



AUDIT AND PERFORMANCE REVIEW PANEL

TUESDAY, 16TH FEBRUARY, 2016

At 7.00 pm

in the

COUNCIL CHAMBER - TOWN HALL,

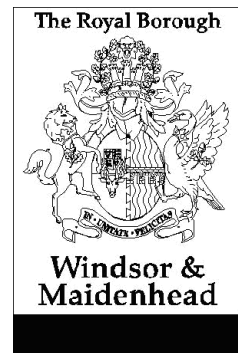
SUPPLEMENTARY AGENDA

PART I

<u>ITEM</u>	<u>SUBJECT</u>	<u>PAGE NO</u>
7.	<u>RBWM ANTI FRAUD AND ANTI CORRUPTION POLICIES REFRESH</u> To consider the report.	3 - 36

This page is intentionally left blank

Report for: ACTION



Contains Confidential or Exempt Information	NO - Part I
Title	Counter Fraud Policies
Responsible Officer(s)	Andrew Brooker, Head of Finance
Contact officer, job title and phone number	Catherine Hickman, Service Manager – Shared Audit and Investigation Service, 07917 265742
Member reporting	Cllr Brimacombe
For Consideration By	Audit and Performance Review Panel
Date to be Considered	16 February 2016
Implementation Date if Not Called In	Immediately
Affected Wards	All

REPORT SUMMARY

1. This report recommends that the Audit and Performance Review Panel (A&PRP) approves the updated Council Corporate Fraud Policies in accordance with the requirements of its Terms of Reference.
2. If adopted, there are no additional financial implications for the Council. The updated Corporate Fraud Policies will come into effect immediately.

If recommendations are adopted, how will residents benefit?

Benefits to residents and reasons why they will benefit	Dates by which residents can expect to notice a difference
Counter fraud work undertaken by the council is supported by robust policies and procedures thereby protecting both the interests of the residents and the council, including the safeguarding of assets.	Immediately

1. DETAILS OF RECOMMENDATION

RECOMMENDATION: Option 1: The A&PRP approve the following Counter Fraud Policies:

- Prosecution and Sanctions Policy
- Anti-Fraud and Anti-Corruption Policy
- Anti-Bribery Policy
- Anti-Money Laundering Policy
- Regulation of Investigatory Powers Act (RIPA) Policy and Procedures

2. REASON FOR RECOMMENDATION(S) AND OPTIONS CONSIDERED

- 2.1 The counter fraud policies have been refreshed to investigation activity complies with legislation and best practice
- 2.2 The Prosecution and Sanctions Policy is a high level policy which outlines the circumstances in which the council will prosecute or offer an alternative sanction.
- 2.3 The Anti-Fraud and Anti-Corruption Policy sets out the council's zero tolerance to fraud and the policy on the control of fraud and suspected fraud.
- 2.4 The Anti-Bribery policy outlines the key elements of the Bribery Act and the council's approach in ensuring it has adequate policies and procedures.
- 2.5 The Anti Money Laundering Policy specifies the council's Money Laundering Reporting Officer and outlines the council's procedures to prevent the use of services for money laundering.
- 2.6 The RIPA policy provides a framework for the use of covert investigatory techniques, ensuring that any covert activities are within the law. The policy also specifies the council's authorising officers.
- 2.7 As part of the Shared Audit and Investigation Service activity in 2016/17, anti-fraud training will be provided both at a strategic level and at an operational level, covering the main principles contained within the policies.

Option	Comments
(1) Approve the policies Recommended	This will ensure that activity undertaken by the Shared Audit and Investigation Service (SAIS) on behalf of the council, complies with legislation and industry best practice.
(2) Amend the policies.	May result in legal challenge through not complying with legislation or inefficiencies within the SAIS.
(3) Not to approve the policies.	May result in legal challenge through not complying with legislation or inefficiencies within the SAIS.

3. KEY IMPLICATIONS

Defined Outcomes	Unmet	Met	Exceeded	Significantly Exceeded	Date they should be delivered by
Residents have confidence that that the Council takes fraud and corruption seriously and that the Council's assets are safeguarded from misappropriation / loss.	<p>Financial losses to the Council are not identified and recovered.</p> <p>Failure of the Council to discharge its responsibilities as set out in the Council Constitution</p> <p>Loss of residents confidence.</p> <p>Council reputation may be affected.</p>	<p>Financial losses are identified and recovered.</p> <p>Gain residents confidence.</p> <p>Council discharges its responsibilities as set out in the Constitution</p> <p>Council reputation protected.</p>	N/A	N/A	Ongoing

4. FINANCIAL DETAILS

Financial impact on the budget

Revenue - Officer time in dealing with updating the Counter Fraud Policies. The proposal relates to existing budgets, no new funds are being sought.

Capital - None

5. LEGAL IMPLICATIONS

5.1 Relevant legislation includes:

- Corruption Act 1906
- Criminal Procedures and Investigations Act (CPIA) 1996;
- Data Protection Act 1998;
- Fraud Act 2006;
- Freedom of Information Act 2000;
- Human Rights Act 1998;
- Local Government Finance Act 1992;
- Police and Criminal Evidence Act (PACE) 1984;
- Proceeds of Crime Act 2002;
- Regulation of Investigatory Powers Act (RIPA) 2000; and
- Bribery Act 2010

6. VALUE FOR MONEY

6.1 Counter Fraud work is planned to assist the Council in ensuring that its assets are safeguarded against misappropriation, loss and fraud.

7. SUSTAINABILITY IMPACT APPRAISAL – N/A

8. RISK MANAGEMENT

Risks	Uncontrolled Risk	Controls	Controlled Risk
Failure to have and follow appropriate fraud policies leads to none compliance with the Council's zero tolerance approach which could result in a decrease in the recovery of identified losses and potential reputational damage.	High	Appropriate Counter Fraud policies are in place, have been approved and are followed.	Low

9. LINKS TO STRATEGIC OBJECTIVES

9.1 Counter Fraud policies help the Council achieve its objectives by safeguarding it's assets from misappropriation, loss or fraud.

10. EQUALITIES, HUMAN RIGHTS AND COMMUNITY COHESION – N/A

11. STAFFING/WORKFORCE AND ACCOMMODATION IMPLICATIONS – N/A

12. PROPERTY AND ASSETS – N/A

13. ANY OTHER IMPLICATIONS – N/A

14. CONSULTATION

14.1 Consultations have been undertaken with the Managing Director, CMT and the S151 Officer in updating the Counter Fraud Policies.

15. TIMETABLE FOR IMPLEMENTATION

Date	Details
17/2/16	Policies will be implemented with immediate effect.

16. APPENDICES

- Appendix A - Prosecution and Sanctions Policy
- Appendix B - Anti-Fraud and Anti-Corruption Policy
- Appendix C - Anti-Bribery Policy
- Appendix D - Anti-Money Laundering Policy
- Appendix E - Regulation of Investigatory Powers Act (RIPA) Policy and Procedures

17. BACKGROUND INFORMATION

17.1 Previous versions of the above mentioned policies.

18. CONSULTATION (MANDATORY)

Name of consultee	Post held and Department	Date sent	Date received	See comments in paragraph:
Internal				
Alison Alexander	Managing Director	27/01/2016		
Corporate Management Team (CMT)	Managing Director, All Strategic Directors, Head of Finance	27/01/2016		
Legal Services		18/01/2016		
Human Resources		18/01/2016		
Cllr Brimacombe		08/02/2016		

REPORT HISTORY

Decision type:	Urgency item?
Non-key decision	No

Full name of report author	Job title	Full contact no:
Catherine Hickman	Service Manager, Shared Audit and Investigation Service	07917265742

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD
CORPORATE PROSECUTION AND SANCTION POLICY

Introduction

The Royal Borough of Windsor and Maidenhead will prosecute any person who commits a criminal offence against the systems, processes and functions of the Council and/or assaults or threatens any member or employee of the Council, if there is sufficient evidence and if, in the opinion of the Council, it is in the public interest to do so.

When deciding if it is in the public interest, all officers authorised to decide whether to prosecute on behalf of the Council will be guided by the Code for Crown Prosecutors. Whenever it is appropriate, the Council will consider offering other sanctions as an alternative to prosecution.

The Council will consider each case on its own merits before deciding whether or not to prosecute. If it is the case that the Council has suffered a material/financial loss, it may take separate action to stop further payments/ recover money, irrespective of whether it decides to take criminal proceedings, and where steps to prevent further losses or recover losses already incurred are not available or desirable in the course of any criminal proceedings.

Alternatives to Prosecution - Cautions

In the issuing of Cautions the Council will be guided by the relevant statutory Guidance, currently the Ministry of Justice – Simple Caution for Adult Offender guidance.

Alternatives to Prosecution - Statutory Sanctions

The Council may consider a Statutory Sanction, whether a monetary penalty or otherwise, as an alternative to prosecution for an offence where the imposition or offer of such a sanction for the specified offence or offences is prescribed by law.

Code for Crown Prosecutors – The Evidential Test

When making a decision on whether to prosecute, the Council will first consider whether there is sufficient evidence:

- a) is there sufficient evidence of the commission of an offence to provide a realistic prospect of conviction? And
- b) is the evidence reliable and able to be used in court?

Code for Crown Prosecutors – The Public Interest Test

Once the Evidential Test has been satisfied, the Council will then consider whether the Public Interest Test is satisfied. The Public Interest Test will be assessed following the guidance in the “Code for Crown Prosecutors” to ensure that any prosecution is in the public interest.

Other Sanctions or Penalties

Where a person engages in conduct which is not criminal, but is otherwise prohibited by legal statute or regulation applicable to the functions of the Council, or fails in their legal obligation to the Council, the Council may consider the imposition or offer of a sanction or monetary penalty where to impose a monetary penalty or sanction for the given circumstances is prescribed by law.

**ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD
CORPORATE ANTI-FRAUD AND ANTI-CORRUPTION POLICY**

1. INTRODUCTION

The Royal Borough of Windsor and Maidenhead ('RBWM', 'The Council') aims to deliver high quality services and provide value for money by being fully accountable, honest and open in everything that it does.

Fraud and corruption undermine these aims by diverting resources from legitimate activities, damaging public confidence in the Council and adversely affecting staff morale.

To achieve its strategic priorities, the Council seeks to ensure that measures are taken to prevent, detect and investigate fraudulent or corrupt acts. The aim of this policy is to reduce losses from fraud and corruption to an absolute minimum.

The Council has a zero tolerance policy regarding fraud and corruption. It has adopted the following approach.

"In administering its responsibilities the Council is opposed to fraud and corruption whether it is attempted on or from within the Council and is committed to preventing, deterring, detecting and investigating fraud and corruption."

This policy is particularly relevant to:

- a) elected Members;
- b) employees;
- c) contractors;
- d) consultants;
- e) suppliers;
- f) service users;
- g) customers (including the public); and
- h) partner organisations.

2. DEFINING FRAUD

The Council defines "fraud" as an intentional distortion of financial statements or other records by persons internal or external to the organisation which is carried out to conceal the misappropriation of assets or otherwise for financial gain. This may involve, but is not limited to:

- a) falsification or alteration of accounting records or other documents;
- b) misappropriation of assets or theft;

- c) suppression or omission of the effects of transactions from accounting records of other documents;
- d) recording transactions which have no substance; and
- e) wilful misrepresentation of transactions or of the Council's state of affairs.

Furthermore, the Fraud Act 2006 has defined fraud in law, defining it in three classes:

- a) fraud by false representation;
- b) fraud by failing to disclose information; and
- c) fraud by abuse of position.

3. DEFINING CORRUPTION

The Council defines corruption as the offering, giving, soliciting or accepting of any inducement or reward which would influence the actions taken by the Council, its Members or Officers. Areas where corrupt practices may occur include, but are not limited to:

- a) tendering and awarding of contracts;
- b) pecuniary interests of Members and Officers;
- c) the award of permissions, planning consents and licenses; and
- d) the disposal of assets.

4. FRAMEWORK FOR PREVENTION AND DETECTION

It is a management responsibility to maintain the internal control system and to ensure that the Council's resources are properly applied in the manner and on the activities intended. This includes responsibility for the prevention and detection of fraud and other illegal acts.

5. KEY PRINCIPLES AND CULTURE

The Council will not tolerate fraud and corruption in the administration of its responsibilities whether from inside or outside of the authority. The Council is committed to creating a culture of opposition to fraud and corruption. The Council is determined that the authority meets the expectations of the Committee on Standards of Public Life and is committed to the ten general principles which govern standards of conduct in local government, namely:

- a) selflessness;
- b) honesty and integrity;
- c) objectivity;
- d) accountability;
- e) openness;

- f) personal judgement;
- g) respect for others;
- h) duty to uphold the law;
- i) stewardship; and
- j) leadership.

The Council expects Members (elected and co-opted) and employees (including agency staff, consultants and contractors) to lead by example in ensuring effective opposition to fraud and corruption. This includes ensuring adherence to legislation, local rules and regulations, National and Local Codes of Conduct and that all procedures and practices are beyond reproach.

6. RAISING CONCERNS

Employees at all levels should be alert to the possibility of fraud and corruption. They are expected, and positively encouraged to raise any concerns relating to fraud and corruption which they become aware of. These can be raised in any way that the employee prefers, including with their line manager, through a Strategic Director, with the Shared Audit and Investigation Service or through the Council's Whistleblowing (*'Raising concerns at work'*) Policy. Whichever route is chosen, the employee can be assured that concerns raised in good faith will be fully investigated and, wherever possible, those raising concerns will be dealt with in confidence.

When management receive concerns from employees or others regarding potential fraud or corruption, they should immediately contact the Service Manager- Shared Audit and Investigation Service with details of the concerns. The Service Manager- Shared Audit and Investigation Service will make preliminary enquiries and in consultation with the Section 151 will determine whether there are grounds for an investigation.

Councillors, service users, suppliers, partner organisations and members of the public are encouraged to report any concerns. These concerns about fraud and corruption should be reported either directly to the Service Manager- Shared Audit and Investigation Service or via the Council's Whistleblowing Policy.

If employees feel that they are unable to use internal routes then they can contact the council's external auditors:

KPMG LLP
Darren Gilbert
100 Temple Street,
Bristol
BS1 6AG

Darren.Gilbert@KPMG.co.uk

Although the Council encourages its staff to report concerns acting in good faith, any maliciously motivated and unfounded allegations may be dealt with through the Council's disciplinary code.

7. CORPORATE GOVERNANCE

The main corporate policies and procedures which formulate the Council's framework for minimising risk and the prevention of fraud and corruption include:

- a) Anti-Fraud and Anti-Corruption Strategy
- b) Internal Audit Charter
- c) Contract Procedure Rules
- d) Finance Procedure Rules
- e) Human Resources Disciplinary Policy and Procedure
- f) Human Resources Code of Conduct for Employees
- g) Human Resources Recruitment and Selection Code of Practice
- h) Members' Code of Conduct
- i) Anti-Money Laundering Policy
- j) Officers' Code of Conduct;
- k) Prosecution and Sanction Policy;
- l) Risk Management Policy and Strategy
- m) Scheme of Delegation
- n) Whistleblowing Policy; and
- o) Anti-Bribery Policy

8. CORPORATE RESPONSIBILITY

Heads of Service must ensure that all employees in their service are familiar with the corporate policies and procedures listed above, in addition to any other relevant rules and regulations specific to their service. Failure to adhere to these policies and procedures could result in the instigation of disciplinary procedures.

9. RECRUITMENT

The Council recognises that one of the most important issues relating to the prevention of fraud and corruption is the effective recruitment of staff and therefore takes pre-employment screening seriously.

Employee recruitment is required to be in accordance with procedures laid down by the Head of Human Resources. As part of these procedures, particular reference is made to:

- a) verifying the identity of the applicant;

- b) obtaining satisfactory references prior to appointment;
- c) verifying the applicant is able to legitimately work in the UK;
- d) verifying and retaining copies of certificates for stated qualifications;
and
- e) undertaking Disclosure and Barring Service checks, where appropriate.

These practices apply to all permanent appointments including those where employees have entered the organisation as an agency worker or consultant in the first instance.

10. SYSTEM OF INTERNAL CONTROL

The risk of fraud and corruption can be minimised by good financial management, sound internal control systems, effective management supervision, and by raising public, member and employee awareness of fraud.

Internal control is the whole system of controls, financial and otherwise, established to provide reasonable assurance of:

- a) proper aims and objectives;
- b) efficient and effective operations;
- c) reliable management information and reporting;
- d) legitimate expenditure;
- e) compliance with laws and regulations;
- f) performance management; and
- g) security of assets and income.

Weaknesses in the design and operation of administrative and financial internal control systems may increase the risk of fraud. Systems should contain efficient, effective, and well documented internal controls that cover the following:

- a) adequate segregation of duties;
- b) proper authorisation and approval procedures;
- c) adequate physical security over assets; and
- d) reliable monitoring and reporting arrangements.

It is management's responsibility to install adequate internal controls and rectify weaknesses if they occur. To help management discharge this responsibility, systems may be subject to review by both Internal and External Audit. Auditors are responsible for reporting to management on significant weaknesses in the control environment, including deficiencies in the operation of internal controls and highlighting exposure to the risk of fraud. Audit concerns are promptly followed up to ensure issues highlighted are appropriately actioned.

Management should instigate occasional deterrent compliance checks on the operation of internal controls within their service and are encouraged to seek advice from the Shared Audit and Investigation Service on what checks should be carried out. This work should be used to inform the Annual Governance Statement.

11. RISK MANAGEMENT

Major fraud risks relating to services should be included within Service Risk Registers and subject to regular review to ensure that appropriate controls are in place to mitigate those risks.

12. ROLE OF STATUTORY OFFICERS

The Council has a statutory responsibility, under Section 151 of the Local Government Act 1972, to ensure the proper administration of its financial affairs and also to nominate one of its Officers to take responsibility for those affairs. The Council's nominated Section 151 Officer is the Head of Finance.

The Council's Monitoring Officer is responsible under Section 5 of the Local Government and Housing Act 1989 to guard against, inter alia, illegality, impropriety and maladministration in the Council's affairs.

13. EFFECTIVE ACTION

Responsibility for investigating suspected fraud and corruption against the Council rests with the Shared Audit and Investigation Service. This is to ensure that the investigation is performed only by properly trained officers in accordance with the appropriate legislation:

- a) Corruption Act 1906
- b) Criminal Procedures and Investigations Act (CPIA) 1996;
- c) Data Protection Act 1998;
- d) Fraud Act 2006;
- e) Freedom of Information Act 2000;
- f) Human Rights Act 1998;
- g) Local Government Finance Act 1992;
- h) Police and Criminal Evidence Act (PACE) 1984;

- i) Proceeds of Crime Act 2002; and
- j) Regulation of Investigatory Powers Act (RIPA) 2000
- k) The Council Tax (Administration and Enforcement) Regulations 1992.

14. PROCEDURE

All referrals will initially be risk assessed and material instances of fraud or irregularity in the Council will be referred to the Shared Audit and Investigation Service.

The Shared Audit and Investigation Service will ensure the following objectives are met:

- a) investigations are undertaken fairly, objectively and in accordance with relevant laws and regulations, so as to avoid jeopardising the outcome on legal and procedural technicalities;
- b) to protect the evidence;
- c) to prove or disprove the original suspicions of fraud;
- d) if proven, to support the findings by producing effective evidence;
- e) to present evidence in an appropriate format accepted by the Crown Prosecution Service or the appropriate disciplining service; and
- f) to apply appropriate sanctions and redress against those individuals and organisations that seek to defraud.

15. COMPLETION

Once an investigation is completed the Shared Audit and Investigation Service may have responsibilities in relation to:

- a) recommending improvements to systems;
- b) attendance at disciplinary hearings and tribunals;
- c) attendance at Court as a witness; and
- d) reporting to the Audit and Performance Review Panel.

Conclusions will be based on fact allowing management to take forward any required disciplinary and/or criminal proceedings as they determine appropriate.

16. DISCIPLINARY

The Council has in place disciplinary procedures which must be followed whenever staff are suspected of committing a fraudulent or corrupt act.

The disciplinary procedures are set out and available on Hyperwave. The Managing Director has overall responsibility for ensuring that the disciplinary procedure is managed effectively. Line managers, under the overall direction of Heads of Service are responsible for day to day management and ensuring compliance with disciplinary policies and procedures.

17. REPORTING AND PUBLICITY

Incidents of fraud and corruption are reported through the following mechanisms:

- a) Corporate Management Team;
- b) Audit and Performance Review Panel; and
- c) External Auditors (currently KPMG).

Where evidence of fraud and corruption is found, appropriate sanctions will be sought in line with the Council's Prosecution and Sanctions Policy. The details of any proven act of fraud or corruption, including action taken by the Council will be publicised to employees, Members and the public. This is aimed at deterring further attempts of fraud or corruption by demonstrating the seriousness with which the Council views such cases. In agreement with the Section 151 Officer and the Monitoring Officer, the Council will report criminal activity to the Police at the appropriate stage.

18. COUNCIL TAX INVESTIGATIONS

The Investigation Team within the Shared Audit and Investigation Service is also responsible for undertaking investigations within the Council Tax Reduction Scheme. This involves:

- a) investigating suspected fraud by false statement and/or failure to declare changes in circumstances or other method;
- b) making random checks on claimants; and
- c) maximising recovery of overpayments.

Where evidence of fraud and corruption is found, appropriate sanctions will be sought in line with the Council's Prosecution and Sanctions Policy. Successful prosecutions will be publicised to help deter further fraud.

19. WORKING WITH OTHERS

Arrangements are in place and continue to develop and encourage the exchange of information between the Council and other agencies on national and local fraud and corruption activity. This includes participation in the National Fraud Initiative which matches data across a wide range of public service organisations in order to detect fraud or erroneous payments.

20. MONEY LAUNDERING

Money laundering is the process of moving illegally generated funds through a cycle of transformation in order to create the end appearance of legitimately earned funds.

The Proceeds of Crime Act 2002 details the three principal money laundering offences as:

- a) assisting another to retain the benefit of crime;
- b) acquisition, possession or use of criminal proceeds; and
- c) concealing or transferring proceeds to avoid prosecution.

In addition there are related offences for failing to report where a person has knowledge, suspicion or reasonable grounds for knowledge or suspicion that money laundering has taken place, as well as for tipping off a person that a disclosure has taken place.

Council Officers and Members who suspect money laundering activities should report their concern to the Council's nominated Money Laundering Reporting Officer (MLRO), the Section 151 Officer (Head of Finance). Further details are contained in the Anti-Money Laundering Policy.

21. CONCLUSION AND REVIEW

The Council has in place a clear framework of systems and procedures to deter and investigate fraud and corruption. It will ensure that these arrangements are fair and are monitored and updated to keep pace with future developments in preventative, deterrent and detection techniques regarding fraudulent or corrupt activity.

To this end, the Council maintains a continuous review of these arrangements through, in particular the Audit and Performance Review Panel, the Section 151 Officer (Head of Finance), Shared Audit and Investigation Service, External Audit and the Monitoring Officer.

**ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD
ANTI-BRIBERY POLICY**

1. POLICY STATEMENT

Bribery is a criminal offence. We do not, and will not, pay bribes or offer improper inducements to anyone for any purpose, nor do we or will we, accept bribes or improper inducements.

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

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

2. OBJECTIVE

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

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

- a) act honestly and with integrity at all times and to safeguard the Council’s resources for which they are responsible; and
- b) comply with the spirit, as well as the letter, of the laws and regulations of all jurisdictions in which the Council operates, in respect of the lawful and responsible conduct of activities.

3. SCOPE

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

Within the Council, the responsibility to control the risk of bribery occurring resides at all levels, in every service.

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

4. COMMITMENT

The Council commits to:

- a) setting out a clear anti-bribery policy and keeping it up to date;
- b) making all employees aware of their responsibilities to adhere strictly to this policy at all times;
- c) training all employees so that they can recognise and avoid the use of bribery by themselves and others;
- d) encouraging its employees to be vigilant and to report any suspicions of bribery, providing them with suitable channels of communication and ensuring sensitive information is treated appropriately;
- e) rigorously investigating instances of alleged bribery and assisting police and other appropriate authorities in any resultant prosecution;
- f) taking firm and vigorous action against any individual(s) involved in bribery;
- g) provide information to all employees to report breaches and suspected breaches of this policy;
- h) include appropriate clauses in contacts to prevent bribery.

5. THE BRIBERY ACT

The Bribery Act defines bribery as ‘an inducement or reward offered, promised or provided to gain personal, commercial, regulatory or contractual advantage’.

There are four key offences under the Act:

- a) bribery of another person (section 1);
- b) accepting a bribe (section 2);
- c) bribing a foreign official (section 6); and
- d) failing to prevent bribery (section 7).

The Bribery Act 2010 (http://www.opsi.gov.uk/acts/acts2010/ukpga_20100023_en_1) makes it an offence to offer, promise or give a bribe (Section 1). It also makes it an offence to request, agree to receive, or accept a bribe (Section 2). Section 6 of the Act creates a separate offence of bribing a foreign public official with the intention of obtaining or retaining business or an advantage in the conduct of business. There is also a corporate offence under Section 7 of failure by a commercial organisation to prevent bribery that is intended to obtain or retain business, or an advantage in the conduct of business, for the organisation. An organisation will have a defence to this corporate offence if it can show that it had in place adequate procedures designed to prevent bribery by or of persons associated with the organisation.

The guidance states that a “commercial organisation” is any body formed in the United Kingdom and “...it does not matter if it pursues primarily charitable or educational aims or purely public functions. It will be caught if it engages in commercial activities, irrespective of the purpose for which profits are made.” Therefore, we are a “commercial organisation”.

6. ADEQUATE PROCEDURES

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

7. PROPORTIONATE PROCEDURES

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

8. TOP LEVEL COMMITMENT

The Managing Director, Strategic Directors and Members are committed to preventing bribery by persons associated with it. Bribery is never acceptable.

9. RISK ASSESSMENT

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

10. DUE DILLIGENCE

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

11. COMMUNICATION

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

12. MONITORING AND REVIEW

The Council monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary. The Council is committed to proportional implementation of these principles.

13. PENALTIES

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

- a) on conviction in a magistrates court, to imprisonment for a maximum term of 12 months (six months in Northern Ireland), or to a fine not exceeding £5,000, or to both;
- b) on conviction in a crown court, to imprisonment for a maximum term of ten years, or to an unlimited fine, or both.

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

14. BRIBERY IS NOT TOLERATED

It is unacceptable to:

- a) give, promise to give, or offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- b) give, promise to give, or offer a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;
- c) accept payment from a third party that you know or suspect is offered with the expectation that it will obtain a business advantage for them;
- d) accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by us in return;
- e) retaliate against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy;
- f) engage in activity in breach of this policy.

15. FACILITATION PAYMENTS

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

16. GIFTS AND HOSPITALITY

The Council's Gifts and Hospitality guidance notes are held on the 'Declaration of the Offer/Receipt of Gifts and Hospitalities Guidance Notes' form. Additional guidance is held in the Anti-Fraud and Anti-Corruption Guidance Notes for Employees. In determining whether to accept a gift or hospitality employees should consider the following:

- Whether the company or individual is seeking a contract;
- Whether the company or individual regularly submits, has submitted, is likely to or is in the process of submitting a planning application, or has been granted planning permission;
- Whether a contract with the company/individual is under negotiation;
- Whether the final contract sum has been agreed;
- Whether the hospitality is genuinely instructive or constitutes more of a social function;
- The level and location of the hospitality;
- The frequency of the hospitality;
- Whether it is directed at you or to a group.

Officers are required to make a declaration within 28 days of receiving or being offered any gift or hospitality over the value of £25.00.

As a general rule it is always wise to err on the side of caution. Any gift that is clearly expensive or hospitality excessive should raise questions with you and should be declined. The offer, however, should still be recorded. You should always consider how such a gift or hospitality could be perceived by others. If you are in any doubt, and for your own protection, you should seek advice from your Service Manager or ultimately from your Strategic Director. There are some instances where gifts and hospitality must not be accepted. These are when dealing with planning applications, negotiating a contract and before a final contract sum is agreed. The overriding guidance to take account of is 'when in doubt, opt out'.

The phrase 'gifts and hospitality' includes the following. However, this list is intended to be illustrative rather than exhaustive:

- Lunches;
- Presents e.g. drink, food, diaries, calendars, stationary, tickets for events;
- Cash, cheques or any other form of reward;
- Being paid or paid for to go anywhere (inside and outside of working hours)
- Visits abroad
- Hospitality tents

The general procedures to be followed in considering whether or not to accept or offer gifts and hospitality is as follows: Receiving:-

- All gifts and hospitality offered, whether received or not, must be recorded and entered in your Directorate's 'Register of Gifts and Hospitality' held by your Strategic Director.
- All hospitality, wherever possible, should be agreed beforehand by your Strategic Director.
- If you find yourself stuck in an awkward situation and unable to get authorisation beforehand, register the acceptance of the gift or hospitality if at all possible, pay for yourself, and then discuss with your Strategic Director whether it is appropriate for the Council to reimburse these expenses.
- Only modest gifts including gifts of a promotional nature e.g. calendars, diaries etc, and gifts of a sort normally given out by that company are acceptable.
- Fees and rewards, whether cash, cheques or air miles, other than as part of your proper remuneration are not acceptable.
- Gifts offered but not received should be returned with a polite and courteous explanation. The same applies to when hospitality has to be declined. In this instance the company should be courteously informed of our procedures and standards.

Giving:-

- All gifts and hospitality given must be registered in the 'Register of Gifts and Hospitality' held by your Strategic Director.
- No cash or cheques should be given.
- It is not normal for gifts to be given, except as part of a promotion or marketing initiative, therefore if you wish to express your gratitude by the way of a gift you must seek prior approval from your Strategic Director.
- Any hospitality to be given out, beyond normal working lunch, should also be agreed beforehand by your Strategic Director. If you are in any doubt you should seek advice from your Strategic Director.

17. PUBLIC CONTRACTS AND FAILURE TO PREVENT BRIBERY

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

18. STAFF RESPONSIBILITIES

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

Staff must:

- a) ensure that you read, understand and comply with this policy; and
- b) raise concerns as soon as possible if you believe or suspect that a conflict with this policy has occurred, or may occur in the future.
- c) As well as the possibility of civil and criminal prosecution, staff that breach this policy will face disciplinary action, which could result in dismissal for gross misconduct.

19. RAISING A CONCERN

The Council is committed to ensuring that we all have a safe, reliable, and confidential way of reporting any suspicious activity. We want each and every member of staff to know how they can raise concerns. We all have a responsibility to help detect, prevent and report instances of bribery. If you have a concern regarding a suspected instance of bribery or corruption, please speak up – your information and assistance will help. The sooner you act, the sooner it can be resolved.

There are multiple channels to help you raise concerns – these are explained in the Raising Concerns at Work (Whistleblowing) Policy. Staff who refuse to accept or offer a bribe, or those who raise concerns or report wrongdoing can understandably be worried about the repercussions. We aim to encourage openness and will support anyone who raises a genuine concern in good faith under this policy, even if they turn out to be mistaken.

We are committed to ensuring nobody suffers detrimental treatment through refusing to take part in bribery or corruption, or because of reporting a concern in good faith. If you have any questions about these procedures, please contact the Service Manager, Shared Audit and Investigation Service, Catherine Hickman.

20. OTHER RELEVANT RBWM POLICIES

Anti-Fraud and Anti-Corruption Policy, Anti-Money Laundering Policy, Raising Concerns at Work (Whistleblowing) Policy, Codes of Conduct, Contract Procedure Rules and Finance Procedure Rules.

**ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD
ANTI-MONEY LAUNDERING POLICY**

1. INTRODUCTION

Money laundering legislation requires local authorities to establish internal procedures to prevent the use of their services for money laundering. Money laundering legislation in the UK is primarily governed by the following legislation:

- a) the Terrorism Act 2000;
- b) the Anti-Terrorist Crime & Security Act 2001;
- c) the Proceeds of Crime Act 2002;
- d) Serious Organised Crime and Police Act 2005; and
- e) the Money Laundering Regulations 2007.

2. SCOPE OF THIS POLICY

This Policy applies to all employees and contractors of the Council. The Policy sets out the procedures that must be followed to enable the Council to comply with its legal obligations.

Staff should report any suspicions to the appointed Money Laundering Reporting Officer (MLRO) and it is for the MLRO to consider if the circumstances warrant the completion of a 'suspicious activity report' (SAR), which is sent to the National Crime Agency.

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

3. WHAT IS MONEY LAUNDERING?

The legislation is not limited to major organised crimes, but covers proceeds of all crimes, however small. The primary money laundering offences and thus prohibited acts under the legislation are:

- a) concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the 2002 Act); or
- b) entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328 of the 2002 Act); or
- c) acquiring, using or possessing criminal property (section 329 of the 2002 Act); or
- d) becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorist Act 2000); or

- e) failing to disclose suspected money laundering

The defence to these offences is to make an 'authorised disclosure' to an approved person. Approved persons are Customs Officers, Police Officers and the Council's Money Laundering Reporting Officer (MLRO).

4. SUSPICIOUS ACTIVITY

Some indications of suspicious activity are:

- a) any unusually large cash payment;
- b) any overpayment or duplicate payment in cash where the refund is requested by cheque; or
- c) if a 'third party' is involved in any transaction (e.g. someone paying cash to settle someone else's bill.)

The Council should be alert to large amounts of "Cash" accepted as a payment, which would normally arouse suspicion.

Officers involved in Treasury Management and cashiering activities are the most likely to encounter attempts to launder money but all staff should be alert to the possibilities.

All organisations and each individual is required by law to try to prevent and to report any attempts to 'launder' money (i.e. to use the proceeds of crime in apparently legitimate business transactions).

Potentially any member of staff could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it.

5. THE COUNCIL'S OBLIGATIONS

Organisations conducting "relevant business" must:

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

6. THE MONEY LAUNDERING REPORTING OFFICER

If you have any suspicions, you must contact the MLRO. The Council's nominated MLRO is the S151 Officer.

7. DISCLOSURE PROCEDURE

Reporting to the MLRO: Where you know or suspect that money laundering activity is taking/has taken place, or become concerned that your involvement in a matter may amount to a prohibited act under the legislation, you must disclose this as soon as practicable to the MLRO. The disclosure should be within “hours” of the information coming to your attention, not weeks or months later. **SHOULD YOU NOT DO SO, YOU MAY BE LIABLE TO PROSECUTION.**

Once you have reported the matter to the MLRO you must follow any directions they may give you. You must NOT make any further enquiries into the matter yourself: Any necessary investigation will be undertaken by the National Crime Agency (NCA).

Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if the SOCA or NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO; otherwise you may commit a criminal offence of “tipping off”. Do not, therefore, make any reference on a client file to a report having been made to the MLRO – should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

On receipt of the disclosure the MLRO will:

- a) consider the report and make such further enquiries as are necessary to form a view on whether a person is engaged in money laundering;
- b) consider all other relevant information in making this judgement;
- c) ensure that nothing is done which could alert the person or business concerned that a report and an investigation could ensue;
- d) make a report to SOCA, if appropriate, making full notes of the reasons for doing so;
- e) co-operate with any enquiries made by the proper authorities; and
- f) maintain all records of disclosures and reports for at least five years.

8. CLIENT IDENTIFICATION PROCEDURE

Each section of the Council conducting relevant business where a business relationship is to be established and an account is to be opened or a one-off transaction or series of linked transactions amounting to 15,000 Euros (approximately £10,000) or more must maintain procedures which:

- a) require satisfactory evidence of the identity of both internal and external clients at the outset of the matter;

- b) require that if satisfactory evidence of identity is not obtained at the outset of the matter then the business relationship or one off transaction(s) cannot precede any further;
- c) recognise the greater potential for money laundering when the client is not present; and
- d) require that where a client appears to act for another that reasonable measures are taken to establish the identity of that person.

Staff involved in Treasury Management should ensure that all dealings are carried out in accordance with the Treasury Management Strategy and Treasury Management Policies which ensure that transactions are only undertaken with approved counterparties.

9. RECORD KEEPING PROCEDURE

Each service of the Council conducting relevant business must maintain records for at least five years of:

- a) client identification evidence obtained; and
- b) details of all relevant business transactions carried out for clients

The precise nature of the records is not prescribed by law however they must be capable of providing an audit trail.

10. FURTHER INFORMATION AND ADVICE

For any further information or guidance, please contact the MLRO (S151 Officer)

RIPA PROCEDURE

Effective from February 2016

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) - GUIDANCE

1.0 Background Information

- 1.1 The Regulation of Investigatory Powers Act (RIPA) provides a framework for the use of covert investigatory techniques by public authorities. It does not provide any powers to carry out covert activities but regulates the use of these techniques so that they are compatible with human rights legislation. Special authorisation arrangements need to be put in place whenever the Local Authority considers commencing a covert surveillance or obtaining information by the use of informants or officers acting in an undercover capacity.
- 1.2 Local Authorities do operate covert activities in a number of key areas. Activities can include covert surveillance in relation to internal audit and personnel where fraud, deception or gross misconduct by staff might be suspected, or as part of a benefit fraud, Environmental Health or Trading Standards investigation. The legal requirements are now supplemented by codes of practice issued by the Home Office for certain surveillance activities (covert surveillance activity and covert human intelligence sources), breaches of which can be cited in Court as evidence of failure to abide by the requirements of RIPA. This may mean that the evidence obtained by that surveillance is excluded.
- 1.3 This policy applies to all employees of Royal Borough of Windsor and Maidenhead, and **also to those companies or individuals working on our behalf.**
- 1.4 From 1 November 2012, two significant changes have been made governing how local authorities use RIPA:
- Approval of Local Authority Authorisations under RIPA by a Justice of the Peace: The amendments in the Protection of Freedoms Act 2012 will mean that local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).
 - Directed surveillance crime threshold: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.
- 1.5 **Surveillance** – includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

- 1.6 **Covert Surveillance** – This is carried out to ensure the person who is the subject of the surveillance is unaware that it is or may be taking place. The provisions of RIPA apply to the following forms of covert surveillance:
- **Intrusive Surveillance** is a covert activity carried out in a residential place or a private vehicle by a person or a surveillance device being present in the premises or vehicle. Local authorities are not allowed to use this type of surveillance.
 - **Directed Surveillance** is a covert activity that is not intrusive, but carried out in support of a specific operation or investigation, likely to result in obtaining private information about any person.
 - **Covert Human Intelligence Source (CHIS)** is an undercover operation whereby an informant or undercover officer establishes or maintains some sort of relationship with the persons in order to obtain private information.
- 1.7 Covert surveillance carried out by the council must be **authorised, necessary and proportional**. The only exception to this being where the surveillance is carried out by way of an immediate response to events, which were unforeseeable and impractical to obtain prior authorisation. Surveillance:
- includes monitoring, observing or listening to persons, their movements, conversations or other activities;
 - Is only covert if it is carried out in a manner that ensures that any persons who are the subject to the surveillance are unaware that it is taking place;
 - May either be – Intrusive, Directed or Covert Human Intelligence Source (CHIS).
- 1.8 **Private information** includes any information relating to a person's private or family life. Generally taken to include; any aspect of a person's private or personal relationships with others, including family and professional or business relationships: personal data, names, telephone numbers and address details.
- 2.0 **Compliance**
- 2.1 From 1st November 2012 covert surveillance which is directed surveillance will only fall within the scope of the RIPA when the crime the activity will 'prevent or detect' meets the 'serious crime' threshold.
- 2.2 This threshold is met where:
- a) The offence the activity seeks to prevent or detect is punishable by imprisonment for a period of at least 6 months or more, or
 - b) The activity is related to the prevention or detection of offences concerning the supply of alcohol or tobacco to persons under 18 years of age. Directed surveillance that does not meet one of these tests will fall outside the scope of the RIPA. In this instance specific authorisation must be sought from the Council's Monitoring Officer before the activity can take place.
- 3.0 **The Policy**
- 3.1 The Council's policy provides the procedures on which it may authorise the use of surveillance for a range of activities relating to the detection of: abuse, fraud, theft and other criminal offences. Legislation regulates the use of covert activities by Local Authorities. The Home Office also issue Codes of Practice that must be followed.

- 3.2 Directed surveillance must be authorised prior to it taking place, be subject to regular review and must be shown to be necessary and proportionate. RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance.

- 3.3 All non-intrusive covert surveillance and CHIS requires prior authorisation by the appropriate Local Authority Officer (as set out in this policy) before any surveillance activity takes place. The only exception to this is where covert surveillance is undertaken by way of an immediate response to events that means it was not foreseeable and not practical to obtain prior authorisation.
- 3.4 All requests for covert surveillance must be submitted (using only the prescribed forms) supported by the relevant authorising officers. The Council's authorising officers are:
- S151 Officer
 - Monitoring Officer
 - Enforcement Principal
- 3.5 The RIPA Coordinator is **Julie Holland (Shared Audit and Investigation Service)**, email julie.holland@wokingham.gov.uk.
- 3.6 The authorising officer will check to make sure the surveillance is, necessary and has a proportionate response to the purpose of the operation or investigation (this will be done in liaison with the relevant Head of Service). The authorising officers should send a copy of the authorisation to the RIPA Coordinator where it is included on a central register.
- 3.7 Once approved internally an application must be made for Judicial Approval before the activity concerned can commence. Shared Legal Solutions will provide advice on this part of the process.
- 3.8 Failure to comply with the policy may result in evidence obtained during an unauthorised operation or investigation being excluded in court and it may be a breach of the Human Rights Act 1998. The Investigatory Powers Tribunal is able to investigate complaints from anyone who feels aggrieved by a public authority's exercise of its powers under RIPA. Obtaining authorisation will ensure the Local Authority's actions are carried out in accordance with the law and satisfy the stringent and necessary safeguards against abuse.

4.0 Grounds of Necessity and Proportionality

- 4.1 The authorisation by itself does not ensure lawfulness, as it is necessary also to demonstrate that the interference was justified as both necessary and proportionate.
- 4.2 Once a ground for necessity is demonstrated, the person granting the authorisation must also believe that the use of an intelligence source or surveillance is proportionate, to what is aimed to be achieved by the conduct and use of that source or surveillance. This involves balancing the intrusive nature of the investigation or operation and the impact on the target or others who might be affected by it against the need for the information to be used in operational terms. Other less intrusive options should be considered and evaluated. All RIPA investigations or operations are intrusive and should be carefully managed to meet the objective in question and must not be used in an arbitrary or unfair way.
- 4.3 An application for an authorisation should include an assessment of the risk of any collateral intrusion i.e. the risk of obtaining private information about persons other than those directly targeted by the operation. Measures should be taken wherever practicable to avoid unnecessary intrusion into the lives of those not directly connected with the operation.
- 4.4 All applications must be renewed every 3 months and cancellation of authorisations should be requested as soon as possible i.e. as soon as the surveillance is no longer considered

necessary. Judicial approval is required for the renewal of an authorisation but it is not required for any internal review or cancellation.

- 4.5 All applications for authorisation and authorisations must be made in accordance with the procedure and on the appropriate forms. The forms can be obtained from the RIPA coordinator:

- RIPA Form 1 – Authorisation Directed Surveillance
- RIPA Form 2 – Review of a Directed Surveillance Authorisation
- RIPA Form 3 – Renewal of a Directed Surveillance Authorisation
- RIPA Form 4 – Cancellation of a Directed Surveillance Authorisation
- RIPA Form 5 – Application for Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)
- RIPA Form 6 – Review of a Covert Human Intelligence Source (CHIS) Authorisation
- RIPA Form 7 – Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation
- RIPA Form 8 – Cancellation of an Authorisation for the use or conduct of a Covert Human Intelligence Source (CHIS)
- RIPA Form 9 – Application request for Communications Data
- RIPA Form 10 – Application for a Judicial Order

- 4.6 All Directors have responsibility for ensuring that they have sufficient understanding to recognise when an investigation or operation falls within the requirements of RIPA. Authorising Officers will keep up to date with developments in the law and best practice relating to RIPA.
- 4.7 Authorising Officers must ensure full compliance with the RIPA Authorisation Procedure.
- 4.8 The role of the RIPA coordinator is to have day-to-day oversight of all RIPA authorisations and maintain a central register of all authorisations, review dates, cancellations and renewals.
- 4.9 All forms should be passed through the coordinator to ensure that there is a complete record of all authorisations, contents of the forms will be monitored to ensure they are correctly filled in and the coordinator will supply annual statistics to the Office of Surveillance Commissioners. All officers will co-operate fully with any inspection arranged by the Office of Surveillance Commissioners.

5.0 Communications Data

- 5.1 Part I of RIPA sets out these requirements. The Council can access certain communications data only “for the purpose of preventing or detecting crime or of preventing disorder”.
- 5.2 The Council is able to obtain certain details (e.g. name and address) of a telephone subscriber from communication service providers (CSP) such as: BT, Vodafone, Orange etc.
- 5.3 The applications to obtain communications data, must be made by a Home Office designated “Single Point of Contact (SPOC)”. Arrangements are in place to enable the authority to access communications data via a “SPOC”. Requests must be forwarded to Steve Johnson, Enforcement Principal who is the council’s SPOC. If the SPOC agrees the request is within the scope of RIPA he will make arrangements for the request to be processed.

6.0 Further information

- 6.1 Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance
<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary>
- 6.2 Home Office Code of Practice on the interception of communications.
[Code of practice for the interception of communications | Home Office](#)
- 6.3 Home Office Code of Practice on the acquisition and disclosure of communications data
[Code of practice for the acquisition and disclosure of communications data | Home Office](#)
- 6.4 Home Office Code of Practice on covert surveillance and property interference
[Code of practice for covert surveillance and property interference | Home Office](#)
- 6.5 Home Office Code of Practice on the use of covert human intelligence sources
[Code of practice for the use of human intelligence sources | Home Office](#)
- 6.6 Home Office Code of Practice for the investigation of protected electronic information
[Code of practice for the investigation of protected electronic information | Home Office](#)
- 6.7 The Regulation of Investigatory Powers Act 2000
[Regulation of Investigatory Powers Act 2000.](#)
- 6.8 RIPA Explanatory Notes
[Regulation of Investigatory Powers Act 2000 - Explanatory Notes](#)