BOROUGH COUNCIL OF WELLINGBOROUGH **AGENDA ITEM 7**

Resources Committee **1 February 2017**

Report of Head of Finance

COUNTER FRAUD AND CORRUPTION STRATEGY

1 Purpose of Report

1.1 To adopt a Counter Fraud and Corruption Strategy. This has been updated to meet current CIPFA guidelines.

2 Executive Summary

2.1 The updated strategy adheres to the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption 2014 (the Code). The Code requires leaders of public sector organisations to embed effective standards for countering fraud and corruption in their organisations to support good governance and demonstrate effective financial stewardship and strong public financial management.

2.2 The key elements of the strategy are to acknowledge and understand fraud risks, prevent and detect more fraud, and pursue fraudsters by punishing and recovering losses.

3. Appendices

3.1 The strategy document is attached at Appendix A.

4 Proposed Action: The committee is invited to RESOLVE that;

4.1 the Counter Fraud and Corruption Strategy attached at Appendix A is adopted.

5 Background

5.1 The Council has a corporate assurance framework of procedures and controls that set out best practice and contribute to the Council's counter-fraud and corruption efforts. Much of this framework is found within the constitution, however this strategy forms a key element of the framework.

5.2 The landscape surrounding counter fraud activities has changed rapidly over the past three years. In order to adapt to these changes it is necessary to update our

existing strategy to meet the current challenges and adopt the latest CIPFA best practice.

6 Discussion

6.1 The existing strategy was established in 2011. There have been significant changes to the landscape nationally covering counter fraud and anti-corruption activities since that date. CIPFA have established a counter fraud centre to support the establishment of best practice and to tackle the main fraud risks. To this end they have issued various strategic documents to support local authorities in bringing governance arrangements up to date.

6.2 Work has therefore been undertaken to update the Council's existing strategy. The updated strategy adheres to the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption 2014 (the Code). The Code and companion document Fighting Fraud and Corruption Locally (2016) requires leaders of public sector organisations to embed effective standards for countering fraud and corruption in their organisations to support good governance and demonstrate effective financial stewardship and strong public financial management.

6.3 The full strategy is produced at Appendix A.

6.4 The opportunity has also been taken to update the policy and procedures for the use of the Regulation of Investigatory Powers (RIPA) which form part of this strategy. This is following recommendation by the Assistant Surveillance Commissioner made during his inspection earlier in the year.

7 Legal Powers

7.1 Local Government Act 1972
7.2 The Local Government Act 1988
7.3 The Local Government Act 1999

8 Financial and Value For Money Implications

8.1 The strategy seeks to protect the Council's valuable resources by ensuring they are not lost through fraud but are used to provide services for borough residents.

9 Risk Analysis

Nature of risk	Consequences if realised	Likelihood of occurrence	Control measures
A strategy not based on current standards	Authority exposed to enhanced levels of risk or emerging fraud & corruption	Low	Periodic review of governance framework and appropriate strategies
Ineffective financial stewardship	Breach of financial control Loss of public funds / resources Reputational damage / intervention	Low	Governance framework Counter fraud & corruption measures External / internal audit review
Complacency to the occurrence of fraud & corruption	Perpetrators may consider targeting the organisation Loss of public funds / resources	Low	Robust leadership An organisational culture that is resilient to fraud Training and awareness

10 Implications for Resources

10.1 No implications foreseen.

11 Implications for Stronger and Safer Communities

11.1 None

12 Implications for Equalities

12.1 None

13 Author and Contact Officer

Nigel Robinson, Principal Revenue and Benefits Manager

14 Consultees

Liz Elliott, Head of Finance
Mark Watkins, Head of Internal Audit
Lorraine Coleman, Senior Human Resources Officer

15 Background Papers

CIPFA Code of Practice on Managing the Risk of Fraud and Corruption 2014
CIPFA Fighting Fraud & Corruption Locally –The Companion 2016

APPENDIX A

Borough Council of Wellingborough

Making Wellingborough a place to be proud of

COUNTER FRAUD AND CORRUPTION STRATEGY

December 2016

BOROUGH COUNCIL OF WELLINGBOROUGH

COUNTER FRAUD AND CORRUPTION STRATEGY

Contents

1.0 Introduction
2.0 Definitions
3.0 External scrutiny of Council Affairs
4.0 Statutory Responsibilities
5.0 Culture
6.0 Strategic aims and objectives
7.0 Managing the risk of fraud and corruption
8.0 Fighting Fraud Locally: Acknowledge – Prevent –Pursue
9.0 Reporting, Advice, Support
10.0 Money Laundering
11.0 External Auditors
12.0 Publicity and Training

Appendix A Action plan
Appendix B Seven principles of public life
Appendix C Anti-money Laundering Policy
Appendix D RIPA Policy

1. Introduction

1.1 Statement of intent

1.2 The Borough Council of Wellingborough takes the responsibility to protect the public purse very seriously and is fully committed to the highest ethical standards, in order to ensure the proper use and protection of public funds and assets. The Council needs to fully utilise the resources available to it and therefore has an ongoing commitment to be resilient to fraud, corruption and other forms of financial irregularity.

1.3 This Strategy adheres to the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption 2014 (the Code). Account has also been taken of the companion document Fighting Fraud and Corruption Locally 2016 which outlines good practice in tackling fraud risks. The Code requires leaders of public sector organisations to have a responsibility to embed effective standards for countering fraud and corruption in their organisations in order to support good governance and demonstrate effective financial stewardship and strong public financial management.

1.4 The five key principles of the code are to:

- acknowledge the responsibility of the governing body for countering fraud and corruption
- identify the fraud and corruption risks
- develop an appropriate counter fraud and corruption strategy
- provide resources to implement the strategy
- take action in response to fraud and corruption

1.5 In implementing these core principles the key elements of our response are to:

- **Acknowledge** and understand fraud risks. Committing support and resource to tackling fraud in order to maintain a robust anti-fraud response.
- **Prevent** and detect more fraud. Making better use of information and technology, enhancing fraud controls and processes and developing a more effective anti-fraud culture.
- **Pursue** fraudsters by punishing and recovering losses. Prioritising fraud recovery and the use of civil sanctions. Developing capability and capacity to punish fraudsters by collaborating across local authorities and with law enforcement.

1.6 This strategy aims to:

- provide a consistent framework for managers and Members, which enables effective deterrence, detection and investigation of fraud and corruption;

- detail the responsibilities of employees, leadership team, management and internal audit with regard to fraud and dishonesty;
- assist the Chief Financial Officer in fulfilment of duties under S.151 of the Local Government Act 1972 and the Monitoring Officer under the Local Government and Housing Act 1989

1.7 This strategy forms part of the Council's corporate assurance framework of procedures and controls which set out best practice and contribute to the Council's counter-fraud and corruption efforts. This framework, much of which is to be found within the Council's Constitution, includes:

- Financial Regulations and related procedure rules
- Contract Procedure Rules
- Procurement Policy and Strategy
- Officers' Code of Conduct
- Members' Code of Conduct
- Whistleblowing Policy
- Fraud and Corruption Action Plan
- Complaints Policy
- Enforcement Policy
- Register of Interests
- Register of Gifts and Hospitality and recording of declined offers
- Member support and training for both Borough and Parish Councillors
- Sound internal control systems, procedures and reliable records
- Clear disciplinary procedures
- An effective Internal Audit team
- Effective recruitment and appointment procedures
- Clear responsibilities, accountabilities and standards set out under the Scheme of Delegation within the Council's Constitution
- Induction and training
- Information Security Policies
- Internet Acceptable Use Policy
- Money Laundering Policy
- Safeguarding Policy
- Corporate and Operational Risk Registers
- Partnerships Protocol

2.0 Definitions

2.1 **Fraud** is a type of criminal activity, defined by the Serious Fraud Office as: 'abuse of position, or false representation, or prejudicing someone's rights for personal gain'. Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party.

The general criminal offence of fraud is defined by the Fraud Act 2006 and can include:

- deception whereby someone knowingly makes false representation
- or they fail to disclose information
- or they abuse a position

2.2 **Corruption** is the deliberate misuse of a position for direct or indirect personal gain. This includes offering, giving, requesting or accepting a bribe or reward, which influences actions or the actions of someone else. The Bribery Act 2010 makes it possible for individuals to be convicted where they are deemed to have given their consent or tacit approval in giving or receiving a bribe.

The Act also created the Corporate Offence of “Failing to prevent bribery on behalf of a commercial organisation” (corporate liability). To protect itself against the corporate offence, the Act requires an organisation to have “adequate procedures in place to prevent bribery”. In addition to this strategy, the Council’s Codes of Conduct and Whistle Blowing Policy, along with the educating of employees (e.g. through induction, e-learning etc.) are designed to meet the requirement.

2.3 **Theft** is the misappropriation of cash or other tangible assets. A person is guilty of “theft” if he or she dishonestly takes property belonging to another, with the intention of permanently depriving the other of it. The criminal offences associated with theft are predominantly set out in the Theft Act 1968 and the Theft Act 1978.

3.0 External scrutiny of council affairs

3.1 The Council’s affairs are subject to extensive scrutiny by a variety of external bodies and individuals, including: -

- the Local Government Ombudsman
- the external auditor is required to ensure that the Council has adequate arrangements for the prevention and detection of fraud and corruption
- members of the public via the complaints procedure, the Freedom of Information Act, and their right to inspect the

Council's published accounts, performance indicators and local performance plans

- HM Revenue and Customs
- the Department of Works and Pensions
- the Standards Board for England

4.0 Statutory responsibilities

4.1 Under section 151 of the Local Government Act 1972 the Council is required to make arrangements for the proper administration of its financial affairs and nominate one of its officers to be responsible for the administration of those affairs. This responsibility currently rests with the Head of Finance.

4.2 The Head of Finance also has a statutory responsibility under section 114 of the Local Government Act 1988 to ensure the proper arrangement of the Council's financial affairs and is required to report to full Council and the external auditor where it appears that a decision has been made or is about to be made that would involve the incurring of expenditure or a loss which is unlawful.

4.3 In addition, the authority has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

4.4 The Monitoring Officer has duties under section 5 of the Local Government and Housing Act 1989 to ensure that actions of officers and councillors are scrutinised as to their legality.

4.5 The Head of Finance has been nominated as the Council's Money Laundering Reporting Officer (MLRO) in accordance with the Money Laundering Regulations 2003. The MLRO will assess reports of potential money laundering and bribery received from Council employees and elected members; and will assume also the responsibility for monitoring contracts and of the application of the rules, regulations, and normal procedures of the Council. (see Appendix C)

4.6 The role of internal audit

Through the council's internal audit provider CW Audit Services, the Council has an adequate and effective system of internal audit established in accordance with the requirements of the Accounts and Audit Regulations 2003, the Accounts and Audit (Amendment) (England) Regulations 2006 and the Public Sector Internal Audit Standards (PSIAS) 2016.

4.7 In accordance with the above legislation and standards, CW Audit Services acts as an assurance function that primarily provides an independent and objective opinion to the organisation on the control environment comprising risk management, control and governance, by evaluating its effectiveness in achieving the organisation's objectives.

4.8 All Internal Audit activity is subject to approval by the Audit Committee and review by the Overview and Scrutiny Committee.

4.9 Annual Governance Statement

The Council provides with its published accounts an Annual Governance Statement. This describes the measures the Council has taken in the accounting year to ensure good governance.

4.10 Code of Corporate Governance

The Council has adopted a Local Code of Corporate Governance which sets out the principles of good corporate governance

4.11 Standards Committee

The Council's Standards Committee plays a key role in promoting and maintaining high standards of conduct by councillors in accordance with their code of conduct.

5.0 Culture

5.1 Scope

The Council will not tolerate fraud or corruption (or other forms of financial irregularity) by anyone. Consequently, this Strategy applies to a wide range of individuals including:

- All Council employees (including volunteers, temporary and agency employees);
- Elected Members;
- Employees and Committee Members of Council funded voluntary organisations;
- Council partners;
- Council suppliers, contractors and consultants (whether engaged directly or indirectly through partnership working);
- Service users; and
- Members of the general public.

5.2 The Council believes the best defence against fraud and corruption is to create a strong anti-fraud and corruption culture within the organisation. It promotes the 'seven principles of public life' (shown at Appendix B) put forward by the Nolan Committee:

- selflessness
- integrity

- objectivity
- accountability
- openness
- honesty
- leadership

We expect all our employees and councillors to follow these principles and all legal rules, procedures and practices, and to protect our legitimate interests at all times.
We also expect that people and organisations we deal with will act with honesty towards us.

6.0 Strategic aims and objectives

6.1 Through this strategy the aims and objectives are to:

- Protect the Council's valuable resources by ensuring they are not lost through fraud but are used to provide quality services to borough residents and visitors;
- Create and promote a robust 'anti-fraud' culture across the organisation which highlights the Council's zero tolerance of fraud, corruption and theft;
- Ensure effective counter fraud systems and procedures are in place which;
- Ensure that the resources dedicated to combatting fraud are sufficient and those involved are appropriately skilled;
- Proactively deter, prevent and detect fraud, corruption and theft;
- Investigate suspected or detected fraud, corruption and theft;
- Enable the Council to apply appropriate sanctions, including criminal and/or civil proceedings, to recover losses, where appropriate; and
- Provide recommendations to inform policy, system, risk management and control improvements, thereby reducing exposure to fraudulent activity;
- Create an environment that enables the reporting of any genuine suspicions of fraudulent activity. However, the Council will not tolerate malicious or vexatious allegations or those motivated by personal gain and, if proven, disciplinary or legal action may be taken;
- Ensure the rights of people raising legitimate concerns are properly protected;
- Work with partners and other investigative bodies to strengthen and continuously improve the Council's resiliency to fraud and corruption.

6.2 The Council is committed to continuing development of systems and procedures designed to prevent or detect possible fraud or corruption.

7.0 Managing the risk of fraud and corruption

7.1 Whilst all stakeholders have a part to play in reducing the risk of fraud, elected members and senior management are ideally positioned to influence the ethical tone of the organisation and play a crucial role in fostering a culture of high ethical standards and integrity.

7.2 As with any risk faced by the Council, it is the responsibility of managers to ensure that fraud risk is adequately considered within their individual service areas and in support of achieving strategic priorities, plans, projects and local outcomes. In making this assessment it is important to consider the risk of fraud occurring (i.e. proactive) rather than the actual incidence of fraud that has occurred in the past (reactive). Once the fraud risk has been evaluated, appropriate action should be taken by management to mitigate those risks on an ongoing basis, for example through introducing and operating effective systems of internal control ("the first line of defence").

7.3 Adequate supervision, recruitment and selection, scrutiny and healthy scepticism should not be seen as distrust, but simply as good management practice. This shapes attitudes and creates an environment opposed to fraudulent activity.

7.4 Good corporate governance procedures are a strong safeguard against fraud and corruption. The Audit Committee plays a key role in scrutinising the Council's approach to both fraud and risk management; and its wider resiliency to financial irregularity in general ("the second line of defence").

7.5 C W Audit Services undertake risk-based assurance work each year centred on a management approved Internal Audit Plan. This assurance work involves a review of systems and procedures, including a review of the management of risk (of both fraud and other types of risk) whereby system vulnerabilities are brought to the attention of management along with recommendations to strengthen procedures ("a third line of defence").

8.0 Fighting Fraud Locally: acknowledge – prevent – pursue

8.1 This Council seeks to fulfil its responsibility to reduce fraud and protect its resources by a strategic approach consistent with that outlined in both CIPFA's Code of Practice on Managing the Risk of Fraud and Corruption and in the Local Government Fraud Strategy – Fighting Fraud Locally, and its three key themes of acknowledge / prevent / pursue: -

8.2 Acknowledge

8.3 Committing support

This Council has a strong commitment to tackling the fraud threat. A robust whistleblowing policy is established and procedures are in place to support those who come forward to report suspected fraud. All reports will be treated seriously and acted upon. Employee awareness of fraud risks is embedded through e-learning and other training. Our policies and procedures are widely published and kept under review.

8.4 Assessing risks

We will continuously assess those areas most vulnerable to the risk of fraud as part of our risk management arrangements. These risk assessments will inform our internal controls and counter fraud priorities. Elected Members and Senior Officers have an important role to play in scrutinising risk management procedures and risk registers.

CW Audit Services will carry out assurance work in areas of higher risk to assist management in preventing fraudulent activity.

8.5 Robust response

We will strengthen measures to prevent fraud. CW Audit Services will work with management and our internal services e.g. HR, Finance and District Law and policy makers to ensure new and existing systems and policy initiatives are adequately fraud proofed.

8.6 Prevent

8.7 Better use of information technology

We will make use of data and analytical software to prevent and detect fraudulent activity. We will look for opportunities to share data and fraud intelligence to increase our capability to uncover potential and actual fraud. We will play an active part in the biennial National Fraud Initiative (NFI) data matching exercise.

8.8 Fraud controls and processes

We will educate managers with regard to their responsibilities for operating effective internal controls within their service areas. We will promote strong management and good governance that provides scrutiny and independent challenge to risks and management controls. Routine internal audit service reviews will seek to highlight vulnerabilities in the control environment and make recommendations for improvement.

8.9 Anti-fraud culture

We will promote and develop a strong counter fraud culture, raise awareness, provide a fraud e-learning tool and provide information on all aspects of our counter fraud work.

8.10 Pursue

8.11 Fraud recovery

A crucial element of our response to tackling fraud is recovering any monies lost through fraud. This is an important part of our strategy and will be rigorously pursued, where it is appropriate to do so.

8.12 Punishing fraudsters

We will apply realistic and effective sanctions for individuals or organisations where an investigation reveals fraudulent activity. This may include legal action, criminal and/or disciplinary action.

8.13 Enforcement

We will investigate instances of suspected fraud detected through the planned proactive work; cases of suspected fraud referred from internal or external stakeholders, or received via the whistleblowing reporting procedure. We will work with internal / external partners / organisations, including law enforcement agencies.

9.0 Reporting, advice, support

9.1 The Council recognises that the primary responsibility for the prevention and detection of fraud rests with management. If anyone believes that someone is committing a fraud or suspects corrupt practices, these concerns should be raised in the first instance directly with line management or to the Monitoring Officer or Head of Finance, in accordance with the Council's Whistleblowing Policy and Financial Procedure Rules.

9.2 Where managers are made aware of suspected fraud by employees, they have responsibilities for passing on those concerns to the Monitoring Officer or Head of Finance. Managers should react urgently to evidence of potential fraud or corruption.

9.3 Employees who wish to raise a serious concern should refer to the detailed Whistleblowing Policy. They can do this, without fear of recrimination, in the knowledge that such concerns will be properly investigated and fairly dealt with.

9.4 If employees still feel unable to raise their concerns through any of the above internal Council routes then they are encouraged to raise them through Public Concern at Work (Tel: 020 7404 6609), a registered Charity whose services are free and confidential.

9.5 The Monitoring Officer will refer all concerns in relation to possible financial impropriety to the Head of Finance (Section 151 Officer). Thereafter, it is likely that C W Audit Services, in conjunction with other

services such as Human Resources, District Law, ICT Services, will give advice and support to managers involved in fraud investigation including on evidence gathering, documentation and retention, disciplinary proceedings and, where relevant, referral to the Police.

9.6 **Investigations** - To avoid potentially contaminating the evidence, managers should not investigate concerns themselves without having sought relevant authority to do so and instead should immediately report all suspicions of fraud or corruption, as detailed above. Investigation of suspected fraud and / or corruption will be conducted in accordance with the Police and Criminal Evidence Act (PACE) 1984. Should an investigator consider utilising directed surveillance they must seek the guidance of an authorising officer to ensure compliance with the Regulation of Investigatory Powers Act (RIPA) 2000. Details are included at Appendix D.

9.7 **Criminal offences** - District Law will provide guidance as to whether a criminal offence has occurred. In such cases the Council will seek a prosecution unless the decision is taken, following legal, that it would be inappropriate to do so.

9.8 **Disciplinary action** - The Head of Service (following legal advice) will decide whether disciplinary action should be taken against an employee. Cases of fraud or corruption are likely to represent gross misconduct and therefore the employee could be liable to dismissal.

9.9 **Elected members** - The Chief Executive and Monitoring Officer will advise on action in relation to members.

9.10 **Recording** - The Head of Finance will maintain a fraud database where summary details of financial irregularities will be recorded. Outcomes of investigations into suspected fraud or corruption will be reported to members an d appropriate regulatory bodies in accordance with corporate governance arrangements. In addition, counter fraud and corruption activity is reported through:

- The National Fraud Initiative
- The CIPFA/TEICCAF Annual Fraud and Corruption Surveys leading to the annual report on Protecting the Public Purse
- The Local Government Transparency Code

10.0 Money laundering

10.1 If there is suspicion that an offence of money laundering may have taken place, the Money Laundering Reporting Officer may refer the matter to the National Criminal Intelligence Service.

10.2 The Council's Anti-Money Laundering Policy is attached at Appendix C.

11.0 External auditors

11.1 In the majority of cases, where the external auditors suspect a fraud, the case will be passed over to the control of CW Audit Services, which will then be expected to oversee the investigation of the case and keep the external auditors informed of progress. However, the external auditors also reserve the right to retain control over a fraud investigation, although this is only likely in exceptional circumstances and, will offer support and assistance to CW Audit Services in investigating significant frauds, where appropriate with District Law

11.2 Finally, the Council may use external audit services for the investigation of a suspected fraud, where it is important for the enquiry to be seen publicly as wholly impartial.

12.0 Publicity and training

12.1 The Council recognises the continuing success of this strategy and its credibility will depend largely on the effectiveness of publicity, training and the responsiveness of its employees.

12.2 The Council supports induction and ongoing training, particularly for employees involved with internal control systems, to ensure their responsibilities and duties are highlighted and reinforced regularly.

APPENDIX A

1.0 Action Plan

1.1 This Strategy sets out the developments / actions the Council proposes over the medium term future to further improve its resilience to fraud and corruption. These developments include the following actions:

1.**2**

Action	**Indicative Implementation Date**
To proactively use the results of previous fraud risk assessments, the issues highlighted in Protecting the Public Purse and other intelligence to direct counter fraud resources in the 2017-18 Internal Audit Plan.	June 2017
To refresh the Council's suite of anti-fraud policies, strategies and procedures and to ensure that they continue to be relevant to national guidance, e.g. CIPFA Code of Practice on Managing the Risk of Fraud and Corruption (2014).	Sept 2017
To ensure that fraud awareness is given adequate prominence in the Council's employee induction procedures.	July 2017
To undertake an annual Fraud Risk Assessment covering the Council's main areas of exposure to fraud and to use the results to influence the Council's approach moving forward.	Sept 2017
To update the Council's e-learning module on Fraud Awareness and to promote its uptake by all employees.	July 2017
To be an active participant in the National Fraud Initiative (NFI) and to robustly investigate suspected cases of fraud identified through NFI.	Oct 2017
To refresh the Fraud Awareness pages on the Corporate intranet and to engage with managers through targeted communications to emphasise their obligations to operate effective systems of internal control which are designed to reduce the risk to the Council of fraud, error or inadvertent loss.	Sept 2017
To assess and address the fraud risks associated with the Council becoming greater involved as a commissioner of services.	Dec 2017
To assess and address the risks associated with partnership work, particularly where the Council is the lead accountable body.	Dec 2017
To work with council partners to further reduce the risk of fraud in areas where there is joint benefit (e.g. Council Tax benefit).	Mar 2018

APPENDIX B

SEVEN PRINCIPLES OF PUBLIC LIFE

- as originally defined by the Nolan Committee in 1996 and revised in 2015

1. Selflessness

Holders of public office should act solely in terms of the public interest.

2. Integrity

Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

3. Objectivity

Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

4. Accountability

Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

5. Openness

Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

6. Honesty

Holders of public office should be truthful.

7. Leadership

Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

APPENDIX C

ANTI-MONEY LAUNDERING POLICY

INTRODUCTION

1. There have been significant changes to the legislation concerning money laundering, namely:-
    - The Terrorism Act 2000
    - The Proceeds of Crime Act 2002 (PoCA)
    - The Money Laundering Regulations 2007 and subsequent revisions 2017(MLR)
    - Counter Terrorism Act 2008

    NOTE:-
    - The Money Laundering Regulations do not cover the offences of being involved with money laundering. They cover the setting up of systems to identify risk, training obligations, and identity information.

2. These changes have broadened the definition of money laundering and the range of activities covered by the statutory framework. As a result, the obligations now impact on certain areas of local authority business and require local authorities to establish internal procedures to prevent the use of their services for money laundering.

SCOPE OF THE POLICY

3. This policy applies to all Members and all employees of the Council and aims to maintain the high standards of conduct and propriety that currently exist in the Council by preventing criminal activity through corruption and in particular money laundering. The policy sets out the procedures which must be followed (e.g. the reporting of suspicions of corruption to include money laundering) to enable the Council to comply with its legal obligations.

4. This policy sits alongside the Council's Whistleblowing Policy and Counter Fraud and Corruption Strategy.

5. Failure by a Member or an employee to comply with the procedures set out in this policy may lead to disciplinary action.

WHAT IS MONEY LAUNDERING?

6. Money laundering means:-
    - concealing disguising, converting, transferring criminal property or removing it from the UK (section 327 of the 2002 Act); or
    - 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; or
    - acquiring, using or possessing criminal property (section 329); or

- 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)

Please note that 'money' is used in this context as a generic term to include money or monies worth; i.e anything that is of value. It includes, money, land, objects, legal rights, interests in land, shares, etc.

These are the primary money laundering offences and therefore prohibited acts under the legislation.

7. Potentially any Member or employee 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. This policy sets out how any concerns should be raised.

8. Whilst the risk to the Council of contravening the legislation is low, it is extremely important that all Members and employees are familiar with their legal responsibilities. **Serious criminal sanctions may be imposed for breaches of the legislation on the Council and individual employees and members.**

WHAT ARE THE OBLIGATIONS ON THE COUNCIL?

9. Organisations conducting "relevant business" must:-
    - Appoint a Money Laundering Reporting Officer ("MLRO") to receive disclosures from employees of money laundering activity (their own or anyone else's)
    - Implement a procedure to enable the reporting of suspicions of money laundering
    - Maintain client identification procedures in certain circumstances
    - Maintain record keeping procedures

10. Not all the Council's business is "relevant" for the purposes of the legislation. However, the safest way to ensure compliance with the law is to apply them to all areas of work undertaken by the Council - therefore all Members and employees are required to comply with the reporting procedure set out in Paragraphs 13 – 28 below. The following sections of this Policy provide detail about the requirements listed in Paragraph 9 above.

THE MONEY LAUNDERING REPORTING OFFICER

11. The officer nominated to receive disclosures about money laundering activities is the Chief Financial Officer.

12. In the absence of the MLRO, the Monitoring Officer, is authorised to deputise for him.

DISCLOSURE PROCEDURE Reporting to the Money Laundering Officer

13. 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 possible 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 and disciplinary action.**

14. Your disclosure should be made to the MLRO. The report must include as much information as possible, e.g.
    - Full details of the people involved (including yourself, if relevant) e.g. name, date of birth, address, company names, directorships, bank account details, VAT numbers, phone numbers, etc
    - Full details of their / your involvement: and details of the transaction or matter giving concern -
    - If you are concerned that your involvement in a transaction would amount to a prohibited act under sections 327-329 of the 2002 Act, then your report must include all relevant details, as consent will need to be obtained from the National Crime Agency (NCA), via the MLRO, to take any further part in the transaction –
    - You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent
    - The types of money laundering activity involved
    - The dates of such activities
    - Whether the transactions have happened, are ongoing or are imminent
    - Where they took place
    - How they are undertaken
    - The (likely) amount of money/assets involved
    - Why, exactly, you are suspicious – the NCA will require clear and concise reasons;

    Along with any other available information, to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering, and to enable him to prepare his report to the NCA, where appropriate. You should also enclose copies of any supporting documentation.

15. Once you have reported the matter to the MLRO you must follow any directions he may give you. **You must NOT make any further enquiries into the matter yourself.** Any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO, who will refer the

matter onto the NCA, if appropriate. All Members and employees will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

16. **Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) you suspect of money laundering.** Even if the NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO.

17. Do not, therefore, make any reference on a file to a report having been made to the MLRO – should the person concerned 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.

Consideration of the Disclosure by the Money Laundering Officer

18. Upon receipt of a disclosure report, the MLRO must note the date of receipt on his section of the report and acknowledge receipt of it. He should also advise you of the timescale within which he expects to respond to you.

19. The MLRO will consider the report and other available internal material he thinks relevant, e.g.
    - reviewing other transaction patterns and volumes
    - the length of any business relationship involved
    - the number of any on-off transactions and linked one-off transactions
    - any identification evidence held

20. The MLRO will undertake such other reasonable enquiries he thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved). The MLRO may also need to discuss the report with you.

21. Once the MLRO has evaluated the disclosure report and any other relevant information, he must make a timely determination as to whether:
    - there is actual or suspected money laundering taking place
    - there are reasonable grounds to know or suspect that is the case whether he needs to seek consent from the NCA for a particular transaction to proceed

22. Where the MLRO does so conclude, then he must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless he has a strong and reasonable excuse for nondisclosure to the NCA.

23. Where the MLRO suspects money laundering but has a reasonable excuse for nondisclosure, then he must note the report accordingly; he can then immediately give his consent for any ongoing or immediate transactions to proceed.

24. In cases where legal professional privilege may apply, the MLRO must liaise with the Head of District Law to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

25. Where consent is required from the NCA for a transaction to proceed, then the transactions in question must not be undertaken or completed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.
26. Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then he shall mark the report accordingly and give his consent for any ongoing or imminent transactions to proceed.

27. All disclosure reports referred to the MLRO and reports made by him to the NCA must be retained by the MLRO in a confidential file kept for that purpose for a period of five years.

28. The MLRO commits a criminal offence if he knows or suspects, or has reasonable grounds to do so, through a disclosure being made to him, that another person is engaged in money laundering and he does not disclose this as soon as practicable to the NCA.

CLIENT IDENTIFICATION PROCEDURE

29. Where the Council is carrying out relevant business (accountancy, audit, property disposal and certain legal services) and:
    - forms an ongoing business relationship with a client; or
    - undertakes a one-off transaction involving payment by or to the client of 15,000 Euro (approximately £10,000) or more; or
    - undertakes a series of linked one-off transactions involving total payment by or to the client(s) of 15,000 Euro or more; or
    - it is known or suspected that a one-off transaction (or a series of them) involves money laundering then this Client Identification Procedure must be followed before any business is undertaken for that client.

    Please note that, unlike the reporting procedure, it must be emphasised that the Client Procedure will only apply to those carrying out relevant business.

30. In the above circumstances, employees in the relevant unit of the Council must obtain satisfactory evidence of the identity of the prospective client, as soon as practicable after instructions are received (unless evidence of

the client has already been obtained). This applies to existing clients, as well as new ones, but identification evidence is not required for matters entered into prior to 1 March 2004.

31. Once instructions to provide relevant business have been received, and it has been established that Paragraph 29 above applies, evidence of identity should be obtained as follows:-
    - Internal Clients

      Appropriate evidence of identity will be either written and signed instructions on Council-headed notepaper at the outset of the matter. Such correspondence should then be placed on the Council's client file along with a prominent note explaining which correspondence constitutes the evidence and where it is located.
    - External Clients

      Appropriate evidence of identity will be written and signed instructions on the organisation's official letter head at the outset of the matter.

    Such correspondence should then be placed on the Council's client file along with a prominent note explaining which correspondence constitutes the evidence and where it is located. With instructions from new clients, or further instructions from a client not well known to you, you may wish to seek additional evidence of the identity of key individuals in the organisation and of the organisation itself.

32. In all cases, the evidence should be retained for at least five years from the end of the business relationship or transaction(s).

33. If satisfactory evidence of identity is not obtained at the outset of the matter, then the business relationship or transaction(s) cannot proceed any further.

RECORD KEEPING PROCEDURES

34. Each Service Area conducting relevant business must maintain records of:
    - client identification evidence obtained
    - details of all relevant business transactions carried out for clients for at least five years. This is so that they may be used in evidence in any subsequent investigation by the authorities into money laundering.

35. The precise nature of the records is not prescribed by law, however, they must be capable of providing an audit trail during any subsequent investigation, e.g.
    distinguishing the client and the relevant transaction and recording in what form funds were received or paid.

36. In practice, the Service Areas will be routinely making records of work carried out for clients in the course of normal business and these should suffice in this regard.

CONCLUSION

37. The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This policy has been written so as to enable the Council to meet the legal requirements in a way which is proportionate to the very low risk to the Council of contravening the legislation.

38. Should you have any concerns whatsoever any transactions then you should contact the MLRO.

APPENDIX D

Policy and Procedures for The Regulation of Investigatory Powers Act 2000 (RIPA)

General

1. This policy sets out the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA) when undertaking investigations requiring Directed Surveillance as defined by the Act, investigations requiring the use of a Covert Human Intelligence Source (CHIS), or obtaining communications data (CD). In simple terms the act requires the Council to have in place procedures which ensure that where required, surveillance is necessary (e.g. to investigate a suspected crime), proportionate (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means) and properly authorised.

2. If the Council wishes to authorise the use of Directed Surveillance, acquisition of CD and use of a CHIS under RIPA it needs to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace[1] (a JP) 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.

3. The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation form and seeking approval from an authorising officer will remain the same.

4. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the Act and the Codes of Practice and take necessary and proportionate actions in these matters.

5. The Monitoring Officer is duly authorised by the Council to keep this policy up to date and accurate, and maintain a central record of authorisations for the purpose of RIPA.

6. Any officer of the Council contemplating taking action under RIPA powers should seek the advice of the Responsible Officer or an Authorising Officer (as detailed at appendix 3).

Background

7. The Human Rights Act 1998 requires the Council and any organisations working on its behalf to respect the private life and family of citizens, their home and their correspondence. The European convention made this a qualified right and not an absolute right and as such the Council may interfere in the citizens rights mentioned above if, the interference is:-

    a) In accordance with the law;

    b) Necessary; and

    c) Proportionate.

[1] A District Judge or lay magistrate

8. Some of the Council's activities will necessarily require covert surveillance to be used where the Council is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more, for example, benefit fraud, certain waste dumping offences and licensing enforcement. Surveillance is usually a last resort that an investigator will utilise to prove or disprove an allegation. RIPA sets out a statutory mechanism for authorising covert surveillance and the use of a CHIS e.g. undercover agents. It seeks to ensure that any interference with an individual's rights under Article 8 of the European convention is necessary and proportionate and therefore there is a balance between public interest and the human rights of individuals. Covert surveillance will only be undertaken where there is no reasonable and effective alternative means of achieving the desired objective. No activity shall be undertaken within the definition of intrusive surveillance.

9. Employees of the Council and external agencies working for the Council are covered by the Act whilst they are working for the Council.

10. Any evidence gathered by surveillance subject to RIPA but not properly authorised may be ruled inadmissible in court. Surveillance without proper authorisation could lead to a challenge and/or claim for compensation under article 8 of the Human Rights Act. Therefore, it is essential that all involved with RIPA comply with this policy.

RIPA does:

- Require prior authorisation of directed surveillance.
- Prohibit the Council from carrying out intrusive surveillance.
- Require authorisation of the conduct and use of CHIS.
- Require safeguards for the handling and use of CHIS.
- Permit the Council to compel disclosure of communications data from telecom and postal companies
- Permit the Council to obtain communications records from communications companies.

RIPA does not:

- Make unlawful conduct which is otherwise lawful.
- Prejudice or invalidate any existing powers available to the Council to obtain information by any means, which does not involve surveillance covered by RIPA: for example the Council's powers to obtain information from the Land Registry regarding ownership of property.

TYPES OF SURVEILLANCE

11. Surveillance includes

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording any of the above in the course of authorised surveillance.

- Surveillance, by or with, the assistance of appropriate surveillance devices.

Surveillance is divided under RIPA into two types: **"directed"** and **"intrusive"**

Surveillance can be overt or covert.

12. Most surveillance carried out by the Council will be overt (open) and not hidden or secretive. Often Officers will be doing their normal jobs for example, inspection of food premises. Any surveillance which is undertaken where the subject knows about it comes under the definition of overt surveillance. (For example, where a resident has been warned that they are going to be recorded for the purposes of dealing with a noise nuisance). Overt surveillance does not require authorisation under RIPA.

13. Surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. It should be noted that surveillance may also intrude on the privacy of others who are not the subject of surveillance but who are unintentionally observed.

14. RIPA regulates surveillance which is Directed Surveillance and Intrusive Surveillance and the use of a CHIS.

15. **"Directed Surveillance"** is defined as**:**

    - covert; and
    - not intrusive as defined below; and
    - not carried out in an immediate response to events which would otherwise be unreasonable to seek authorisation e.g. spotting something suspicious and continuing to observe it; and
    - undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for the purposes of an investigation). (Section 26 (10) of RIPA).

    The key issue in "Directed Surveillance" is the targeting of an individual with the likelihood of gaining private information.

16. **"Intrusive Surveillance"** is defined as:

    Covert surveillance that is carried out in relation to residential premises (including hotel bedrooms, prison cells and rented accommodation), premises where legal consultations take place or private vehicles (including hire or company cars, boats or caravans) and involves the presence of a person **on** the premises or **in** the vehicle or is carried out by a surveillance device in the premises or vehicle.

    Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises or vehicle. High quality video or CCTV cameras may run a significant risk of providing high quality data which may be considered intrusive. Similarly some recording devices used by Environmental Health Officers to record noise may provide evidence of the same quality as if the device was actually in the premises.

Care must be taken to properly assess whether the information will be intrusive. If officers are in any doubt they must seek advice from the Council's legal service.

A Local Authority and its Officers cannot carry out intrusive surveillance, but information about it is included here to help investigating officers avoiding inadvertently breaching this rule.

This form of surveillance can only be carried out by the police and other law enforcement agencies.

17. **A "Covert Human Intelligence Source" (CHIS)** is defined as:

- a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:
- using such relationship to obtain information or to provide access to any information to another person or
- covertly disclosing information obtained by the use of such a relationship or as a result of the existence of such a relationship
- where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose or (in the case of disclosure of information) it is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the disclosure in question.

18. A local authority authorisation for the conduct and use of a CHIS may include:

- someone employed or engaged by a local authority to hide their true identity or motivation and covertly use a relationship to obtain information and disclose it to the local authority (an undercover officer); or
- a member of the public who provides a tip-off to a local authority and is asked to go back and obtain further information by establishing or continuing a relationship whilst hiding their true motivation (an informant).

19. The Council has considered the use of CHIS but has concluded that it will not be used, except in exceptional circumstances, given the need for trained handlers and controllers.

Use of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS may only be authorised by the Head of Paid Service (Chief Executive) or, in his absence, the acting Head of Paid Service. "Confidential information" is defined for the purposes of RIPA as matters subject to legal privilege, confidential personal information or confidential journalistic material.

Persons who complain about Anti-Social Behaviour and are asked to keep a diary will not normally be Covert Human Intelligence Source and therefore do not require authorisation as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. decibel) will not normally capture private information and, therefore, does not require authorisation.

Examples of Different types of Surveillance

Type of Surveillance	Examples
Overt	• Signposted Town Centre CCTV cameras (in normal use) • Recording noise from outside the premises after the occupier has been warned that this will occur if the noise persists
Covert but not requiring prior authorisation	• CCTV cameras providing general traffic, crime or public safety information. • 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).
Directed must be RIPA authorised.	• Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment.
Intrusive council officers cannot do this.	• Planting a listening or other device (bug) in a person's home or in their private vehicle.

Communications Data

20. The provisions of Part I Chapter II of RIPA permits local authorities to access communications data where it is necessary for the purpose of preventing or detecting crime or preventing disorder.

21. Communication data means any traffic or any information that is or has been sent by over a telecommunications system or postal system, together with information about the use of the system made by any person.

22. In effect the term communications data embraces the "who, when and where" of a communication but not the content, not what was said or written. It includes the manner in which and by what method a person (or machine) communicates with another person (or machine), but excludes what they say or data they pass on, including text, audio and video.

23. These powers must be used in accordance with the Code of Practice on Accessing Communications. Access to communications data must be authorised by a designated authorising officer and be obtained through the Council's "Single Point of Contact" (SPoC), which for these purposes is the Council's Head of Legal Services. The grounds for authorisations are the same as those for Directed Surveillance. The Council has however never sought to use this power and has not put the required arrangements in place other than identifying its SPoC.

Codes of Practice

24. There are Codes of practice regarding Covert Surveillance, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data that supplement and expand on the provisions of the Act. The Codes together with other information on the Act can be accessed via the Office of Surveillance Commissioners' website at http://surveillancecommissioners.independent.gov.uk.

Procedures for Authorisation

25. A flowchart of the procedures to be followed appear at Appendices 1 and 2.

26. The Principal Revenue and Benefits Manager shall hold the Central record of authorisations for the purpose of RIPA.

27. Authorisations must be given in writing by an Authorising Officer. Authorising Officers are those whose posts appear in Appendix 3 to this document and, any that are duly added to the list or substituted by the Monitoring Officer. All officers authorised to sign RIPA forms will be given the appropriate training.

28. All surveillance covered by the Act must be authorised using the appropriate application forms and before an application is made to a Justice of the Peace (JP) seeking an Order to approve the grant or renewal of a RIPA authorisation (a JP Order).

29. A written application for a directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- confirmation that the suspected offence attracts a maximum custodial sentence of six months or more
- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- an explanation of what other methods had been considered and why they are not considered feasible;
- the nature of the surveillance;
- a location plan showing the proposed observation points
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;

- an explanation how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- the details of any potential collateral intrusion and why the intrusion is justified, and steps proposed to be taken to mitigate it;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance (Note: this is unlikely to be required and prior advice should be sought from Legal Services);
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- a subsequent record of whether authorisation was given or refused, by whom, and the time and date this happened.

30. Directed surveillance, the conduct and use of CHIS or access to communications data can only be authorised by the Council on the grounds that it is for **the purpose of preventing or detecting a criminal offence** and it meets the condition set out in new article 7A(3)(a) or (b) of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012[2]

31. As a result, the Council can no longer authorise directed surveillance for the purpose of preventing disorder (unless this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment), nor may it any longer authorise the use of directed surveillance under to investigate disorder that does not involve criminal offences or to investigate offences the punishment for which does not meet the threshold. This may include, for example, littering, dog control and fly-posting.

32. In assessing an application form the Authorised Officer must:

    a) Be mindful of the corporate policy.

    b) Satisfy himself or herself that the RIPA authorisation is in accordance with the law, necessary and proportionate.

        i. Assessing proportionality 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. If overt investigative methods would be effective, it is unlikely to be proportionate to authorise intrusive covert activity.

    c) Take into consideration the risk and proportionality of interfering with the privacy of people not connected with the investigation.

    d) Set a date for reviewing the authorisation.

[2] Those conditions are (1) that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or (2) would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (criminal offences relating to the underage sale of alcohol or tobacco). The offences referred to in the second of these conditions are usually investigated by the County Council's Trading Standards service.

e) Forward a copy of the authorisation and JP Order to the officer maintaining the central record within 5 working days of obtaining the Order approving the grant of the authorisation.

Each action authorised should bring an expected benefit to the investigation 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.

33. When authorising the conduct or use of CHIS the Authorised Officer must also:

a) Be satisfied that the conduct and/or use of the CHIS is proportionate to what is being sought to be achieved.

b) Be satisfied that the appropriate arrangements are in place for the management of the CHIS. This should include a risk assessment for health and safety,

c) Consider the degree of intrusion for those likely to be affected.

d) Consider the diverse impact on community confidence that may result from the information obtained.

e) Ensure that records are available on a need to know basis.

34. The authorisation must be reviewed within the time stated on the application form and cancelled if no longer necessary. An authorisation for a directed surveillance ceases to have effect 3 months from day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect (12 months in the case of a CHIS). However, the forms are not deemed to have expired at the end of the duration, and therefore it is essential that the authorisations are reviewed or cancelled as appropriate. Authorisations can be renewed when the authorisation has expired but these must be considered as a fresh application.

35. If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

36. The Monitoring Officer is the Officer responsible for the integrity of the processes in place within the Council in respect of the Act. The Monitoring Officer shall report to Members on the use of RIPA powers periodically.

Working with Other Organisations

37. Where another agency has been instructed by the Council to undertake any action under RIPA this must be done in accordance with this policy. The appropriate officer requesting the work must ensure that the agency is made explicitly aware of what they are authorised to do.

38. The investigating officer must ensure that authorisations are properly implemented even when acting on behalf of others, such as the Department for Work and Pensions, because the product is primarily the Council's and it may be the Council that receives complaints or claims in the case of misuse.

Maintenance of Records

39. The following documents must be retained where an authorisation has been granted

- A copy of the forms and JP Order with any supporting documentation
- A record for the period which the surveillance has taken place.
- The frequency of reviews as prescribed by the Authorising Officer.
- A record of each review of an authorisation
- The date and time of when any instruction was given for the Authorisation.

39. The Corporate forms include application, renewal, review and cancellation for directed surveillance and CHIS. JP Orders are sought on the approved judicial application/order form

40. The Council will retain records for a period of 3 years after the date of the authorisation.

Central Register of Authorisations

41. This will be held and kept up to date by the Principal Revenue and Benefits Manager and reviewed by the Monitoring Officer.

42. If you need any further advice on RIPA please contact the Monitoring Officer.

Complaints and Copies of Codes of Practice

43. Complaints about the Council's actions under RIPA should be submitted in writing to the Monitoring Officer.

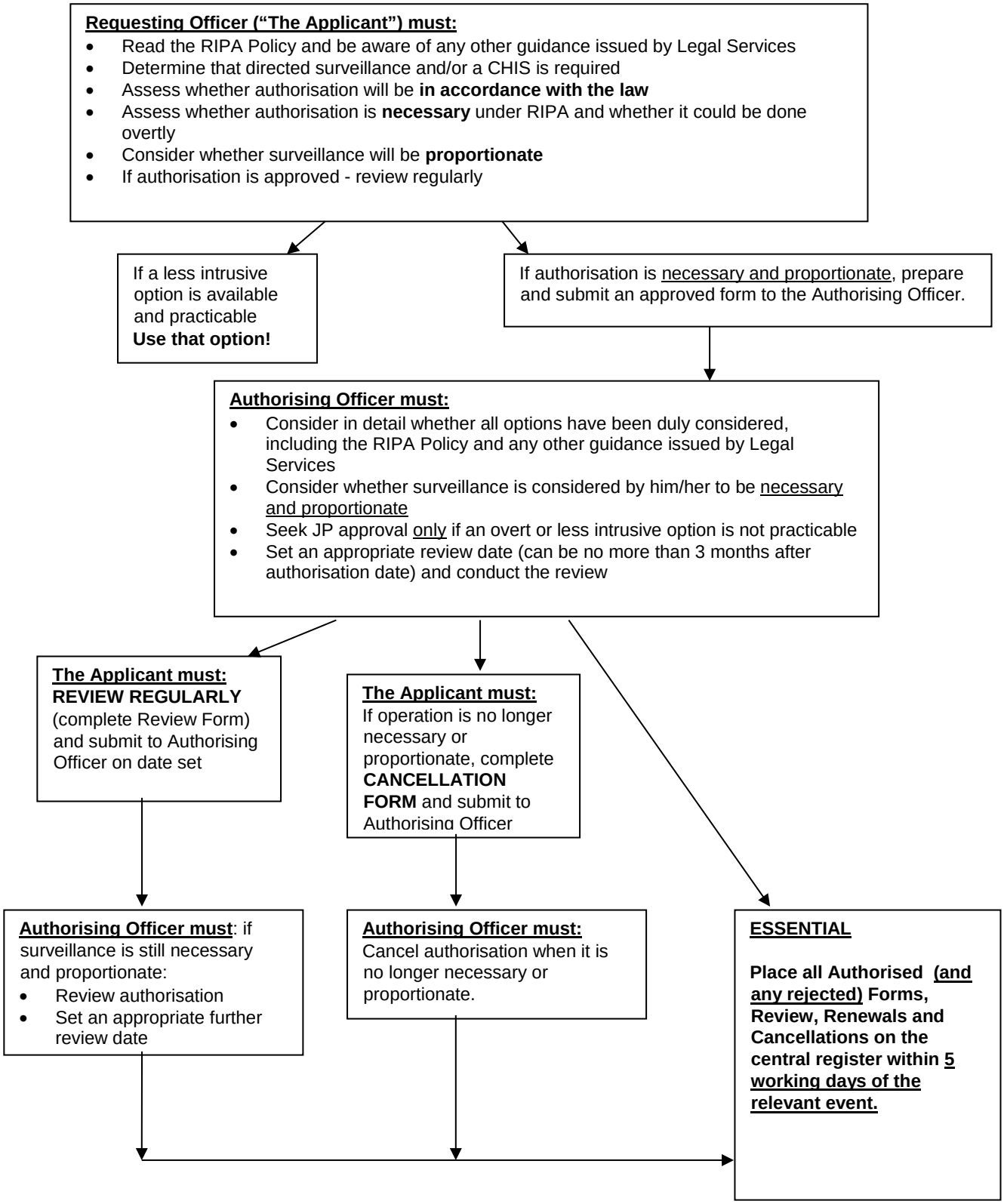
44. Information on the Investigatory Powers Tribunal will be provided as part of the response to any RIPA complaint, including the provision of copies of the Tribunal's complaint form and information leaflet. An Investigatory Powers Tribunal (IPT) established under section 65 of RIPA investigates complaints made by people who are concerned that public authorities have deployed covert investigatory techniques against them unlawfully. There is no domestic right of appeal against IPT decisions, although individuals may seek appeal to the European Court of Human Rights. The IPT's website is at: http://www.ipt-uk.com/. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

45. The Codes of Practice on use of RIPA published by the Home Office, together with other information on the Act can be accessed via the Office of Surveillance Commissioners' website at http://surveillancecommissioners.independent.gov.uk

    Copies of the Codes of Practice may also be inspected at the Council's Offices. Please contact the Monitoring Officer to arrange an inspection.

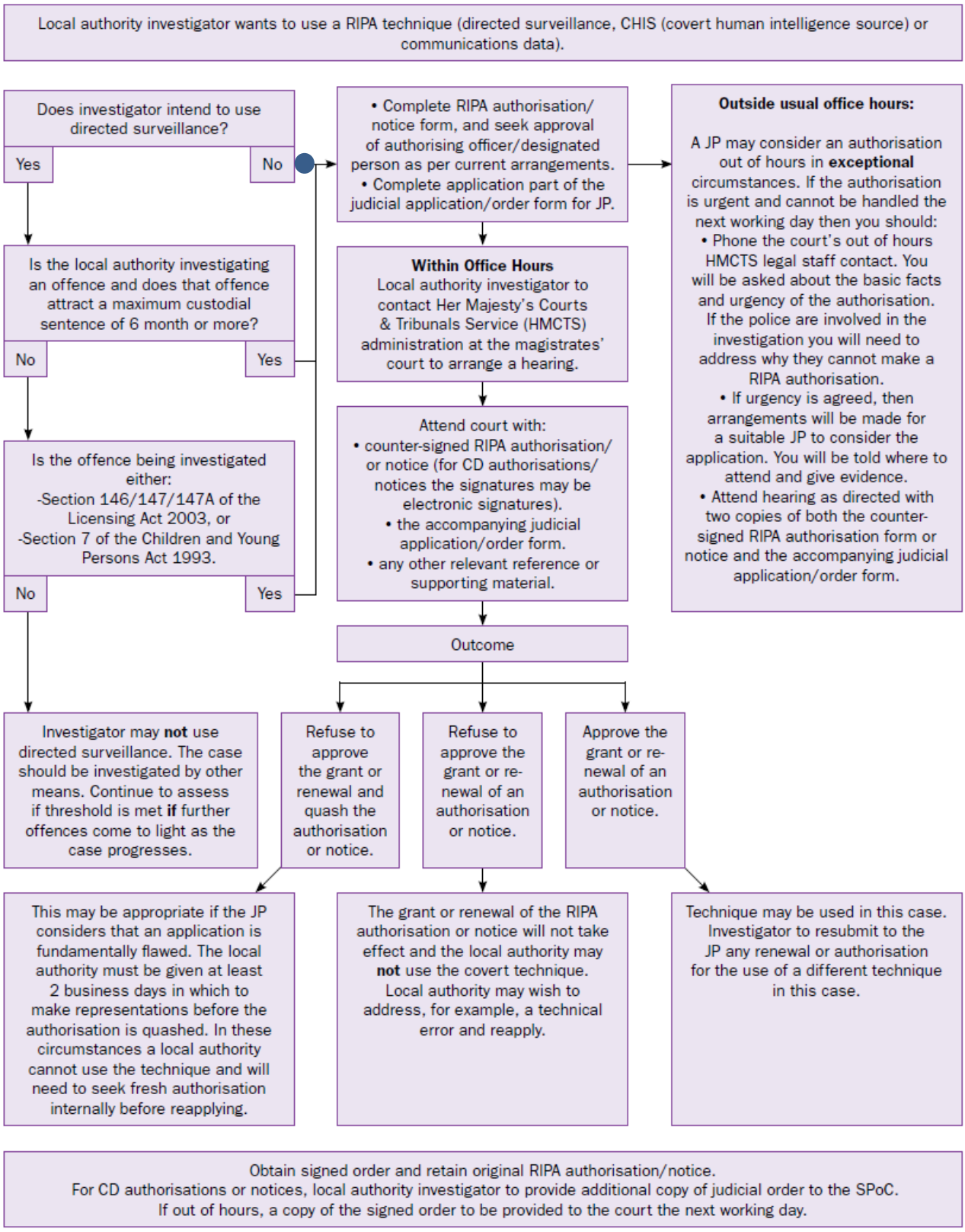
APPENDIX 1

RIPA AUTHORISATION FLOW CHART



APPENDIX 2

Local Authority procedure: application to a Justice Of The Peace seeking an Order to approve the grant of a RIPA authorisation or notice



From: *Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance*, October 2012

APPENDIX 3

AUTHORISING OFFICERS

The following Officers shall be designated as Authorising Officers for the purposes specified on behalf the Borough Council of Wellingborough under the Regulation of Investigatory Powers Act 2000:

Liz Elliott – (Responsible Officer) Head of Finance

Nigel Robinson – Principal Revenue and Benefits Manager

Amanda Wilcox – Principal Environmental Health Manager

If confidential information is likely to be obtained as a consequence of the surveillance then authorisation may only be obtained from:

John Campbell – Chief Executive

Following advice from the Office of Surveillance Commissioner's Office, the list of authorising officers has been limited to officers with a working knowledge of RIPA. Services without a named authorising officer should present applications to one of the named Authorising Officers.

IMPORTANT NOTES

A. Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a renewal or cancellation) unless s/he has been certified by the relevant Chief Officer and notified to the Monitoring Officer.

B. If a Chief Officer wishes to add, delete or substitute a post, s/he must make and record the necessary decision and notify the Monitoring Officer.

C. If in doubt, ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

D. The hearing before the JP is a 'legal proceeding' and therefore officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. It is preferable that the Authorising Officer and the case investigator seeking authorisation are present as they are best able to fulfil this role, as they will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case.