

**REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)
POLICY STATEMENT, STRATEGY & GUIDANCE NOTES**

Document Status: Final

Originator: J M Hackett

Updated: J M Hackett

Owner: Solicitor to the Council – Corporate Services

Version: 01.01.03

Date: 17/01/2017

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is Jane Marie Hackett, Solicitor to the Council – Corporate Services.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

| Revision Date | Version Control | Summary of changes |
|----------------|-----------------|--------------------|
| | 1.01.01 | Scheduled review |
| December 2008 | 1.01.02 | Scheduled review |
| September 2010 | 1.01.03 | Scheduled review |
| September 2011 | 1.01.04 | Scheduled review |
| December 2012 | 1.01.05 | Scheduled review |
| November 2014 | 1.01.06 | Scheduled review |
| April 2015 | 1.01.07 | Scheduled review |
| February 2016 | 1.01.08 | Scheduled review |
| January 2017 | 1.01.09 | Scheduled review |

Approvals

| Name | Title | Approved |
|------------------------------|---|----------|
| Audit & Governance Committee | Committee Approval | Yes |
| Council | Council Approval | Yes |
| CMT | Group Approval | Yes |
| John Wheatley | Executive Director – Corporate Services | Yes |
| Jane Marie Hackett | Solicitor to the Council and Monitoring Officer | Yes |

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the website.

CONTENTS PAGE

| | Page |
|--|------|
| Anti-Money Laundering Policy Statement | 4 |
| Anti-Money Laundering Policy | |
| 1.0 Introduction | 5 |
| 2.0 Scope of the Policy | 5 |
| 3.0 Definition of Money Laundering | 5 |
| 4.0 Requirements of the Money Laundering Legislation | 6 |
| 5.0 The Money Laundering Reporting Officer (MLRO) | 7 |
| 6.0 Due Diligence Procedures | 7 |
| 7.0 Reporting Procedure for Suspicious Transactions | 8 |
| 8.0 Additional Guidance | 9 |
| 9.0 Consideration of the disclosure by the MLRO | 9 |
| 10.0 Training | 10 |
| 11.0 Conclusions | 10 |
| 12.0 Review | 11 |
| <u>Appendix 1</u> | |
| Role of the Money Laundering Reporting Officer | 12 |
| <u>Appendix 2</u> | |
| Money Laundering – Internal Reporting Form | 13 |
| <u>Appendix 3</u> | |
| Money Laundering Avoidance Aide Memoir | 18 |

TAMWORTH BOROUGH COUNCIL

ANTI-MONEY LAUNDERING POLICY STATEMENT

- 1.0 Tamworth Borough Council fully recognises its responsibility in relation to the spending of public money (Protecting the Public Purse) and is committed to the fullest support for Councillors and Employees in upholding the reputation of the Council and maintaining public confidence in its integrity. It also recognises its responsibilities under the Proceeds of Crime Act 2002, Money Laundering Regulations 2007 and the Bribery Act 2010.
- 2.0 The Council acknowledges the threat of money laundering and the harm that it can cause. The Council is committed to maintaining an ethical culture which does not and will not tolerate any form of fraud and corruption. Any such issues will be thoroughly investigated and, if confirmed, dealt with rapidly in the strongest possible way. We will seek the strongest possible sanctions against those who seek to defraud the Council. This includes taking appropriate action against employees, Councillors, contractors, external individuals and organisations.
- 3.0 To deliver the Council's corporate priorities, aims and strategic objectives we need to maximise the financial resources available to us. In order to do this we must reduce the risk of fraud to an absolute minimum.
- 4.0 This Policy Statement, together with the Anti-Money Laundering Strategy, is intended to provide advice and information to Employees and Councillors but suppliers, contractors and the general public are also encouraged to use this advice and guidance.



Chief Executive



Leader of the Council

TAMWORTH BOROUGH COUNCIL ANTI-MONEY LAUNDERING POLICY

1. Introduction

Although local authorities are not directly covered by the requirements of the Money Laundering Regulations 2007, guidance from CIPFA indicates that they should comply with the underlying spirit of the legislation and regulations.

Tamworth Borough Council is committed to the highest possible standards of conduct and governance, therefore, it has put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements.

All organisations, including the Council, must report any money laundering suspicions for cash transactions over 15,000 Euros. **To help prevent money laundering, the Council has set a cash payment limit of £5,000. No cash payments above £5,000 are to be accepted by any Council service.**

This is not designed to prevent customers making payments for Council services but to minimise the risk to the Council of high value cash transactions.

2. Scope of the Policy

This policy applies to all employees, whether permanent or temporary, and Members of the Council.

Its aim is to enable employees and Members to respond to a concern they have in the course of their dealings for the Council. Individuals who have a concern relating to a matter outside work should contact the Police.

3. Definition of Money Laundering

Money laundering is a general term for any method of disguising the origin of “dirty” or criminal money. This money may be the proceeds of any criminal activity including terrorism, drugs trafficking, corruption, tax evasion and theft. The purpose of money laundering is to hide the origin of the dirty money so that it appears to have come from a legitimate source. Unfortunately, no organisation is safe from the threat of money laundering, particularly where it is receiving funds from sources where the identity of the payer is unknown. It is, therefore, possible that Council may be targeted by criminals wishing to launder the proceeds of crime.

In addition, it is possible that the proceeds of crime may be received from individuals or organisations who do not realise that they are committing an offence. It is no defence for the payer or the recipient to claim that they did not know that they were committing an offence if they should have been aware of the origin of the funds. All staff therefore dealing with the receipt of funds or having contact with third parties from whom funds may be received need to be aware of the possibility of money laundering taking place.

Money laundering describes offences involving the integration of the proceeds of crime or terrorist funds into the mainstream economy. Such offences are defined under the Proceeds of Crime Act 2002 (“the Act”); the following are ‘prohibited acts’:

- Concealing, disguising, converting, transferring or removing criminal property from the UK
- Becoming involved in an arrangement which an individual knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquiring, using or possessing criminal property
- Failure to disclose one of the offences listed above, where there are reasonable grounds for knowledge or suspicion
- Doing something that might prejudice an investigation e.g. falsifying a document
- Tipping off a person(s) who is or is suspected of being involved in money laundering in such a way as to reduce the likelihood of or prejudice an investigation

Provided the Council does not undertake activities regulated under the Financial Services and Markets Act 2000, the offences of failure to disclose and tipping off do not apply. However, the Council and its employees and Members remain subject to the remainder of the offences and the full provisions of the Terrorism Act 2000.

The Terrorism Act 2000 made it an offence of money laundering to become concerned in an arrangement relating to the retention or control of property likely to be used for the purposes of terrorism, or resulting from acts of terrorism.

Although the term ‘money laundering’ is generally used to describe the activities of organised crime, for most people it will involve a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.

Potentially very heavy penalties (unlimited fines and imprisonment up to fourteen years) can be handed down to those who are convicted of one of the offences above.

It is important therefore that staff are aware of the rules and procedures that the Council has in place to ensure that they comply with the relevant legislation and approach taken by the Council as set out in this policy.

4. Requirements of the Money Laundering Legislation

The main requirements of the legislation are:

- To appoint a money laundering reporting officer
- Maintain client identification procedures in certain circumstances
- Implement a procedure to enable the reporting of suspicions of money laundering
- Maintain record keeping procedures

5. The Money Laundering Reporting Officer (MLRO)

The Council has designated the Monitoring Officer as the Money Laundering Reporting Officer (MLRO). She can be contacted on 01827 709258 or by email jane-hackett@tamworth.gov.uk.

In the absence of the MLRO or in instances where it is suspected that the MLRO could be involved in suspicious transactions, concerns should be raised with the Section 151 Officer – Executive Director (Corporate Services). He can be contacted on 01827 709252 or by email john-wheatley@tamworth.gov.uk.

6. Due Diligence Procedures

The Money Laundering Regulations require us to carry out “Customer Due Diligence”. Staff should therefore be alert to where Tamworth Borough Council (TBC) may be targeted by individuals trying to launder the proceeds of crime; avoid alerting anyone dealing with TBC that they have a suspicion that they may be attempting to launder, or have laundered, the proceeds of crime; and to report any suspicions of money laundering. Any suspicions must be reported to the Money Laundering Reporting Officer.

Training will be provided to all relevant staff regarding money laundering to assist them in their awareness of how money laundering could take place and the appropriate method of dealing with this. In effect, any areas where money changes hands could therefore be at risk of money laundering attempts, i.e. Application fees for taxi licences, planning applications, payment of housing benefits etc.

The Council already has procedures in place to limit the amount of cash that it receives, with other payment methods being made available. To ensure however that the system is manageable, if a cash payment of less than £5,000 is received; no identification checks will be needed.

Where the £5,000 limit is exceeded, officers dealing with the matter will need to establish the identity of the individual/company involved to seek to ensure that the risk of receiving the proceeds of crime can be minimised.

For individuals, their passport or photo driving licence should be provided, together with one of the following:

- Utility bills i.e. electricity, water etc. however mobile phone bills are not acceptable
- Mortgage/building society/bank statements
- Credit card statements
- Pension or benefit books

If passport or photo driving licence is not available, then two of the other items listed above will need to be produced.

For companies, a Companies House Search should be undertaken to confirm the existence of the company and identify who the directors are. Personal identification should then be obtained for the representatives of the company together with proof of their authority to act on behalf of the company. Care should be taken if it becomes

clear that the individual has only recently become a director of the company or if there has been a recent change in the registered office.

For any other type of organisation, for example a sole trader or partnership, personal identification should be obtained for the individuals together with documents indicating their relationship to the organisation.

Copies of any evidence provided in support of the identification of an individual or organisation should be kept on a central file so that it can be referred to later if necessary. Records should be kept for 5 years after the end of the transaction.

7. Procedure for Reporting Suspicious Transactions

Any suspicious transactions which staff may become aware of in the course of their work must be reported to the MLRO immediately using the Council's Internal Disclosure Form (see Appendix 2). Failure to make the appropriate report immediately will be regarded as gross misconduct and may result in dismissal without notice or pay in lieu of notice.

The report must include as much detail as possible including:

- Full details of the people involved
- Full details of the nature of their/your involvement.
- The types of money laundering activity involved
- The date(s) of such activity/ies
- Whether the transactions have happened, are ongoing or are imminent;
- Where they took place (if applicable);
- How they were undertaken (if applicable);
- The (likely) amount of money/assets involved;
- Why, exactly, you are suspicious.

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 her to prepare a report to the National Crime Agency (NCA), where appropriate. You should also enclose copies of any relevant supporting documentation.

It is imperative that, if staff have a suspicion concerning an individual or organisation with which they are dealing that they do not alert them to that suspicion i.e. that no "tipping off" is done. Staff must, therefore, **not** make them aware that an internal disclosure report may be made. Once the report is made, the cash/cheques/other form of payment from this source should not be banked until clearance has been received from the MLRO. Such clearance may take up to seven days from the time when the initial report to the MLRO is made.

If the funds are banked in this period without getting clearance from the MLRO that staff members runs the risk of a fine and/or imprisonment for up to 14 years.

8. Additional Guidance

If you require any additional information or guidance in relation to the contents of this policy and your responsibilities please contact either the MLRO or his deputy. An Aide Memoir has been prepared – Appendix 3, which can be used as a brief reminder to staff of their responsibilities.

9. Consideration of the disclosure by the Money Laundering Reporting Officer

Upon receipt of a report, the MLRO must note the date thereof and acknowledge receipt. She should also advise you of the timescale within which she expects to respond to you.

The MLRO will consider the report and any other available internal information she thinks relevant e.g.

- reviewing other transaction patterns and volumes;
- the length of any business relationship involved;
- the number of any one-off transactions and linked one-off transactions;
- any identification evidence held;

She will also undertake such other reasonable inquiries that are 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.

Once the MLRO has evaluated the report and any other relevant information, she must make a timely determination as to whether:

- there is actual or suspected money laundering taking place; or
- there are reasonable grounds to know or suspect that is the case; and
- there is a requirement to seek consent from the NCA for a particular transaction to proceed.

Where the MLRO does so conclude, then she must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless she has a reasonable excuse for non-disclosure to the NCA (for example, if you are a lawyer and you wish to claim legal professional privilege for not disclosing the information).

Where the MLRO suspects money laundering but has a reasonable excuse for non-disclosure, then she must note this accordingly; she can then immediately give her consent for any ongoing or imminent transactions to proceed.

In cases where legal professional privilege may apply, the MLRO must liaise with the Section 151 Officer to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

Where consent is required from the NCA for a transaction to proceed, then the transaction(s) 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.

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then she shall note this accordingly and give consent for any ongoing or imminent transaction(s) to proceed.

All reports referred to the MLRO and reports made by her to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

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

10. Training

Officers considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training. In effect, any areas where money changes hands could therefore be at risk of money laundering attempts ie. application fees for taxi licences, planning applications, payment of housing benefits etc.

Additionally, all employees and Members will be familiarised with the legal and regulatory requirements relating to money laundering and how they affect both the Council and themselves.

Notwithstanding the paragraphs above, it is the duty of officers and Members to report all suspicious transactions whether they have received their training or not.

11. Conclusions

The Council has put into place a number of arrangements to protect itself from the risk of money laundering. However in the current climate of change there are issues that will increase this risk. Changes in structure, changes in systems and the turnover of staff all contribute to our exposure to the risk of money laundering. To mitigate against this risk the Council will regularly review arrangements.

The Money Laundering Policy provides a framework for preventing and tackling money laundering acts against the Authority. The approval of the Policy by the Audit and Governance Committee and the Council demonstrates the Council's commitment to protecting public funds. Having made this commitment, it is imperative that the MLRO puts in place arrangements for disseminating the Policy and promoting money laundering awareness, throughout the Council. The Council believes that this policy represents a proportionate response to the level of risk it faces from money laundering offences.

12. Review

This policy and associated procedure will be subject to a review every 2 years unless any changes or updates to any of the relevant legislation require that it is undertaken sooner.

Role of the Money Laundering Report Officer – “MLRO”

The duties of the Money Laundering Reporting Officer are:

- To ensure that the Council complies with the requirements of the Money Laundering Regulations 2007 and the Proceeds of Crime Act 2002.
- To ensure that all relevant staff are aware of and comply with the Council’s Money Laundering Policy.
- To ensure that the Council properly identifies all third parties dealing with the Council where there is a higher risk of the Council receiving the proceeds of crime and to ensure that copies of any documents taken as proof of evidence are kept on a central file by the Council.
- To ensure that all relevant staff receives training on how to identify, deal with and prevent money laundering.
- To ensure that all necessary disclosures to the National Crime Agency (NCA) are made and that they are made as soon as practically possible after the suspicion has been raised.
- To decide whether a suspicious transaction report requires a disclosure to be made to NCA.
- To liaise with NCA regarding the outcome of the disclosure and update staff accordingly.



MONEY LAUNDERING – INTERNAL REPORTING FORM

Money laundering legislation requires all individuals within the Council to report any knowledge or suspicions that they might have of money laundering (as defined in the Proceeds of Crime Act 2002) to the Council's Money Laundering Reporting Officer. To assist individuals the following pro forma has been developed. Particular circumstances may require different information to be disclosed and this should be fully explained, if applicable.

Instructions for Completion

It is your legal duty and a requirement of your employment with Tamworth Borough Council that you report any suspicion concerning proceeds of crime to:

**Money Laundering Reporting Officer
 Tamworth Borough Council
 Marmion House
 Lichfield Street
 Tamworth
 Staffordshire
 B79 7BZ**

This should be marked **URGENT – **RESTRICTED** TO THE ADDRESSEE ONLY.**

You are also reminded that “**Tipping-Off**” is a criminal offence. You should therefore avoid discussing the content of this report with anyone other than the Money Laundering Reporting Officer.

| | | | |
|------------------------------|--|-------------------------------|--|
| Date of Report: | | Date suspicion first aroused: | |
| Prepared by: Name & Dept: | | | |
| Disclosure Type: | (ie. Connections to crime/drugs/terrorism) | | |

Main Subject (Person)

| | | | | | |
|--------------------|--|--------------|---------------------------|------------------|--|
| Surname: | | Forename(s): | | Title: | |
| Date of Birth: | | Gender: | | | |
| Occupation: | | Employer: | | | |
| Address: (in full) | | Postcode: | Home/Business /Registered | Current/Previous | |
| | | | | | |

Or**Main Subject (Company)**

| | | | | | |
|--------------------|--|-------------|---------------------------|------------------|--|
| Company Name: | | Company No: | | | |
| Type of Business: | | VAT No: | | | |
| Country of Reg: | | | | | |
| Address: (in full) | | Postcode: | Home/Business/ Registered | Current/Previous | |
| | | | | | |

Bank Account Details

| | | | |
|---------------|--|-------------|--|
| Account Name: | | Sort Code: | |
| Opened: | | Account No: | |
| Closed: | | Balance: | |

Other Information

Any information/evidence held to confirm identification and/or address, ie. Passport/driving licence etc:

Connected Subject Person (if any)

| | | | | | |
|--------------------|--|--------------|---------------------------|------------------|--|
| Surname: | | Forename(s): | | Title: | |
| Date of Birth: | | Gender: | | | |
| Occupation: | | Employer: | | | |
| Address: (in full) | | Postcode: | Home/Business /Registered | Current/Previous | |
| | | | | | |

**Or
Connected Subject Company (if any)**

| | | | |
|--------------------|-----------|--------------------------|------------------|
| Company Name: | | Company No: | |
| Type of Business: | | VAT No: | |
| Country of Reg: | | | |
| Address: (in full) | Postcode: | Home/Business/Registered | Current/Previous |
| | | | |

Bank Account Details

| | | | |
|---------------|--|-------------|--|
| Account Name: | | Sort Code: | |
| Opened: | | Account No: | |
| Closed: | | Balance: | |

Other Information

| |
|---|
| Any information/evidence held to confirm identification and/or address, ie. Passport/driving licence etc: |
| |

Reason for the Suspicion

| | | |
|--|------------------------------|-----------|
| Please tick any or all of the following which might apply | | |
| Drugs | Personal Tax Fraud | Vat Fraud |
| Crime | Company Tax Fraud | |
| Immigration | Tobacco/Alcohol Excise Fraud | |
| Following on from above, please set out the reason for the suspicion: | | |
| Please continue on separate sheet if required | | |
| Names of all other colleagues (principals and staff) who have been involved in the case | | |
| | | |

Declaration

The above is an accurate account of the facts that are available to me at the time of making the report. If I become aware of additional and/or changes in the information provided I will disclose these to the Money Laundering Reporting Officer in a timely manner. I am aware of the risks and penalties regarding “tipping-off” or frustrating in any way an investigation of the above or related matters by the authorities.

Signed: _____ Date: _____

Name in Full: _____ Position: _____

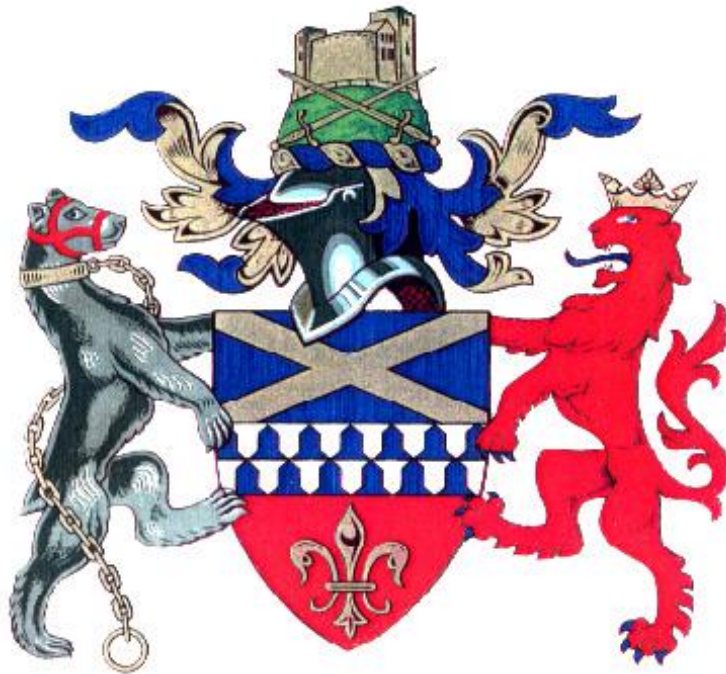
MONEY LAUNDERING AVOIDANCE AIDE MEMOIR

1. No member of staff must accept cash of more than £5,000 from any member of the public.
2. If you are offered cash of more than £5,000 you should advise the person offering it to you that it is not Council policy to accept large amounts of cash of more than £5,000 and that you need to obtain guidance from a senior member of staff. You should then contact the Money Laundering Reporting Officer to obtain authorisation to take cash, if appropriate.
3. Any large cash sums should not be banked in the first instance. The Money Laundering Reporting Officer should be contacted to seek guidance as to how to deal with the funds. Forms to report the matter are included in the policy document at Appendix 2.
4. Whilst it is not acceptable to be suspicious of all cash based businesses, anyone whom you know to be associated with such a business should be dealt with using a higher degree of scepticism. If you have any reason to suspect the source of their funds then you should contact the Money Laundering Reporting Officer to discuss your concerns, even if the payment is not received in cash.
5. If you receive a complaint from a member of the public in relation to possible criminal activity being carried out by someone who may be a customer of the Council (i.e. a Council Tax or Business Rates payer, rent payer, licensee etc) you must pass this on to the Money Laundering Reporting Officer.

TAMWORTH BOROUGH COUNCIL

POLICY & PROCEDURE

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)



Jane Marie Hackett
Solicitor to the Council
Tamworth Borough Council
Policy date: Review: Revised: January 2017

CONTENTS

| | Page No. | |
|------------------|--|---------|
| Section A | Introduction | 3 - 4 |
| Section B | Effective Date of Operation and Authorising Officer Responsibilities | 5 |
| Section C | General Information on RIPA | 7 |
| Section D | What RIPA Does and Does Not Do | 8 |
| Section E | Types of Surveillance | 9 - 11 |
| Section F | Conduct and Use of a Covert Human Intelligence Source (CHIS) | 12 - 16 |
| Section G | The Role of the RIPA Co-ordinator | 17 – 18 |
| Section H | Authorisation Procedures | 19 - 27 |
| Section I | Working with other Agencies | 28 |
| Section J | Record Management | 30 - 31 |
| Section K | Acquisition of Communications Data | 32 - 35 |
| Section L | Conclusion | 36 |
| Appendix 1 | A Forms – Directed Surveillance | 37 |
| Appendix 2 | B Forms – Conduct of a Covert Human Intelligence Source | 38 |
| Appendix 3 | C Forms –CHIS | 39 |
| Annex A | Local Authority Procedure | 40 |
| Annex B | P Procedure | 41 |
| Annex C | Application for Judicial Approval and Order Form | 42 - 44 |

Section A

Introduction

1. OBJECTIVE: SUSTAINABLE COMMUNITIES; SAFER AND STRONGER COMMUNITIES

Tamworth Borough Council is committed to improving the quality of life for the communities of Tamworth which includes benefiting from an attractive place to live, meeting the needs of local people and employers with opportunities for all to engage in community life. It also wishes to maintain its position as a low crime borough and a safe place to live, work and learn. Although most of the community comply with the law, it is necessary for Tamworth to carry out enforcement functions to take full action against those who flout the law. Tamworth Borough Council will carry out enforcement action in a fair, practical and consistent manner to help promote a thriving local economy.

2. HUMAN RIGHTS ACT 1998 – ARTICLE 8 – RIGHT TO RESPECT FOR PRIVATE & FAMILY LIFE, HOME AND CORRESPONDENCE

The Human Rights Act 1998 brought into UK domestic law much of the European Convention on Human Rights and Fundamental Freedoms 1950. Article 8 of the European Convention requires the Council to respect the private and family life of its citizens, their homes and their correspondence. Article 8 does, however, recognise that there may be circumstances in a democratic society where it is necessary for the state to interfere with this right.

3. USE OF COVERT SURVEILLANCE TECHNIQUES AND HUMAN INTELLIGENCE SOURCES

The Council has various functions which involve observing or investigating the conduct of others, for example, investigating anti-social behaviour, fly tipping, noise nuisance control, planning (contraventions), fraud, licensing and food safety legislation. In most cases, Council officers carry out these functions openly and in a way which does not interfere with a person's right to a private life. However, there are cases where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation. The use of covert surveillance techniques is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which seeks to ensure that the public interest and human rights of individuals are appropriately balanced. This document sets out the Council's policy and procedures on the use of covert surveillance techniques and the conduct and use of a Covert Human Intelligence Source. You should also refer to the two Codes of Practice published by the Government. These Codes are on the Home Office website and supplement the procedures in this document. The Codes are admissible as evidence in Criminal and Civil Proceedings. If a provision of these Codes appear relevant to any court or tribunal, it must be taken into account.

The Codes of Practice for both Covert Surveillance and Covert Human Intelligence Sources can be obtained by following the link below:

<https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>

There are also two other guidance documents relating the procedural changes regarding the authorisation process requiring Justice of the Peace approval from the 1st November 2012. These have been issued by the Home Office to both Local Authorities and Magistrates.

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/>

4. ACQUISITION OF COMMUNICATIONS DATA

RIPA also regulates the acquisition of communications data. Communications data is data held by telecommunications companies and internet service providers. Examples of communications data which may be acquired with authorisation include names, addresses, telephone numbers, internet provider addresses. Communications data surveillance does not monitor the content of telephone calls or emails. This document sets out the procedures for the acquisition of communications data. You should also refer to the Code of Practice which is available on the Home Office website.

Acquisition and Disclosure of Communications Data Revised Draft Code of Practice:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015

Section B

EFFECTIVE DATE OF OPERATION AND AUTHORISING OFFICER RESPONSIBILITIES

1. The Policy and Procedures in this document have been amended to reflect the latest Codes of Practice which are in force and the legislative amendments which require Justice of the Peace (JP) approval for all Local Authority RIPA applications and renewals, which came in effect on 1 November 2012, changes in website addresses and application forms, as well as to reflect recommendations arising out of inspection by the Office of Surveillance Commissioners and their guidance documents. It is essential, therefore, that Authorising Officers, take personal responsibility for the effective and efficient observance of this document and the Office of Surveillance Commissioners (OSC) guidance documents.
2. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained as 'Applicants'.
3. Authorising Officers will also ensure that staff who report to them follow this Policy and Procedures Document and do not undertake or carry out surveillance activity that meets the criteria as set out by RIPA without first obtaining the relevant authorisations in compliance with this document.
4. Authorising Officers must also pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until they are satisfied that
 - the health and safety of Council employees/agents are suitably addressed
 - risks minimised so far as is possible, and
 - risks are proportionate to the surveillance being proposed.

If an Authorising Officer is in any doubt, prior guidance should be obtained from the Solicitor to the Council.

5. Authorising Officers must also ensure that, when sending copies of any Forms to the Solicitor to the Council (or any other relevant authority), that they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.
6. In Accordance with the Codes of Practice, the Senior Responsible Officer (SRO) who is the Solicitor to the Council is responsible for
 - the integrity of the process in place within the public authority to authorise directed and intrusive surveillance
 - compliance with Part II of the 2000 Act, and with this code;
 - engagement with the Commissioners and inspectors when they conduct their inspections, and
 - where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

The Solicitor to the Council is also the RIPA Co-ordinator. The key responsibilities of the RIPA Co-ordinator are set out in Section G of this document.

7. The Chief Executive in consultation with Corporate Management Team has power to appoint Authorising Officers for the purposes of RIPA. Authorising Officers will only be appointed on the Chief Executive being satisfied that suitable training on RIPA has been undertaken.
8. The Solicitor to the Council will review the policy every six months and annual reports on performance of the policy will be presented to Council.
9. Quarterly reports on the use of RIPA will be considered by the Audit and Governance Committee.

Section C

GENERAL INFORMATION ON RIPA

1. The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their homes and their correspondence.
2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-
 - (a) **in accordance with the Law;**
 - (b) **necessary** in the circumstances of the particular case; **and**
 - (c) **proportionate** to what it seeks to achieve.
3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (ie. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('**CHIS**') – eg. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA and this Policy and Procedure document seeks to ensure both the public interest and the human rights of individuals are suitably balanced.
4. Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf, must be properly authorised by one of the Council's designated Authorising Officers. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. It is also important that the Authorising Officer is aware of the abilities of the operatives to ensure they are capable of undertaking the surveillance. Please refer to Section H and to the paragraph on "Authorising Officers."
5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman and/or the Council could be ordered to pay compensation.

Section D

WHAT RIPA DOES AND DOES NOT DO

1. RIPA:

- requires prior authorisation of directed surveillance.
- prohibits the Council from carrying out intrusive surveillance.
- requires authorisation of the conduct and use of a CHIS.
- requires safeguards for the conduct and use of a CHIS.

2. RIPA does not:

- make lawful conduct which is otherwise unlawful.
- prejudice or affect any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, the Council's current powers to obtain information from the DVLA or from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Solicitor to the Council BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Section E

TYPES OF SURVEILLANCE

'Surveillance' includes:

- monitoring, observing and listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It may be conducted with or without the assistance of a surveillance device.
- recording anything mentioned above in the course of authorised surveillance.

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. They will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded).

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

Directed Surveillance is surveillance which:-

- is **covert**; and
- is **not intrusive surveillance** (see definition below – the Council cannot carry out any intrusive surveillance).
- is not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act reasonable, eg. spotting something suspicious and continuing to observe it; and
- it is 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 purposes of an investigation). (*Section 26(10) RIPA*).

Private Information in relation to a person includes any information relating to his private and family life, his home or his correspondence. The fact that covert

surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact. Private information may include personal data such as names, addresses or telephone numbers. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Privacy considerations are likely to arise if several records are examined together to establish a pattern of behaviour.

For the avoidance of doubt, only those Officers appointed as ‘Authorising Officers’ for the purpose of RIPA can authorise ‘Directed Surveillance’ IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, are followed.

Intrusive Surveillance

This is when it:-

- is covert;
- relates to residential premises and private vehicles, even if used on a temporary basis and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/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/vehicle.

This form of surveillance can be carried out only by police and other law enforcement agencies. Intrusive surveillance relates to the location of the surveillance, and not any consideration of the information that is likely to be obtained. Council officers cannot carry out intrusive surveillance.

“Proportionality”

This term contains three concepts:-

- the surveillance should not be excessive in relation to the gravity of the matter being investigated;
- the least intrusive method of surveillance should be chosen; and
- collateral intrusion involving invasion of third parties’ privacy and should, so far as possible, be minimised.

Proportionality involves balancing the intrusiveness of the activity on the subject and others who might be affected by it against the need for the activity in operational

terms. The activity will not be proportionate if it is excessive in the circumstances of the case, or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers :

- 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.

When considering the intrusion, it is important that the Authorising Officer is fully aware of the technical capabilities of any proposed equipment to be used, and that any images are managed in line with the Data Protection Act and Home Office Guidance. These issues have a direct bearing on determining proportionality.

Section F

Covert Human Intelligence Source (CHIS)

Staff will need to know when someone providing information may become a CHIS, and in these circumstances the Council is required to have procedures in place should this be necessary. However, if it appears that use of a CHIS may be required, Authorising Officers must seek legal advice from the Solicitor to the Council.

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However, the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources.

Under section 26(8) of the 2000 Act a person is a source if:

- a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
- b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

Conduct and Use of a Source

The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

The **conduct of a source** is any conduct falling within a), b), or c), mentioned above, or which is incidental to anything falling within those sections.

The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

When completing applications for the use of a CHIS, the applicant must state who the CHIS is, what they can do and for which purpose.

When determining whether a CHIS authorisation is required, consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

Management of Sources

Within the provisions there has to be;

- (a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare (**Handler**)
- (b) at all times there will be another person who will have general oversight of the use made of the source (**Controller**)
- (c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare;

The **Controller** will be responsible for the general oversight of the use of the source.

Tasking

Tasking is the assignment given to the source by the Handler or Controller by asking him to obtain information, to provide access to information, or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a source may be tasked with finding out purely factual information about the layout of

commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice

Management Responsibility

The Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary, the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

Security and Welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

Record Management for CHIS

Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are;

- a. the identity of the source;
- b. the identity, where known, used by the source;
- c. any relevant investigating authority other than the authority maintaining the records;
- d. the means by which the source is referred to within each relevant investigating authority;

- e. any other significant information connected with the security and welfare of the source;
- f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- g. the date when, and the circumstances in which the source was recruited;
- h. the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- i. the periods during which those persons have discharged those responsibilities;
- j. the tasks given to the source and the demands made of him in relation to his activities as a source;
- k. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- l. the information obtained by each relevant investigating authority by the conduct or use of the source;
- m. any dissemination by that authority of information obtained in that way; and
- n. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her. Only the Chief Executive, or in his absence, the Deputy Chief Executive can authorise the use of a juvenile as a source.

Vulnerable Individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive, or in his absence, the Executive Director Corporate Services can authorise the use of a vulnerable individual as a source.

Test Purchases

Carrying out test purchases will not normally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation as a CHIS would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance. However it will be necessary to complete the relevant separate application forms.

Authorising Officers should consider the likelihood that the test purchase will lead to a relationship being formed with a person in the shop. If the particular circumstances of a particular test purchase are likely to involve the development of a relationship Authorising Officers must seek legal advice from the Solicitor to the Council.

If several shop premises are included on one application for Directed Surveillance, each premises will be required to be assessed by the Authorising Officer individually on their own merits.

Anti-Social Behaviour Activities (e.g. Noise, Violence, Race etc.)

As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour, unless there are criminal offences involved which attract a maximum custodial sentence of six months. Should it be necessary to conduct covert surveillance for disorder which does not meet the serious crime criteria of a custodial sentence of a maximum of six months, this surveillance would be classed as surveillance outside of RIPA, and would still have to meet the Human Rights Act provisions of Necessity and Proportionality

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (eg. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Section G

THE ROLE OF THE RIPA CO-ORDINATOR

Key Responsibilities of the RIPA Co-ordinator

In this document the RIPA Co-ordinator is the Solicitor to the Council. The key responsibilities of the RIPA Co-ordinator are to:

- Retain all applications for authorisation (including those that have been refused), renewals and cancellations for a period of at least **three years** together with any supplementary documentation;
- Provide a unique reference number and maintain the central register of all applications for authorisations whether finally granted or refused (see section below);
- Create and maintain a spread sheet for the purpose of identifying and monitoring expiry dates and renewal dates although the responsibility for this is primarily that of the officer in charge and the Authorising Officer;
- Retain an oversight of the authorisation process
- Monitor types of activities being authorised to ensure consistency and quality throughout the Council;
- Ensure sections identify and fulfil training needs;
- Periodically review Council procedures to ensure that they are up to date;
- Assist Council employees to keep abreast of RIPA developments by organising training and raising RIPA awareness throughout the Council;
- Provide a link to the Surveillance Commissioner and disseminate information on changes on the law, good practice etc. Officers becoming aware of such information should, conversely, send it to the RIPA Co-ordinator for this purpose;
- Check that Authorising Officers carry out reviews and cancellations on a timely basis.

Central Record of Authorisations

A centrally retrievable record of all authorisations will be held by the RIPA Co-ordinator (Solicitor to the Council) which must be up-dated whenever an authorisation is granted, renewed or cancelled. These records will be retained for a period of **three years** from the ending of the authorisation and will contain the following information:

- The type of authorisation;
- The date the authorisation was given;

- The date approved by the Magistrate
- The name and title of the Authorising Officer;
- The unique reference number of the investigation (URN);
- The title of the investigation or operation, including a brief description and the names of the subjects, if known;
- Whether the investigation will obtain confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- The dates the authorisation is reviewed and the name and title of the Authorising Officer;
- If the authorisation is renewed, when it was renewed and the name and title of the Authorising Officer;
- The date the authorisation was cancelled.
- Joint surveillance activity where Council staff have been authorised on another agencies authorisation will also be recorded.

Access to the data will be restricted to the RIPA Co-ordinator and Authorising Officers to maintain the confidentiality of the information.

Section H

AUTHORISATION PROCEDURES

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Authorising Officers

Forms can only be signed by Authorising Officers. The Authorising Officers are:

| | |
|---|----------------|
| Chief Executive | Tony Goodwin |
| Executive Director Corporate Services | John Wheatley |
| Corporate Director Growth Assets & Environment | Andrew Barratt |

Appointment of the aforesaid officers is subject to the training requirements set out in the paragraph below.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and any internal departmental Schemes of Management.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled at the earliest opportunity once the specific surveillance is complete. **The authorisations do not lapse with time.**

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises such an investigation or operation the centrally retrievable record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during the next inspection.

Training

Authorising Officers will only be appointed if the Chief Executive is satisfied that they have undertaken suitable training on RIPA. Evidence of suitable training is to be supplied in the form of a certificate/confirmation from the trainer to the effect that the Authorising Officer has completed a suitable course of instruction.

The Solicitor to the Council will maintain a Register of Authorising Officers and details of training undertaken by them.

If the Chief Executive is of the view that an Authorising Officer has not complied fully with the requirements of this document, or the training requirements then that Officer's authorisation can be withdrawn until they have undertaken further approved training or has attended a one-to-one meeting with the Chief Executive.

Grounds for Authorisation

On 1 November 2012 two significant changes came into force that effects 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 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**
- **Directed surveillance crime threshold:** The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 ("the 2012 Order") states that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating (1) criminal offences which attract a maximum custodial sentence of six months or more or (2) criminal offences under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 relating to the sale of alcohol or tobacco products to children.

The crime threshold, as mentioned is only for Directed Surveillance.

Therefore the only lawful reason is **prevention and detection of crime** in respect of its Core Functions. As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months.

APPLICATION PROCESS

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete

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

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP.

The Authorising Officer will be expected to attend the hearing along with the applicant officer. Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the Solicitor to the Council.

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

The original RIPA application/authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA application/ authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. **However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.**

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to:

Approve the Grant or renewal of an authorisation

The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case. The duration of the authorisation commences with the magistrate's approval.

Refuse to approve the grant or renewal of an authorisation

The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the application/authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, The officers are now allowed to undertake the activity.

The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the Authorising Officer.

A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will decide what action if any should be taken.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Application, Review, Renewal and Cancellation Forms

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP’s approval. The duration of the authorisation commences with the magistrate’s approval. (see procedure above RIPA application and authorisation process)

Duration of Applications

| | |
|---|------------------|
| Directed Surveillance | 3 Months |
| Renewal | 3 Months |
| Covert Human Intelligence Source | 12 Months |
| Juvenile Sources | 1 Month |
| Renewal | 12 months |

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire. (See cancellations page 16)

Reviews

The reviews are dealt with internally by submitting the review form to the authorising officer. In such circumstances seek advice from the RIPA Co-ordinator. There is no requirement for a review form to be submitted to a JP. However if a different surveillance techniques is required it is likely a new application will have to be completed and approved by a JP.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation, this must be approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusion issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has

been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the authorising officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

Cancellation should take place at the earliest opportunity.

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraph 5.18 in the Codes of Practice). **It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Senior Responsible Officer.**

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Before an Authorising Officer signs a Form, they must:-

- (a) Be mindful of this Policy & Procedures Document and the training undertaken
- (b) Be satisfied that the RIPA authorisation is:-

- (i) **in accordance with the law;**
- (ii) **necessary** in the circumstances of the particular case on the ground mentioned

and

- (iii) **proportionate** to what it seeks to achieve. (see section on proportionality)
- (c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information.

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

The following elements of proportionality should therefore be considered:

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, what other methods have been considered and why they were not implemented.

The least intrusive method will be considered proportionate by the courts.

- (d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. This matter may be an aspect of determining proportionality;
- (e) Set a date for review of the authorisation and review on only that date;
- (f) Obtain a Unique Reference Number (URN) for the application from the Solicitor to the Council on 01827 709258
- (g) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Solicitor to the Council, Central Register, **within 5**

working days of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer must also:-

- (a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.
- (b) Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;
- (c) Consider the likely degree of intrusion of all those potentially affected;
- (d) Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
- (e) Ensure **records** contain particulars and are not available except on a need to know basis.
- (f) Ensure that if the CHIS is under the age of 18 or is a vulnerable adult the Authorising Officer is the Chief Executive or in his absence, the Deputy Chief Executive.

The Authorising Officer must attend to the requirement of section 29(5) RIPA and of the Regulation of Investigatory Powers (Source Records) Regulations 2000. It is strongly recommended that legal advice is obtained in relation to the authorisation of a CHIS.

Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation is to take place.

Urgent Authorisations

As from 1 November 2012 there is now no provision under RIPA for urgent oral authorisations.

Section I

WORKING WITH / THROUGH OTHER AGENCIES

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. The agency must be made aware explicitly what they are authorised to do. The agency will be provided with a copy of the application form (redacted if necessary) or at the least the authorisation page containing the unique number.

Equally, if Council staff are authorised on another agencies RIPA authorisation, the staff will obtain a copy of the application form (redacted if necessary), or at the least the authorisation page containing the unique number, a copy of which should be forwarded for filing within the central register. They must ensure that they do not conduct activity outside of that authorisation.

Provisions should also be made regarding any disclosure implications under the Criminal Procedures Act (CPIA) and the management, storage and dissemination of any product obtained.

When another agency (e.g. Police, Customs & Excise, Inland Revenue etc):-

- (a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, the Officer must obtain a copy of that agency's RIPA form (redacted if necessary) or at the least the authorisation page containing the unique number for the record (a copy of which must be passed to the Solicitor to the Council for the Central Register) Should this be an urgent oral authorisation they should obtain a copy of the contemporaneous notes of what has been authorised by the Authorising Officer in line with current guidance. A copy of these notes will be forwarded for filing in the central register.
- (b) wish to use the Council's premises for their own RIPA action, the Chief Officer or Head of Service should, normally, cooperate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's cooperation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

If the Police or any other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other Agency before any Council resources are made available for the proposed use.

If in doubt, please consult with the Solicitor to the Council at the earliest opportunity.

Section J

RECORD MANAGEMENT

The Council must keep detailed records of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Solicitor to the Council.

Records Maintained in the Department

The following documents must be retained by the Department authorising the surveillance:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

Central Register maintained by the Solicitor to the Council

Authorising Officers must forward a copy of the form to the Solicitor to the Council for the Central Register, within 5 working days of the authorisation, review, renewal, cancellation or rejection. The Solicitor to the Council will monitor the same and give appropriate guidance to Authorising Officers from time to time, or amend this document in the light of changes of legislation or developments through case law.

Retention and Destruction of Material

The retention of the material obtained during a RIPA operation is governed by the Criminal Procedures Investigations Act (CPIA) 1996 and the Data Protection Act 1998.

Arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS. Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and

any relevant codes of practice produced by individual authorised relating to the handling and storage of material.

The Council will retain records for a period of at least five years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations. The Office of the Surveillance Commissioners will also write to the Council from time to time, requesting information as to the numbers of authorisations made in a specific period. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Errors

There is a requirement as set out in the OSC procedures and Guidance 2011 to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

Section K

ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

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

Powers

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies (“Communications Companies”).

S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a private telecommunications company is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.

In order to compel a communications company to obtain and disclose, or just disclose communications data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a permitted Local Authority is for the purposes of “preventing or detecting crime or of preventing disorder”. The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Company will most probably have means of collating and providing the communications data requested.

Single Point of Contact

In accordance with the Home Office Acquisition and Disclosure of Communications Data Code of Practice the Council is required to have a “the Council Single Point of Contact” is NAFN. The role of the SPoC is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data. Before an officer can be a SPoC specialist training recognised by the Home Office has to be undertaken. A SPoC must also register his or her details with the Home Office. The Solicitor of the Council is SPoC for Tamworth Borough Council.

Details of the training undertaken is kept in the Central Register.

The functions of the SPoC are to:

- Assess, where appropriate, whether access to communications data is reasonably practical for the postal or telecommunications operator;

- Advise Applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators
- Advise Applicants and Authorising Officers on whether communications data falls under section 21(4)(a), (b) or (c) of RIPA
- Provide safeguards for authentication
- Assess any cost and resource implications to both the Council and postal or telecommunications operator.

The Senior Responsible Officer

In accordance with the Code of Practice each public authority must have a Senior Responsible Officer who is responsible for:

- The integrity of the process in places within the public authority to acquire communications data;
- Compliance with Chapter II of Part 1 of RIPA and with the Code;
- Oversight of the reporting of errors to the Interception of Communications Commissioner's Office (IOCCO) and the identification of both the cause of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the IOCCO inspectors when they conduct their inspections and;
- Where necessary, oversee the implementation of post – inspection action plans approved by the Commissioner

The Council's Senior Responsible Officer is the Solicitor to the Council.

Application Forms

Only the approved Accessing Communications Data forms referred to in Appendix 4 must be used. The forms have to be downloaded and completed in the Applicants handwriting

Procedure

All applications to obtain communications data must be channelled through the SPoC. If an investigating officer is considering making an application to obtain communications data they should contact the SPoC for advice and to obtain the appropriate forms.

In completing the forms the investigating officer must address the issues of necessity, proportionality and collateral intrusion. The following is guidance on the principles of necessity, proportionality and collateral intrusion.

“Necessity” should be a short explanation of the crime (together with details of the relevant legislation), the suspect, victim or witness and the telephone or communications address and how all these three link together. It may be helpful to outline the brief details of the investigation and the circumstances leading to the application as this will assist with justifying necessity. The source of the telephone number or communications address should also be outlined. E.g. if the number was

obtained from itemised billing or a business flyer there should be specific identifiers such as the telephone number or exhibit number.

As regards “proportionality” there should be an outline of what the investigating officer expects to achieve from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. The investigating officer should give an explanation as to why specific date/time periods of data have been requested. An explanation of what is going to be done with the communications data once it is acquired and how that action will benefit the investigation will assist with the justification of proportionality. The investigating officer should outline what other checks or methods have been tried e.g. visiting other known addresses, ringing the number etc. or why such methods are not deemed feasible.

“Collateral intrusion” should also be addressed on the suspect or individual in question to demonstrate that the intrusion is not arbitrary or unfair. There will only be minimal collateral intrusion in relation to subscriber checks or none will be identified at the time of making the application. In some case it will be clear that the suspect has been contacted on the actual telephone number by the complainant or the investigating officer and therefore this reduces the potential for collateral intrusion. Investigating officers should also mention whether it is known that the telephone number (or other type of data) has been used to advertise the business, either in the press/internet or on business cards/flyers as this would also be evidence to show that the suspect is actually using the telephone number and further reduce the potential for collateral intrusion. Collateral intrusion becomes more relevant when applying for service use data and investigating officers should outline specifically what collateral intrusion may occur, how the time periods requested impact on collateral intrusion and whether they are likely to obtain data which is outside the realm of their investigation.

Once the investigating officer has completed the application form it should be passed to the SPoC together with a draft Notice to the Communications Service Provider. If the SPoC is satisfied that the application should proceed, the Application and the draft Notice to the Communications Service Provider will be considered by an Authorising Officer¹. If the SPoC decides that the application is not justified it will be rejected. If the SPoC requires further information in order to consider the application this will be requested from the investigating officer and recorded on the SPoC Log Sheet.

The Authorising Officer must consider:

- (a) whether the case justifies the accessing of communications data for the **purposes of preventing or detecting crime or of preventing disorder** and why obtaining the data is **necessary** in order to achieve the aims of the investigation and on the grounds permitted to the Council;

and

- (b) whether obtaining access to the data by the conduct authorised, or required of the postal or telecommunications operator in the case of a notice, is **proportionate** to what is sought to be achieved.

The Authorising Officer will complete the Application Form as appropriate.

If the Authorising Officer becomes directly involved in the operation, such involvement and their justification for undertaking the role of Authorising Officer must be explicit in the written considerations on the Application Form or alternatively the application should be passed to another Authorising Officer for consideration.

If the accessing of communications data is authorised the Authorising Officer will sign the Notice to the Communication Service Provider, complete the date/time of issue and return all forms to the SPoC

The SPoC will then issue the Notice to the Communications Service Provider

1. NOTE: The Code of Practice referred to in paragraph 5 above refers to "Designated Persons" as those whose authority is obtained with regard to the application. However, for the purposes of this policy and procedure the term "Authorising Officer" will be used for that of "Designated Person".

Duration

Authorisations and notices are only valid for one month. A shorter period should be specified if this is satisfied by the request. An authorisation or notice may be renewed during the month by following the same procedure as obtaining a fresh authorisation or notice.

An Authorising Officer shall cancel an authorisation or notice as soon as it is no longer necessary or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

Record Management

Applications, authorisations and notices for communications data must be retained by the SPoC until audited by the IOCCO. All such documentation must be kept in locked storage.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record shall be kept and a report and explanation sent to the IOCCO as soon as reasonably practicable.

Oversight

The IOCCO will write to the Council from time to time requesting information as to the numbers of applications for communications data and confirmation as to whether there have been any errors which have occurred when obtaining data communications. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Section L

CONCLUSION

Obtaining an authorisation under RIPA and following the guidance and procedures in this document will assist in ensuring that the use of covert surveillance or a CHIS is carried out in accordance with the law and subject to safeguards against infringing an individual's human rights. Complying with the provisions of RIPA protects the Council against challenges for breaches of Article 8 of the European Convention on Human Rights.

Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.

Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on RIPA, please contact the Solicitor to the Council (who is also the Monitoring Officer).

APPENDIX 1

A FORMS

DIRECTED SURVEILLANCE

All forms can be obtained from:

<https://www.gov.uk/government/collections/ripa-forms--2>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Application for Authorisation Directed Surveillance

Application for Review of a Directed Surveillance Authorisation

Application for Renewal of a Directed Surveillance Authorisation

Application for Cancellation of a Directed Surveillance Authorisation

APPENDIX 2

B FORMS

CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

All forms can be obtained from:

<https://www.gov.uk/government/collections/ripa-forms--2>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Application for Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS).

Application for Review of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for Cancellation of an authorisation for the use or Conduct of a Covert Human Intelligence Source.

APPENDIX 3

C FORMS

ACQUISITION OF COMMUNICATIONS DATA

All forms can be obtained from the Home Office: RIPA Codes of Conduct website:

<https://www.gov.uk/government/collections/ripa-forms--2>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Part I Chapter II request schedule for subscriber information

Specimen Part I Chapter II authorisation

Specimen Part I Chapter II Notice

Chapter II application for communications data

Guidance notes regarding chapter II application form

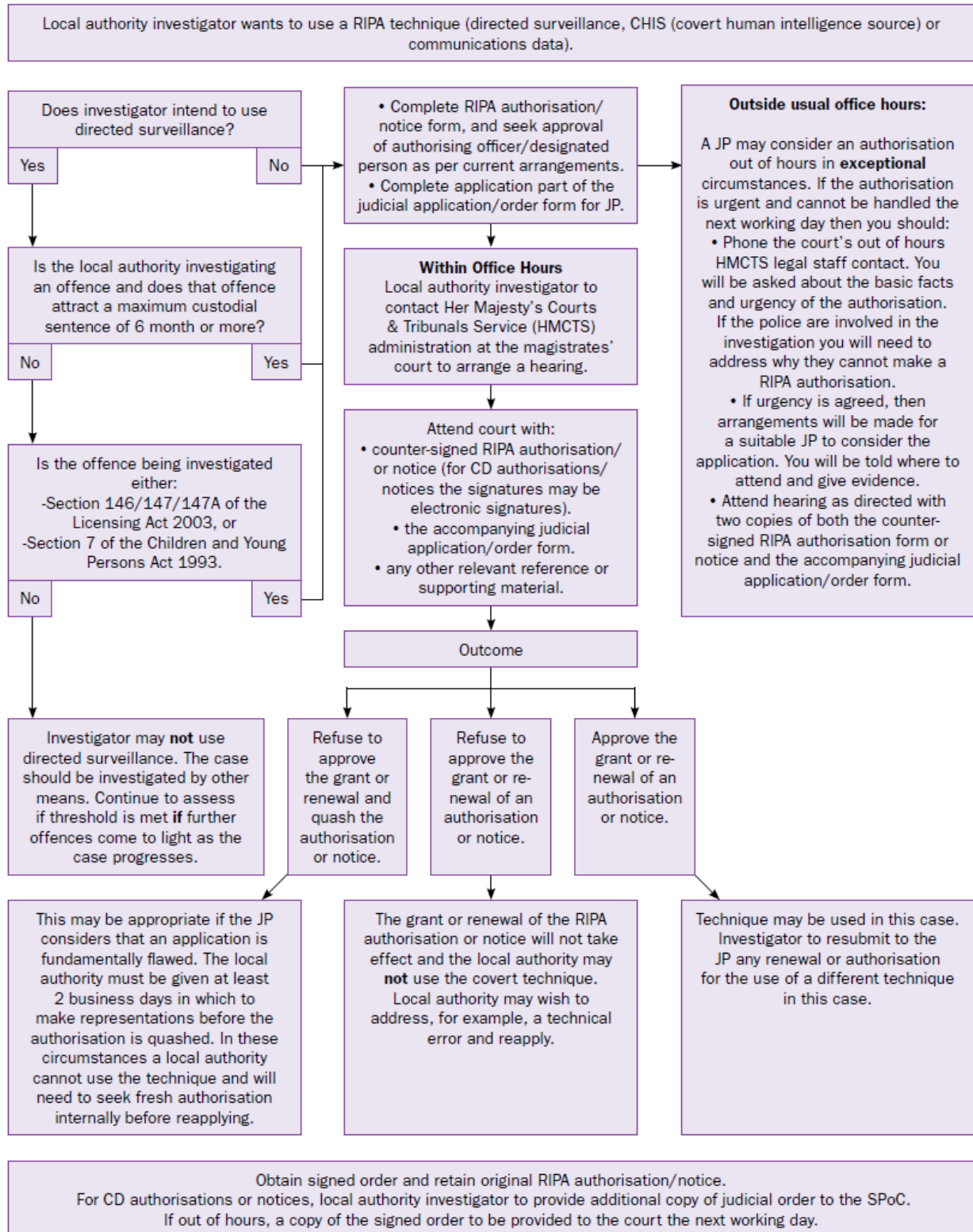
RIPA Section 22 notice to obtain communications data from communications service providers

Reporting an error by a CSP to the IOCCO

Reporting an error by a public authority to the IOCCO

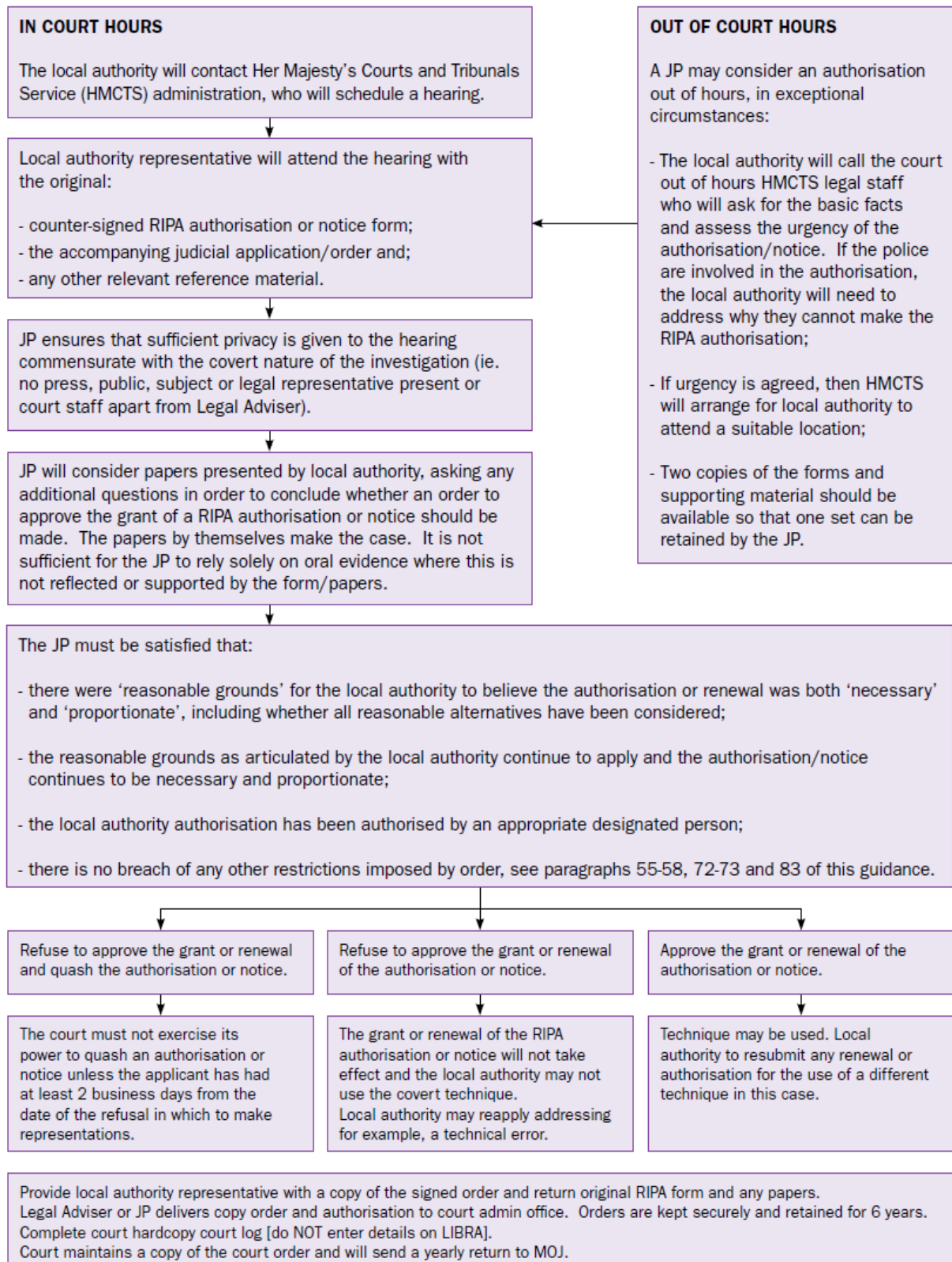
Annex A Local Authority Procedure

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Annex B JP Procedure

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....
.....
.....

Covert technique requested: (tick one and specify details)

- Communications Data**
- Covert Human Intelligence Source**
- Directed Surveillance**

Summary of details
.....
.....
.....
.....
.....
.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....
.....

Contact telephone number:.....

Contact email address
(optional):.....

Local authority
reference:.....

Number of
pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: