillance equipment should be securely held and suitability for use discussed with the Security & Investigations or Assurance & Counter Fraud Group.

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. PAASC will receive quarterly summaries on the Council's use of RIPA.

The Inspection Process

The Investigatory Powers Commissioner's Office (IPCO) 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

The latest Codes of Practice for RIPA can be found on the GOV.UK website at:

https://www.gov.uk/government/collections/ripa-codes

Further information can be found on the Investigatory Powers Commissioner's Office website & via the Home Office website:

https://www.ipco.org.uk/

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

Relevant Acts:

Regulation of Investigatory Powers Act 2000:
http://www.legislation.gov.uk/ukpga/2000/23/contents

Protection of Freedoms Act 2012:
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Human Rights Act 1998:
http://www.legislation.gov.uk/ukpga/1998/42

Data Protection Act 1998:
http://www.legislation.gov.uk/ukpga/1998/29/contents

General Data Protection Regulation:
https://www.eugdpr.org/eugdpr.org.html

The latest version of the RIPA Policy and all our documents can be obtained either by contacting the Assurance and Counter Fraud Group directly or by visiting our intranet pages

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:
caft@lbbd.gov.uk

Appendix 1 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.

Monitoring Officer (MO)
The Monitoring Officer has the day to day responsibility to maintain a central and up-to-date record of all authorisations (Central Register) and arrange appropriate training.

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.

Reviewing Officer (RO)
The Head of Legal Services has been designated as the Reviewing Officer. The role is responsible for ensuring an oversight to the RIPA policy, an Authorising Officer as well as counter signatory in cases of non-RIPA applications.

Senior Responsible Officer (SRO)
The SRO is responsible for the integrity of the processes 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.

Appendix 2

The Human Rights Act 1998

Key Articles of Schedule 1 of the Human Rights Act relevant to RIPA:

- Article 6 – Right to a Fair Trial
- Article 8 – Right to Private and Family Life

ARTICLE 6

RIGHT TO A FAIR TRIAL

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

   a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

   b. to have adequate time and facilities for the preparation of his defence;

   c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

   d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

   e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

ARTICLE 8

RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

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

Appendix 3

The Data Protection Act 1998/General Data Protection Regulations 2018

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 individual's rights
- Be secure
- Not be transferred to non-European Economic Area countries without adequate protection.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Appendix 4

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.

Principal RIPA Officers

Claire Symonds Senior Responsible Officer (SRO)	Chief Operating Officer
Kevin Key RIPA Monitoring Officer (MO)	Corporate Investigation Manager: Assurance & Counter Fraud Group
Fiona Taylor Reviewing Officer (RO)	Director: Law & Governance

Authorising Officers

Chief Executive	Chief Executive
Deputy to Chief Executive	Strategic Director: Service Development & Improvement
Fiona Taylor	Director: Law, Governance & Human Resources
Jonathon Toy Authorising Officer (AO)	Operational Director
Matthew Cole Authorising Officer (AO)	Director of Public Health

Appointment of Staff designated as "Gatekeepers"

Name	Designation
Theo Lamptey	Service Manager, Public Protection
Simon Scott	Senior Investigator - ACFG
Jaiyesh Patel	Senior Investigator - ACFG

Appendix 5

Judicial Oversight – LBBD Council's Authorised Applicants

I certify that the following have been appointed under Section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with section 223(1) Local Government Act 1972:

List of all staff that have attended and passed the training

Name	**Section**	**Appointed from**
Glen Mark	Food Safety, Enforcement Service	12/12/2016
Meribel Mujih	Private Sector Housing, Regulatory Services	13/12/2016
Rob Harvey	Anti-Social Behaviour	13/12/2016
Nicholas Saunders	Anti-Social Behaviour	13/12/216
Pat Jarman	Assurance & Counter Fraud Group	25/01/2017
Arfan Naseem	CCTV & Security	25/01/2017
Geraldine Bowker	Anti-Social Behaviour	25/01/2017
Cenred Elworthy	Trading standards	25/01/2017
Carolyn Greenaway	Care Management	25/01/2017
Philip Bayfield	Regulatory services	25/01/2017
Simon Scott	Assurance & Counter Fraud Group	26/01/2017
Vincent Searle	Trading Standards	26/01/2017
Natalie Males	Private Sector Housing, Enforcement Service	26/01/2017
Robert Redmond	Regulatory Services	26/01/2017

In addition; all Gatekeepers have attended training and are approved for the purpose of making applications.

Kevin Key
RIPA Monitoring Officer

Unique Reference Number	

RIPA Application Form

Part II of the Regulation of Investigatory Powers Act 2000

Application for Authorisation for Directed Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

1. Give name and rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. The exact position of the Authorising Officer should be given.
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• **Name:** • **Address:** • **DOB:** • **Other information as appropriate:**
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*
NB: UNDER SECTION 28 OF RIPA, THE ONLY GROUND AVAILABLE TO THE COUNCIL IS: "FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME OR OF PREVENTING DISORDER". **THIS APPLICATION MUST BE REJECTED, IF THIS GROUND IS NOT RELEVANT TO THE PROPOSED SURVEILLANCE.**
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **Describe precautions you will take to minimise collateral intrusion.**
9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade and Rank or position		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]
I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, Whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Grade and Rank/Position**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 20016 - expires on 30 June 2016, 23:59]				

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		**Grade and Rank or position**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72-hour rule for urgent authorities – check Code of Practice.		e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

Unique Reference Number	

RIPA Renewal Form

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)	----------	**Grade / Rank**	----------
Signature	----------	**Date**	----------
Renewal From:	**Time:**	**Date:**	

Date of first review.	
Date of subsequent reviews of this authorisation.	

Unique Reference Number	

RIPA Review Form

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*			
Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.
3. Detail the reasons why it is necessary to continue with the directed surveillance.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.			
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal] [it should be cancelled immediately].			
Name (Print):	----------	**Grade / Rank**	----------
Signature:	----------	**Date:**	----------

10. Date of next review	

Unique Reference Number	

RIPA Cancellation Form

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch/ Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.			
I, [**insert name**], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date**	----------

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**

Forms can also be obtained from the Assurance and Counter Fraud Group at: caft@lbbd.gov.uk

Or can be printed of and completed as required from the GOV.UK website at:

RIPA Application for Directed Surveillance

Renewal of a Directed Surveillance Authorisation

Review of a Directed Surveillance Authorisation

Cancellation of a Directed Surveillance Authorisation

Appendix 7

Central Register

A central register will be maintained by the RIPA Monitoring 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 8

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 officer's 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.

Checklist 6: Compiling an Audit Trail for Digital Images
in the National Policing Improvement Agency's document:
"PRACTICE ADVICE ON POLICE USE OF DIGITAL IMAGES which is available at:

http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf

provides a list of what information should be included (with date and time of action) in order to make the evidence admissible.

Appendix 9

Authorising Officer's Aide-Memoire

Has the applicant satisfactorily demonstrated proportionality? Court will ask itself should (not could) we have decided this was proportionate. Is there a less intrusive means of obtaining the **same** information? 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? What is the least intrusive way of conducting the surveillance? Has the applicant asked for too much? Can it safely be limited? Remember – Don't use a sledge-hammer to crack a nut! YOUR COMMENTS	**Yes**	**No**

Has the applicant satisfactorily demonstrated necessity? What crime is alleged to be being committed? Has the applicant described it in full? Is surveillance necessary for what we are seeking to achieve? Does the activity need to be covert, or could the objectives be achieved overtly? YOUR COMMENTS	**Yes**	**No**

What evidence does applicant expect to gather? Has applicant described: (a) what evidence he/she hopes to gain, and (b) the value of that evidence in relation to THIS enquiry? YOUR COMMENTS	**Yes**	**No**

Is there any likelihood of obtaining confidential information during this operation? **If "Yes" operation must be authorised by the Chief Executive or in their absence their deputy.**	**Yes**	**No**

Have any necessary risk assessments been conducted before requesting authorisation? Detail what assessment (if any) was needed in this particular case. In the case of a CHIS authorization an appropriate bespoke risk assessment must be completed.	**Yes**	**No**

When applying for **CHIS** authorisation, have officers been identified to: a) have day to day responsibility for the CHIS (a handler) b) have general oversight of the use of the CHIS (a controller) c) be responsible for retaining relevant CHIS records, including true identity, and the use made of the CHIS.	**Yes**	**No**

Have all conditions necessary for authorisation been met to your satisfaction? GIVE DETAILS	**Yes**	**No**

Do you consider that it is necessary to place limits on the operation? IF YES, GIVE DETAILS (e.g. no. of officers, time, date etc.) and REASONS	**Yes**	**No**

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 the Assurance and Counter Fraud Group. Retain copy.

Appendix 10

Open Source

Investigators make much use of the internet to assist with their enquiries. Many of the checks completed could be considered 'open source' that are unlikely to amount to either Directed Surveillance or the use of a CHIS. However, consideration must be had for certain circumstances where RIPA authorisation may be deemed appropriate.

a. Normal Use

When an investigator makes normal checks on the internet, accessing information held within the public domain, on a single occasion, this would be considered acceptable and within the bounds of normal usage. Full records must be kept taking into consideration the expectations of the Criminal Procedure and Investigations Act. Throughout an investigation, it would be appropriate for an investigator to make ***occasional*** further checks. If, on the other hand, it becomes apparent that regular checks are taking place to monitor someone's activities, this may constitute Directed Surveillance.

b. Directed Surveillance

When regular checks of the same pages occur, in order to monitor activity, this may be Directed Surveillance. Should this be happening, consideration should be had for the use of RIPA.

c. Covert Human Intelligence Source

Looking at publicly available pages is considered 'Open Source' but should a decision be made to request access to view page then the situation changes. In order to access specific information a personal or other relationship would have to be created or maintained potentially amounting to the use of a CHIS. An example where this is likely is sending a friend request within Facebook.

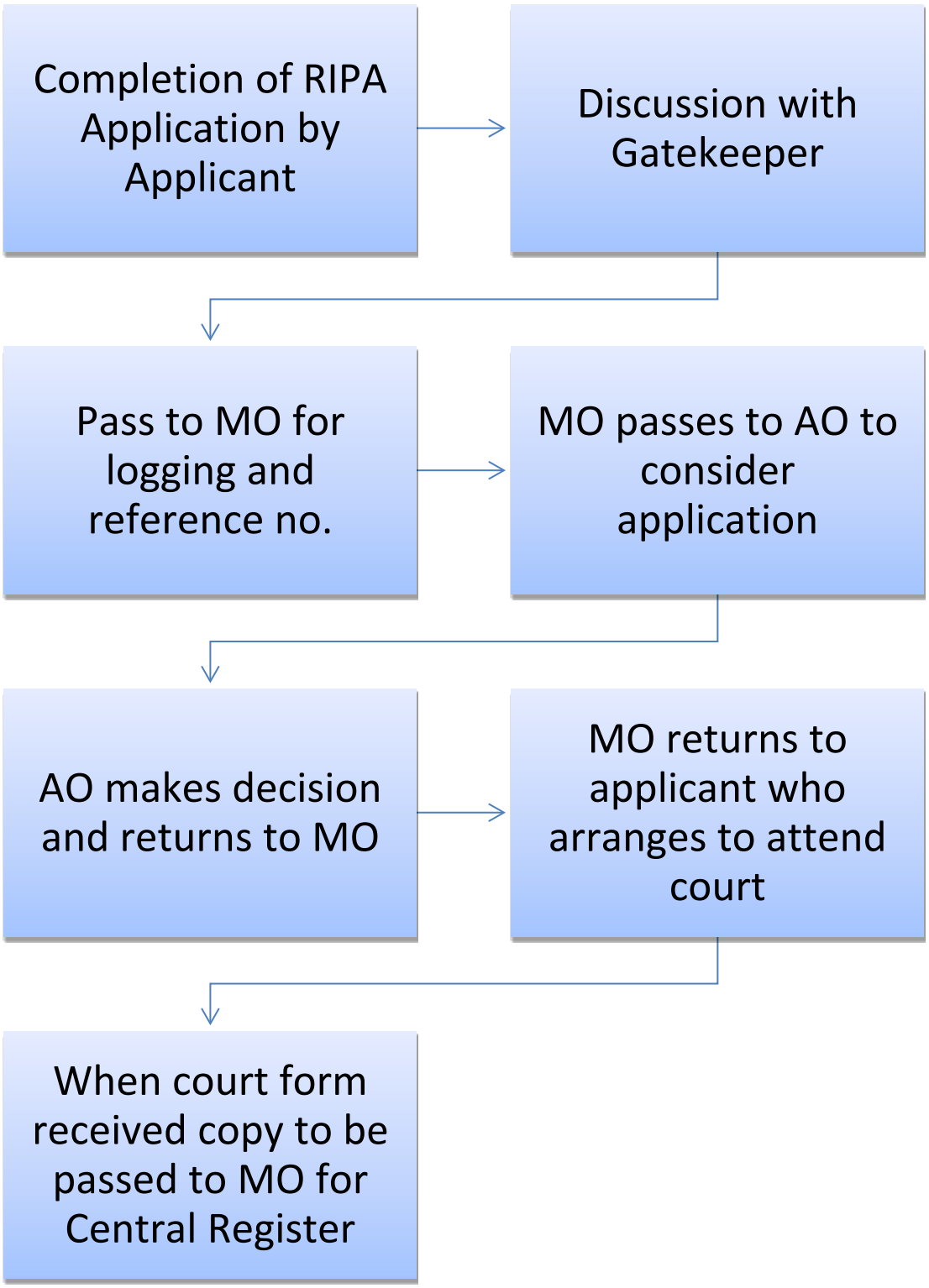
EXCEPTION

Should you use an identity that is overt (such as LBBD Fraud Investigations or LBBD trading Standards) to send the request from. In this instance, it would be classed as monitoring and not Directed Surveillance/CHIS.

Officers are encouraged to follow the procedures of this policy (either RIPA or Non-RIPA) should the above circumstances present themselves.

Appendix 11

Flow Chart for RIPA Applications



APPENDIX G

Assurance & Counter Fraud

The Bribery Act Policy

June 2018

Date Last Reviewed:	June 2017
Approved by:	PAASC
Date Approved:	*Draft for approval*
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

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

Contents

Title	Page No.
The Bribery Act	1
What are adequate procedures?	2
What are the six principles	2
Golden Rules	4
Employee Responsibilities	4
Reporting a concern	5
Further support, tools and guidance	6

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 of the Bribery Act 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 tough stance against 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 Senior 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 as part of a wider fraud risk assessment. We keep a record of the assessment, 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 Corporate Investigation Manager (Assurance & Counter Fraud Group) 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 on the Council Intranet). 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 2015, persons are to be excluded from consideration to be awarded public contracts if they have been convicted of a corruption offence. Organisations that are convicted of failing to prevent bribery are not automatically barred from competing for public contracts.

This is a complex area and procurement advice must be sought where verification has revealed conviction(s) relating to bribery, fraud and other specified unlawful activities within the Regulations. 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 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 information on 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; 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, leading to dismissal 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. 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 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 Corporate Investigation Manager (Assurance & Counter Fraud Group) on: 0208 227 2850.

Other relevant policies

- Fraud Prosecution Policy
- Money Laundering Policy
- Whistleblowing Policy
- Counter Fraud Policy
- Employee Code of Conduct
- Rules in respect of Gifts and Hospitality
- Disciplinary Procedure and Disciplinary Rules

Further Support, Tools & Guidance

The latest version of the Bribery Act Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages

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:

caft@lbbd.gov.uk

APPENDIX H

Assurance & Counter Fraud

Proceeds of Crime Act Policy & Procedures

June 2018

Date Last reviewed:	June 2017
Approved by:	PAASC
Date Approved:	draft
Version Number:	1.1
Review Date:	June 2019
Document Owner:	Finance Director

This Policy sets out the Council's commitment to use the proceeds of crime act as a primary tool in its efforts to disrupt and dismantle individuals and organised crime groups that operate within our jurisdiction.

What are the aims and requirements of this policy?

The Council wishes to ensure that those prosecuted for fraud offences do not profit from the benefit obtained from their criminal activity. Following proper processes, the Council will take appropriate action to confiscate assets and money held where it cannot be evidenced that these were acquired through legitimate means. Additional powers under the act will be used to ensure the comprehensive investigation of relevant cases.

Who is governed by this policy?

The policy applies to Accredited Financial Investigators employed directly or engaged by the London Borough of Barking & Dagenham and those who prosecute cases where proceeds of crime recovery is appropriate.

Executive Summary

The Proceeds of Crime Act (POCA) 2002 is to be used by the Assurance & Counter Fraud Group within Barking and Dagenham Council as a primary tool in its efforts to disrupt and dismantle individuals and organised crime groups that operate within our jurisdiction.

The Assurance & Counter Fraud Group will also look for opportunities to use the Proceeds of Crime Act 2002 to support its Counter Fraud Strategy. When cases are highlighted within such areas as Housing, Planning, Trading Standards or other Regulatory Services, the Financial Investigator will be tasked in ensuring that those convicted of an offence from which they have benefitted from are stripped of the benefit of that crime. The purpose of this policy is to provide information and guidance on the use of the Proceeds of Crime Act 2002 and the procedures to be adopted by accredited Financial Investigators employed or engaged by the London Borough of Barking & Dagenham.

Contents

Background 1
Key Provisions 1
Further Support, Tools & Guidance 17

Background

The Proceeds of Crime Act 2002 received Royal Assent on 24 July 2002 and was the subject of phased implementation, becoming fully effective on 24 March 2003.

Key Provisions

The Act is broken down into 12 Parts. The following parts are relevant to this Policy;

Part 1 - Introduction

Part 2 – Confiscation (including Restraint) - England & Wales

Part 5 – Cash Seizure

Part 7 – Money Laundering

Part 8 – Investigations

Part 1 – Introduction

The Proceeds of Crime Act 2002 (POCA) extends to all parts of the UK.

The Act requires that all Financial Investigators and Financial Intelligence Officers are registered and accredited and that accreditation may relate to all or specific provisions of the Act. Accreditation is bestowed by the National Crime Agency (NCA) Proceeds of Crime Centre (POCC), who is also required to monitor the performance of accredited Financial Investigators and Financial Intelligence Officers, withdrawing the accreditation from any person who contravenes or fails to comply with any condition subject to their accreditation. The NCA POCC 'Financial Investigators' Registration, Accreditation and Monitoring Policy' can be accessed via the Financial Investigation Support System (FISS) gateway.

Barking and Dagenham Council has its own Financial Investigator and will maintain a financial investigation capability to deal with matters arising. The Financial Investigator role will sit within Regulatory Services with a Senior Authorising Officer (SAO), based with The Assurance and Counter Fraud Group, taking responsibility for all authorisations of requests relating to POCA.

Barking and Dagenham is required to nominate a Single Point of Contact (SPOC) to liaise with the NCA POCC in respect of all training, accreditation matters and Joint Asset Recovery.

Part 2 – Confiscation

The legislation

The POCA confiscation legislation came into force on the 24 March 2003. It replaced previous confiscation legislation namely the Criminal Justice Act 1988 and the Drugs Trafficking Act 1994. When an offence has occurred before the 24 March 2003 or where an offence straddles this date, then the earlier legislation must be used.

Confiscation is conducted in the Crown Court following conviction in the Crown Court or where the case has been committed to the Crown Court for sentence. Where a case is considered

suitable for confiscation and the subject has been tried / sentenced in the Magistrates Court then, on application of the Crown, the case can be committed to the Crown Court for specific consideration of confiscation. This includes summary only offences.

The confiscation process is mandatory where the prosecutor (Director of Law & Governance) asks the Court to proceed or where the Court itself considers it appropriate to do so.

The expression 'Confiscation Order' is a misnomer as the Order itself does not confiscate any specific property but, instead, requires the defendant to pay over a sum of money. This is termed as the 'Recoverable Amount'.

Confiscation involves the calculation of the benefit obtained by the subject as a result of, or in connection with, their 'criminal conduct'. 'Criminal conduct' is conduct which constitutes an offence in England and Wales or would do if it occurred there. There are two types of 'criminal conduct', 'particular criminal conduct' and 'general criminal conduct'.

In certain circumstances the Court must determine whether a subject has a 'criminal lifestyle'. This determination is purely a formulaic exercise.

Where it is found that a defendant does have a 'criminal lifestyle' then the Court is required to make certain assumptions about any property transferred to the subject in the six years before proceedings were commenced; any expenditure incurred by the subject in the six years before proceedings were commenced and, any property held by the subject at any time after the date of conviction, unless it can be shown that making a particular assumption would be incorrect. The accrued value of the assumptions is the subjects benefit from 'general criminal conduct'.

Where the subject is not found to have a 'criminal lifestyle' then the Court must decide whether they have benefited from their 'particular criminal conduct', or offences with which they have been convicted.

Procedure

In all cases where there is evidence to suggest that a subject has benefited from an offence or offences under investigation, or where they have been charged with an offence listed in Schedule 2 of the Proceeds of Crime Act 2002, it will be the duty of the officer in charge of the investigation to contact the Financial Investigator. They will decide on the suitability of the case for a confiscation investigation and whether the Investigation can be run alongside the original Investigation with the aid of the Financial Investigator.

It will be the responsibility of the Investigating officer in charge of the case to notify the appointed Financial Investigator of the name and contact details of the relevant prosecutor responsible for the case and full details of all subsequent Court hearings in advance of that hearing. The officer in charge of the case will also provide the Financial Investigator with access to all material considered relevant to the Financial Investigator, including seized material in a timely manner.

Further, the Investigating officer in charge of the case or Barking and Dagenham Legal Services must notify the Senior Appropriate Officer and or Financial Investigator of the confiscation investigation before any 'Basis of Plea' is accepted by Barking and Dagenham Council as this is often a means by which defendants and their legal teams mitigate subsequent Confiscation Orders.

As an incentive to law enforcement agencies to pursue confiscation the UK Government currently have a scheme in place, the 'Asset Recovery Incentivisation Scheme' (ARIS), whereby

18.75% of all confiscated money is paid to the agency obtaining the Order. This money is paid by the Home Office to the Audit and Counter Fraud Group. Through its POCA Single Point of Contact (SPOC), the Audit and Counter Fraud Group can then draw on this money but it must be used in accordance with Home Office guidelines, namely that it will be utilised in improving asset recovery performance or in tackling crime. In making the application to draw on ARIS money the POCA SPOC must detail, on the relevant form, how they intend to use the money in accordance with the Home Office Guidelines. POCA SPOC will then, on an annual basis, be required to certify that the money has been used in accordance with their initial application.

Before paying any incentivisation money the Home Office reconciles the money received by it to the relevant entry on the Joint Asset Recovery Database (JARD). Access to JARD is granted to individual Financial Investigators by the NCA and controlled by the JARD Single Point of Contact for Local Authorities (SPOC). It is the relevant Financial Investigators responsibility to ensure that JARD records are opened and maintained in accordance with JARD Guidelines.

The Local Authority JARD SPOC is Justin Miller within London Borough of Southwark's Trading Standard's Team.

Restraint

The legislation

The POCA permits an application for a Restraint Order to be made to the Crown Court as soon as a criminal investigation has been started, but not concluded, if there is reasonable cause to believe that the alleged offender has benefited from their 'criminal conduct' and that there is risk that assets will be dissipated if the Order is not made.[1]

The power to apply for a Restraint Order lies only with the prosecutor or an Accredited Financial Investigator with part 2 powers, namely a person who has been authorised to make such applications by the NCA. Where the application is made by an accredited Financial Investigator within Barking and Dagenham Council the application must have been authorised by the prosecutor of Barking and Dagenham Legal Services. The procedure for application for a Restraint Order is set out in the Criminal Procedure Rules.

A Restraint Order prohibits any specified person from dealing with any realisable property held by him whether or not it is described in the Order. It includes property held by a person other than the alleged offender. This could include banks, solicitors etc.

An application for a Restraint Order is made ex parte.

In making an application the Accredited Financial Investigator must compile a written statement outlining the full facts of the case and the reason why the making of such Order is required. A copy of this Statement together with a copy of the Restraint Order must be served as soon as possible after its issue on all relevant persons.

Procedure

In all cases where there is reason to believe or suspect that a defendant or person under investigation has benefited from his criminal conduct and there is reason to believe that the person has, or is likely to, dissipate their assets, officers should seek immediate advice from the Financial Investigator. The Financial Investigator will consider the suitability of obtaining a

[1] Re AJ and DJ. Unreported, 9 December 1992, CA & Re B [2008] EWCA Crim 1374

Restraint Order and, where suitable, will make such application with the support of Barking and Dagenham Legal Services and the SAO.

In considering the suitability of the application the Financial Investigator, in conjunction with the officer in charge of the case, should consider any risks to the investigation by making the full and frank disclosure required within the supporting Statement.

Where a Restraint Order is obtained, the Financial Investigator will liaise with the officer in charge of the main investigation to ensure that the Order is served on all relevant persons as soon as possible.

It is the Financial Investigators responsibility to ensure that the Order is properly recorded on JARD.

All Restraint Orders must be signed by the prosecutor (Barking and Dagenham Legal Services) and not a Financial Investigator as there are personal liabilities if the application is made by an individual.

Part 7 – Money Laundering

The legislation

Money laundering is an act which constitutes and offence under Sections 327, 328 or 329 of the Proceeds of Crime Act, or an attempt, conspiracy or incitement to commit any of those offences, or aiding, abetting, counselling or procuring there commission.[2]

It is important to remember that the term money laundering is a misnomer as it does not solely relate to money, it relates to 'criminal property'.

'Criminal property' is defined as;[3]

'Property is criminal property if it constitutes a person's benefit from criminal conduct or it represents such benefit, and the alleged offender knows or suspects that it constitutes or represents such a benefit'.

'Criminal conduct' is defined as;[4]

'Criminal conduct' is conduct which constitutes an offence in any part of the United Kingdom or would constitute an offence in any part of the United Kingdom if it occurred there'.

The three principle offences of Money Laundering are;

<u>Section 327 – Concealing the proceeds of criminal conduct</u>

A person commits an offence if he:

i. Conceals criminal property;

ii. Disguises criminal property;

[2] Section 340(11) Proceeds of Crime act 2002
[3] Section 340(3) Proceeds of Crime act 2002
[4] Section 340(2) Proceeds of Crime act 2002

iii. Converts criminal property;

iv. Transfers criminal property;

v. Removes criminal property from England and Wales or from Scotland or from Northern Ireland.

Section 328 – Assisting another to retain the benefits of criminal conduct

A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Section 329 – Acquisition, use, and possession of the proceeds of crime

A person commits an offence if he:

i. Acquires criminal property;

ii. Uses criminal property;

iii. Has possession of criminal property.

Defences to Money Laundering offences:

There are a number of statutory defences to the three principle offences of Money Laundering.

A person does not commit an offence if:

a) He makes an authorised disclosure[5] and (if the disclosure is made before he does the act mentioned) he has the appropriate consent;

b) He intended to make such a disclosure but had a reasonable excuse for not doing so;

c) The act is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

Nor does a person commit an offence if;

a) He knows, or believes on reasonable grounds, that the relevant criminal conduct occurred in a particular country or territory outside the UK, and

b) The relevant criminal conduct-

(i) Was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory, and

(ii) Is not of a description prescribed by an Order made by the Secretary of State.

[5] Under Section 338 Proceeds of Crime Act 2002

There is an additional defence in relation to the offence of 'Acquisition, use, and possession of the proceeds of crime' under Section 329 where someone has acquired or used or had possession of the said property for adequate consideration.

Important notes – Money Laundering offences:

It is vital in any prosecution for a money laundering offence that it can be shown, to the criminal standard, that the property in question constitutes or represents someone's benefit from an offence and that they either knew or suspected that to be the case.

There are two ways in which the Crown can prove that property derives from crime. Firstly by showing that it derives from conduct of a particular kind or kinds and that conduct is unlawful, or by evidence of the circumstances in which the property is handled which are such as to give rise to the irresistible inference that it can only be derived from crime.[6]

When considering the Section 328 offence of 'Assisting another to retain the benefits of criminal conduct' the property in question must be criminal property at the time the person becomes concerned in the arrangement.[7] Where the arrangement facilitates an offence and thus subsequently turns legitimate property into criminal property, alternative offences must be considered.

An 'authorised disclosure' is one that is made to the NCA, who then decide whether or not to grant consent for the transaction to proceed. This will always be in writing and on prescribed forms and can be obtained if necessary.

Other offences:

In addition to the three principle money laundering offences outlined above there are a number of additional offences covered by the Act. These offences and various defences are complex and primarily relate to persons involved in the regulated sector. They include;

Failure to disclose knowledge or suspicion of money laundering[8]

A person commits an offence if the following conditions are satisfied:

1. That he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

2. That the information or other matter on which his knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.

3. That he can identify the other person mentioned or the whereabouts of any of the laundered property, or that he believes, or that it is reasonable to expect him to believe that the information or other matter will or may assist in identifying that other person or the whereabouts of any of the laundered property.

---

[6] R v Anwoir [2008] 4 All ER 582 EWCA Crim 1354
[7] R v Geary [2010] EWCA Crim 1925
[8] Section 330 Proceeds of Crime Act 2002

4. That he does not make the required disclose to a nominated officer, or a person authorised by the Director General of NCA as soon as is practicable after the information or other matter comes to him.

Tipping off[9]

(1) A person commits an offence if:

(a) The person discloses any matter within (2) below;

(b) The disclosure is likely to prejudice any investigation that might be conducted following the disclosure; and

(c) The information on which the disclosure is based came to the person in the course of a business in the regulated sector.

(2) The matter are that the person or another person has made a disclosure under this Part:

(a) To a constable;

(b) To an officer of revenue and Customs;

(c) To a nominated officer, or

(d) To a member of staff of NCA authorised by the Director General to receive such disclosures.

Procedure

Where there is evidence to support a charge of Money Laundering contrary to Sections 327 or 328 which is over and above the evidence proving the original offence these charges should be seriously considered. Where advice is needed to establish whether the act or acts support a charge of Money Laundering the advice of the Financial Investigator should be sought.

When considering offences of Failure to Disclose Knowledge or Suspicion of Money Laundering or Tipping Off it is strongly recommended that advice is sought from the Financial Investigator.

Where a person is charged with an offence contrary to Sections 327 or 328 of POCA they should advise the Financial Investigator immediately as both offences fall within Schedule 2 of POCA 2002 (see above).

Part 8 – Investigations

The legislation

The primary focus of the powers conferred by Part 8 of the POCA 2002 is the investigation into the proceeds of crime with a view to recovery and confiscation of those proceeds and prosecution for money laundering offences. These extensive powers enable an investigator to obtain information in order to trace criminal property, to monitor the activity of transactions and to identify persons in control of such property. A failure or refusal to comply with Court Orders

[9] Section 333A Proceeds of Crime Act 2002

can result in proceedings for contempt or for specific criminal offences including the offence of 'Prejudicing an Investigation' (see below).

The investigative powers contained within POCA 2002 can be granted for the purpose of five different types of POCA investigations. They are;

1. Confiscation Investigations

A confiscation investigation is an investigation into whether a person has benefited from his criminal conduct or the extent or whereabouts of such benefit.

2. Money Laundering Investigations

A money laundering investigation is an investigation into whether a person has committed a money laundering offence. (See definition of a money laundering offence above).

3. Civil Recovery Investigations

A civil recovery investigation is an investigation into whether property is recoverable property or associated property, to determine who holds that property, and its extent and whereabouts.

4. Detained Cash Investigations

A detained cash investigation is an investigation into the derivation of cash detained under the 'Cash Seizure' provisions or whether it was intended for use in unlawful conduct.

5. Exploitation Proceeds Investigations

An exploitation proceeds investigation is an investigation for the purposes of the 'criminal memoirs' provision of the Coroners and Justice Act 2009.[10]

The five investigative powers contained within POCA 2002 are;

- Production Orders;
- Search and Seizure Warrants;
- Account Monitoring Orders;
- Customer Information Orders; and
- Disclosure Orders.

Production Orders

The purpose of a Production Order is to obtain material relating to a known person or business, such as account holder details, identity documents used when opening an account, bank statements and correspondence. A Production Order can be extended to grant the power of entry onto premises to obtain access to the material detailed in the Order.[11] A Production Order is available for all categories of investigation.

[10] Schedule 19 of the Coroners and Justices Act 2009.
[11] Section 347 Proceeds of Crime Act 2002

Applications for Production Orders

Applications must be made by an 'appropriate officer'[12] and must state that, a person specified in the application is subject to a money laundering, a confiscation or an exploitation proceeds investigation, or, that the property specified in the application is subject to a civil recovery or a detained cash investigation. The application must state that the Order is sought for the purposes of the investigation; that the Order is sought in relation to material or material of a description, specified in the application; and, that a person specified in the application appears to be in possession or control of the said material. The Order is an order either requiring the person named to produce the material to an appropriate officer for him to take it away, or requiring the person named in it to give an appropriate officer access to it, within the period stated. The period stated must be a period of seven days unless it appears to the judge that a shorter or longer period would be appropriate.[13]

The general rule is that the application must identify the respondent and be in writing. The Court and the respondent (unless the Court otherwise directs) must be served with a copy of the application. The applicant must serve any Order made on each respondent.[14]

In making the application the applicant must describe the material that it seeks; explain why they think the material is in the respondent's possession or control; explain why the material is likely to be of substantial value to the investigation and why it is in the public interest for the material to be produced. They must also confirm that none of the material is expected to be subject to legal privilege or excluded material and propose the terms of the Order and the period within which it should be produced if it is considered that seven days from the date of the Order is not appropriate.[15]

Where an applicant wants the Court to make an Order to grant entry, they must additionally specify the premises to which entry is sought, explain why the Order is needed, and propose the terms of the Order.[16]

The Court must determine an application for an Order at a hearing (which will be in private unless the Court directs otherwise) in the applicant's presence. The Court must not determine an application in the absence of the respondent or any other person affected by the Order unless the absentee has had at least 2 business days in which to make representations, or, the Court is satisfied that the applicant cannot identify or contact the respondent; it would prejudice the investigation if the respondent were present; or it would prejudice the investigation to adjourn or postpone the application so as to allow the respondent to attend.[17]

Where the application includes information that the applicant thinks ought not be revealed to the recipient the applicant must omit that information from the part of the application that is served on the respondent or other persons; identify that information on the Court copy to show that it is only for the Court; and explain on the Court copy why the applicant has withheld it. A hearing of an application where information has been withheld from the respondent may take place, wholly or partially, in the absence of the respondent and any other person.[18]

---

[12] See Section 378 Proceeds of Crime Act 2002
[13] Section 345 Proceeds of Crime Act 2002
[14] Rule 6.14 Criminal Procedure Rules 2011
[15] Rule 6.15 Criminal Procedure Rules 2011
[16] Rule 6.16 Criminal Procedure Rules 2011
[17] Rule 6.3 Criminal Procedure Rules 2011
[18] Rule 6.21 Criminal Procedure Rules 2011

Search and Seizure Warrants

A Search and Seizure warrant is a warrant giving authority to enter and search the specified premises and to seize and retain any material found there which is likely to be of substantial value to the investigation. In general there are two situations where a Search and Seizure warrant will be necessary: the first is where a Production Order has been made and not complied with, and there are reasonable grounds for believing that the required material is on the premises; the second is in circumstances where it is not possible to make a Production Order.

Applications for Search and Seizure Warrants

Applications must be made by an 'appropriate officer'[19] and must state that, a person specified in the application is subject to a money laundering, a confiscation or an exploitation proceeds investigation, or, that the property specified in the application is subject to a civil recovery or a detained cash investigation. The application must also state that the Warrant is sought for the purposes of the investigation; that it is sought in relation to the premises specified in the application; and, that it is sought in relation to material specified in the application. [20]

Account Monitoring Orders

An Account Monitoring Order, unlike the other investigative tools which are concerned with historical information, allows an investigator to monitor the activity of a particular account held at a financial institution for a period of up to 90 days after the Order is made. It is available for all types of POCA investigation except a 'detained cash' investigation.

Applications for Account Monitoring Orders

Applications must be made by an 'appropriate officer'[21] and must state that a person specified in the application is subject to a money laundering, confiscation or an exploitation proceeds investigation, or, that the property specified in the application is subject to a civil recovery investigation, and the person specified in the application appears to hold the property. The application must also state that the Order is sought for the purposes of the investigation and that it is sought in relation to account information of the description specified.[22] Account Monitoring Orders are not available in 'Detained Cash' investigations.

'Account information' is information relating to an account or accounts held at the financial institution. The application may specify information relating to all accounts held by the person specified in the application; a particular description of accounts held by that person; or a particular account or accounts held by that person.

An Account Monitoring Order requires the named financial institution to provide account information for the period stated to an appropriate officer in the manner, and at or by the time or times, stated in the Order. The application must specify why the information is likely to be of substantial value to the investigation and explain why it is in the public interest for the information to be provided. [23]

---

[19] See Section 378 Proceeds of Crime Act 2002
[20] Section 352 Proceeds of Crime Act 2002
[21] See Section 378 Proceeds of Crime Act 2002
[22] Section 370 Proceeds of Crime Act 2002
[23] Section 370 Proceeds of Crime Act 2002 and Rule 6.19 Criminal Procedure Rules 2011

The general rule is that the application must identify the respondent and be in writing. The Court and the respondent (unless the Court otherwise directs) must be served with a copy of the application. The applicant must serve any Order made on each respondent.[24]

The Court must determine an application for an Order at a hearing (which will be in private unless the Court directs otherwise) in the applicant's presence. The Court must not determine an application in the absence of the respondent or any other person affected by the Order unless the absentee has had at least 2 business days in which to make representations, or, the Court is satisfied that the applicant cannot identify or contact the respondent; it would prejudice the investigation if the respondent were present; or it would prejudice the investigation to adjourn or postpone the application so as to allow the respondent to attend.[25]

Where the application includes information that the applicant thinks ought not be revealed to the recipient the applicant must omit that information from the part of the application that is served on the respondent or other persons; identify that information on the Court copy to show that it is only for the Court; and explain on the Court copy why the applicant has withheld it. A hearing of an application where information has been withheld from the respondent may take place, wholly or partially, in the absence of the respondent and any other person.[26]

Customer Information Orders

A Customer Information Order requires a financial institution to provide details of any accounts held by a person under investigation. The Order may require all such institutions, or a selection of them, to comply with the Order.

Applications for Customer Information Orders

Applications must be made by an 'appropriate officer'[27] and must state that a person (including company of any description) specified in the application is subject to a money laundering, confiscation or an exploitation proceeds investigation, or, that the property specified in the application is subject to a civil recovery investigation, and the person specified in the application appears to hold the property. The application must also state that the Order is sought for the purposes of the investigation and that it is sought against the financial institution or financial institutions specified in the application.[28] Customer Information Orders are not available in 'Detained Cash' investigations.

'Customer information' is information whether the person holds, or has held, an account or accounts (or any safe deposit box) at the financial institution (whether solely or jointly with another) and (if so) information as to:-[29]

If the account holder is a person:

- The account number or numbers (or the number of any safe deposit box);
- The person's full name;

[24] Rule 6.14 Criminal Procedure Rules 2011
[25] Rule 6.3 Criminal Procedure Rules 2011
[26] Rule 6.21 Criminal Procedure Rules 2011
[27] See Section 378 Proceeds of Crime Act 2002
[28] Section 363 Proceeds of Crime Act 2002
[29] Section 364 Proceeds of Crime Act 2002

- Their date of birth;
- Their most recent address and any previous addresses;
- The account (or safety deposit box) opening and closing dates;
- Evidence of identity obtained under Anti-Money Laundering legislation;
- The full details of any joint account holders.

If the account holder is a company:

- The account number or numbers (or the number of any safe deposit box);
- The person's full name;
- A description of any business which the person carries out;
- The country or territory in which it is incorporated or otherwise established;
- Any VAT number assigned to it;
- Its Registered office and any previous Registered Office;
- The account (or safety deposit box) opening and closing dates;
- Evidence of identity obtained under Anti-Money Laundering legislation;
- The full details of any joint account holders.

The general rule is that the application must identify the respondent and be in writing. The Court and the respondent (unless the Court otherwise directs) must be served with a copy of the application. The applicant must serve any Order made on each respondent.[30]

The application must specify why customer information about the person under investigation is likely to be of substantial value to that investigation and explain why it is in the public interest for the information to be provided. It must also propose the terms of the Order.[31]

The Court must determine an application for an Order at a hearing (which will be in private unless the Court directs otherwise) in the applicant's presence. The Court must not determine an application in the absence of the respondent or any other person affected by the Order unless the absentee has had at least 2 business days in which to make representations, or, the Court is satisfied that the applicant cannot identify or contact the respondent; it would prejudice the investigation if the respondent were present; or it would prejudice the investigation to adjourn or postpone the application so as to allow the respondent to attend.[32]

Where the application includes information that the applicant thinks ought not be revealed to the recipient the applicant must omit that information from the part of the application that is served

[30] Rule 6.14 Criminal Procedure Rules 2011
[31] Rule 6.18 Criminal Procedure Rules 2011
[32] Rule 6.3 Criminal Procedure Rules 2011

on the respondent or other persons; identify that information on the Court copy to show that it is only for the Court; and explain on the Court copy why the applicant has withheld it. A hearing of an application where information has been withheld from the respondent may take place, wholly or partially, in the absence of the respondent and any other person.[33]

Disclosure Orders

A Disclosure Order is an Order authorising an 'appropriate officer'[34] to give any person the 'appropriate officer' considers has relevant information, notice in writing requiring him to answer questions, provide information, or produce documents. A Disclosure Order may only be obtained in relation to confiscation, exploitation proceeds and civil recovery investigations. Relevant information is information (whether contained in a document or not) which the appropriate officer considers to be relevant to the investigation.[35]

Applications for Disclosure Orders

Applications for a Disclosure Order may be made by a 'the relevant authority', namely a prosecutor in confiscation cases, or a member of NCA's staff in an exploitation proceeds or civil recovery investigation. The 'relevant authority' may only make an application for a Disclosure Order in relation to a confiscation investigation if it is in receipt of a request to do so from an 'appropriate officer'.

The application must state that, a person specified in the application is subject to a confiscation or exploitation proceeds investigation, or, that the property specified in the application is subject to a civil recovery or a detained cash investigation and that the Order is sought for the purposes of the investigation.

The general rule is that the application must identify the respondent and be in writing. The Court and the respondent (unless the Court otherwise directs) must be served with a copy of the application. The applicant must serve any Order made on each respondent.[36]

In making the application the applicant must describe in general terms the information the applicant wants the respondent to provide; explain why the material is likely to be of substantial value to the investigation and why it is in the public interest for the material to be produced. He must also confirm that none of the material is expected to be subject to legal privilege or excluded material and propose the terms of the Order.[37]

Where the application includes information that the applicant thinks ought not be revealed to the recipient the applicant must omit that information from the part of the application that is served on the respondent or other persons; identify that information on the Court copy to show that it is only for the Court; and explain on the Court copy why the applicant has withheld it. A hearing of an application where information has been withheld from the respondent may take place, wholly or partially, in the absence of the respondent and any other person.[38]

Procedure

---

[33] Rule 6.21 Criminal Procedure Rules 2011
[34] See Section 378 Proceeds of Crime Act 2002
[35] Section 357 Proceeds of Crime Act 2002
[36] Rule 6.14 Criminal Procedure Rules 2011
[37] Rule 6.17 Criminal Procedure Rules 2011
[38] Rule 6.21 Criminal Procedure Rules 2011

The Financial Investigator is responsible for conducting confiscation and money laundering investigations.

Section 378 Proceeds of Crime Act 2002 states that an 'appropriate officer' includes a constable and an accredited Financial Investigator. However, all applications for a Production Order, Search and Seizure Warrant, Account Monitoring Order or Customer Information Order under this Act will be made by an Accredited Financial Investigator. All applications for a Disclosure Order will be made by Barking and Dagenham Legal Services on application by a Financial Investigator.

Prejudicing an Investigation

The Proceeds of Crime Act 2002 also creates a specific offence relating to POCA investigations of Prejudicing an Investigation,[39] namely:

A person commits an offence if he knows or suspects that an appropriate officer is acting, or proposing to act, in connection with a money laundering investigation, a confiscation investigation, a civil recovery investigation, a detained cash investigation or an exploitation proceeds investigation which is being or is about to be conducted and he:

1) Makes a disclosure which is likely to prejudice the investigation; or

2) Falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.

A person does not commit an offence if:

He does not know or suspect that the disclosure is likely to prejudice the investigation; and

1) The disclosure is made in the exercise of a function under this Act; or

2) He is a professional legal advisor and the disclosure is to a client (or his representative) in connection with the giving of legal advice to the client, or to any person in connection with legal proceedings or contemplated legal proceedings.

Procedure

Where an officer in charge of an investigation has cause to suspect that the above offence has been committed they should liaise with either the SAO or the Financial Investigator to consider the best course of action.

Criminal Forfeiture

In addition to confiscation under the Proceeds of Crime Act 2002 there are further criminal powers to forfeit property which should be considered as a supplement to the Proceeds of Crime Act 2002 when considering how to tackle assets / property held by criminals. In each case the property in question must have been lawfully seized and the defendant must have been found guilty of an offence

[39] Section 342 Proceeds of Crime Act 2002

Financial Investigators

Accredited Financial Investigators will need to adhere to CPD (Continuing Professional Development) activities which are held on FISS and are monitored by the NCA, failure to do so will lead to suspension on FISS and loss of Financial Investigation powers.

The CPD activities are set bi-monthly via FISS, with a twelve-week completion period for each activity. The activities are either 'Information only' or 'Assessed'.

In addition to the activities described above, all those in the CPD system are required to update their CPD 'Evidence Summary Sheet' quarterly.

For Corporate and Housing fraud cases, the officer in charge of the case will refer and highlight potential assets, proceeds of crime and money laundering. A referral form will then be completed for Financial Investigation with full details of the case including properties owned, cash in the bank, assets. This referral will then need to be passed to the Financial Investigator for consideration. The Financial Investigator will then liaise with the officer in charge of the case for further financial Investigation.

The Financial Investigator must record all matters arising from a financial Investigation onto the case log and on JARD in a timely manner.

Further Support, Tools & Guidance

The latest version of the Proceeds of Crime Act Policy and all of our documents can be obtained either by contacting the Assurance & Counter Fraud Group directly or by visiting our intranet pages

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:

caft@lbbd.gov.uk