BABERGH DISTRICT COUNCIL and MID SUFFOLK DISTRICT COUNCIL

From:	**Interim Head of Law and Governance and Monitoring Officer**	**Report Number:**	**R54**
To:	**Executive Committee Strategy Committee**	**Date of meeting:**	**5 October 2015 8 October 2015**

REGULATION OF INVESTIGATORY POWERS ACT 2000 ("RIPA") JOINT CORPORATE POLICY AND PROCEDURES AND RIPA USE UPDATE

1. Purpose of Report

1.1 To seek Members' approval for a revised RIPA Joint Corporate Policy and Procedure attached as an appendix to this report.

1.2 To advise Members as to the general use of surveillance within the Babergh and Mid Suffolk Districts of Suffolk from July 2013 to date and to inform Members as to the results of an inspection last year by the Office of Surveillance Commissioners (OSC).

2. Recommendations

2.1 That the RIPA Joint Corporate Policy and Procedure within the appendix (a) to this report be adopted with immediate effect

2.2 That the Interim Head of Law and Governance and Monitoring Officer be authorised to make minor amendments to the RIPA Joint Corporate Policy and Procedure above as may be necessary from time to time.

2.3 That the information relating to the Councils' use of RIPA for the period July 2013 to date and the outcome of the Office of the Surveillance Commissioner's (OSC's) inspection in 2014 is noted.

The Committee is able to resolve this matter.

3. Financial Implications

3.1 None directly.

4. Legal Implications

4.1 RIPA provides a legal framework for the Councils to use covert methods of surveillance and information gathering to assist in the detection and prevention of crime in relation to the Councils' core functions. The legislation ensures that any investigatory activity conducted by the Councils is legal, proportionate and necessary. The legislative changes introduced by the Protection of Freedoms Act 2012 provide further protection to individuals by ensuring that the Councils can only exercise the powers available to it if they are both judicially approved and are required to detect or prevent serious crime.

4.2 The proposed revised Policy helps safeguard the Councils in their use of RIPA and when followed will ensure the Councils continue to comply with the law.

5. Risk Management

5.1 This report is not linked with any of the Council's Corporate / Significant Business Risks. Key risks are set out below:

Risk Description	Likelihood	Impact	Mitigation Measures
Failure to comply with the legal requirements set out in RIPA. This may result in a challenge under the Human Rights Act 1998.	Unlikely (if RIPA Policy is adhered to).	If successfully challenged, the impact would be serious both financially and reputationally.	Follow the revised RIPA Policy.

6. Consultations

6.1 Consultation has been carried out with the Council Officers who may operate surveillance activities covered by RIPA and those Authorising Officers who are able to authorise Council Officers to carry out such surveillance activities.

7. Equality Analysis

7.1 An Equality Impact Assessment (EqIA) has not been completed at this stage. However, if the Councils do need to consider any future applications under RIPA, a full EqIA assessment will be carried out as part of the individual circumstances of an individual who may be the subject of an application under RIPA.

8. Shared Service / Partnership Implications

8.1 The RIPA Policy is a joint corporate policy of both Councils.

9. Links to Joint Strategic Plan

9.1 The RIPA Policy is a Legal requirement.

10. Key Information

10.1 The Regulation of Investigatory Powers Act 2000 ('RIPA') puts a regulatory framework around a range of investigatory powers used by Local Authorities. This is done to ensure the powers are used lawfully and in a way that is compatible with the European Convention on Human Rights. It also requires, in particular, those authorising the use of covert surveillance techniques to give proper consideration to whether their use is necessary and proportionate.

10.2 RIPA legislates for the use by Local Authorities of covert methods of surveillance and information gathering to assist in the detection and prevention of crime in relation to an authority's core functions. There are three separate investigatory powers available to the Councils under RIPA:

Obtaining communications data – the 'who, when and where' of communications, such as telephone billing or subscriber details. However it does not include the 'what' (i.e. the content of what was said or written).

Covert Directed surveillance – which includes covert surveillance in public areas (not including residential premises or private vehicles which is never permissible) and CCTV which is likely to result in the obtaining of private information.

Use of covert human intelligence sources ('CHIS') – this includes undercover officers, public informants and people making test purchases (most relevant in trading standards cases, for example).

10.3 On 26 January 2011 the Home Office Review into counter-terrorism and security was published. Before the 2010 General Election both partners in the coalition which was formed thereafter had promised to overhaul RIPA on the basis that it was thought that surveillance carried out under it was often used to investigate minor offences and in a disproportionate manner.

10.4 The Protection of Freedoms Act 2012 was passed on 1 May 2012. From 1 November 2012 Local Authorities have been required to obtain judicial approval prior to using covert techniques or obtaining communications data. Local Authority authorisations and notices under RIPA are only given effect once an order has been granted by a Justice of the Peace (also called a Magistrate).

10.5 Additionally from that date Local Authority use of the three investigatory powers available to them under RIPA has been limited to the investigation of crimes which attract a six month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco.

10.6 The Council' RIPA Policy covering the obtaining of communications data, covert directed surveillance and the use of covert human intelligence sources has been revised in light of the above changes.

10.7 In accordance with the revised RIPA Codes of Practice; which require Local Authorities to involve Members in strategic oversight of RIPA including setting the relevant Policy and considering reports on its use by the Council; the approval of this Committee is sought to the revised RIPA Policy which is attached as an appendix to this report.

10.8 The Councils' use of RIPA is subject to regular inspection by the Office of the Surveillance Commissioner (OSC) in respect of covert surveillance authorisations under RIPA. During these inspections the Councils' authorisations and procedures are closely scrutinised and relevant Council officers are interviewed by the Inspector. Both Councils were inspected in September 2014 by Sir David Clarke, Assistant Surveillance Commissioner with the OSC.

10.9 The Inspection went very well and Sir David Clarke made only a few fairly minor recommendations which will have all been implemented when the revisions to the current RIPA Policy are implemented.

10.10 Members are advised that from July 2013 to date each Council has used covert directed surveillance on one occasion only. Both investigations related to Housing Benefit Fraud enquiries in relation to “living together” cases.

10.11 Members are further advised that during the same period no requests have been made by either Council to obtain communications data. In the future, if any such requests are made, these will have to be processed by the National Anti-Fraud Network (NAFN) on the Councils’ behalf. Your Officers are currently investigating the cost effectiveness of paying the annual subscription to NAFN (approximately £1,500 per Council) in order to access this service and whether there are any other cheaper payment options.

10.12 On 22 April 2015, 21 Council Officers including all the current Authorising Officers under RIPA and many of the Council Officers who may operate surveillance activities covered by RIPA received one day’s RIPA training from one of the leading Trainers in this field. Your Officers will continue to organise RIPA training for all those Officers involved or likely to be involved in matters in which RIPA may be relevant. In the future following the transfer of Housing Benefit Fraud cases to the DWP it may well be that RIPA awareness training will become more important than the RIPA investigations themselves.

11. Appendices

Title	Location
(a) The RIPA Joint Corporate Policy and Procedure	Attached

12. Background Documents

12.1 Councils’ joint RIPA Policy of April 2013

12.2 OSC Report following visit in September 2014

Authorship:

Jonathan Reed
Senior Solicitor & Deputy Monitoring Officer

01449 724677
Jonathan.Reed@baberghmidsuffolk.gov.uk

k:\docs\committee\reports\strategy\2015\081015-ripa report.docx

Appendix A

BABERGH DISTRICT COUNCIL

AND

MID SUFFOLK DISTRICT COUNCIL

RIPA JOINT CORPORATE POLICY AND PROCEDURES

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA')

Babergh & Mid Suffolk District Councils
September 2015

Document Control	
Title	RIPA Joint Corporate Policy and Procedures
Document Type	Policy and Guidance
Author	Jonathan Reed– Senior Solicitor and Deputy Monitoring Officer
Owner	Suki Binjal – Monitoring Officer and Interim Head of Law and Governance
Subject	Investigatory Powers
Protective marking	UNCLASSIFIED
Created	3 September 2015
Approved	
Review period	Every two years
Revision History	
Version Date	**Brief Description of Change(s)**

Contents

1.1 Introduction

The Regulation of Investigatory Powers Act 2000 is better known by its acronym "RIPA". The legislation, Codes of Practice and procedures provide a lawful framework for interference with Article 8, The Right to Privacy by law enforcement and other public authorities as they undertake 'core ' duties and responsibilities.

Failure to obtain an authorisation in accordance with RIPA would not mean the activity was unlawful. However, if a person subject of surveillance were to challenge the activity, either in a case brought by the enforcing agency, or were to make a stand-alone challenge to the way the surveillance was carried out, it would not be in accordance with the legislation provided, (RIPA), and all of the issues relating to the interference of Article 8 The Right to Privacy might not have been properly addressed. Therefore the interference might be deemed to be unnecessary and/or disproportionate, and not be lawful.

Failure to follow the procedures contained within RIPA and its Codes may render any evidence gathered inadmissible and/or may result in a breach of an individual's human rights, leading to legal challenge.

Under Article 8 of The Human Rights Act 1998, public authorities must respect an individual's "right to respect for his private and family life, his home and his correspondence". This right is not absolute, and is qualified thus: -

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

Any such interference with the right under Article 8 must be:

- lawful
- necessary and
- proportionate.

RIPA provides a statutory mechanism for the authorisation of:

- covert 'directed' surveillance
- covert use of a 'human intelligence source'.

This policy document gives an overview of the parts of the Act relevant to Mid Suffolk and Babergh District Councils ("the Councils") and explains the procedures to be followed. Appropriate training will be organised at regular

intervals and is compulsory both for those officers identified by their Heads of Service as being involved in enforcement work and for Authorising Officers. A register of attendees will be kept by the Councils' Legal Team. Various departments may need to carry out surveillance in order to prevent or detect crime. These include the following service areas: -

Audit & Fraud Investigation (including Housing Fraud)
Food Safety
Planning Enforcement
Environmental Services
Waste Management
Licensing
Housing & Community Development

1.2 Review and Scrutiny of this Policy & the Council's activities under RIPA

This policy will be regularly reviewed, by the Senior Responsible Officers, by the RIPA Working Group and by the Strategy Committee for Babergh District Council and the Executive Committee for Mid Suffolk District Council in relation both to legal developments and for the purpose of monitoring practice and procedure.

The Councillors should review the authority's use of RIPA at least once a year. They should also consider internal reports on any RIPA authorisations to ensure that the powers are being used consistently with the Council's policy and that the policy remains fit for purpose.

The Senior Responsible Officers ("SROs") are responsible for the integrity of process for the management of Directed Surveillance and Covert Human Intelligence Sources, for compliance with Part 2 of the Act and its Codes; for oversight of the reporting of errors to the Commissioner; for engagement with Inspectors from the Office of the Surveillance Commissioner (OSC); and for the implementation of post-inspection action plans approved by a Commissioner. For Babergh District Council and for Mid Suffolk District Council the SRO will be the Senior Solicitor and Deputy Monitoring Officer.

2. Amendments applicable specifically to local authorities

The use of RIPA by local authorities has come to the attention of the public, with adverse publicity because some local authorities have used RIPA authorisations to investigate matters relating to school catchment areas, dog fouling and people putting their bins out too early. Such authorisations were regarded by press and public as an inappropriate use of RIPA powers, and it was mooted that such powers were appropriate only for anti-terrorism activities or serious crime. As a result the government carried out an extensive consultation, which led to the introduction of revised Codes of Practice and Consolidating Orders, which came into force on 6 April 2010. The publication "Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice, A Public Consultation Paper" had made it clear that it was the government's intention to curb the RIPA powers previously held by local authorities.

The revised Codes of Practice:

1) added further levels of scrutiny into the process, with Councillors taking responsibility for reviewing policy and practice;
2) created the role of "Senior Responsible Officer" which has overall responsibility for the integrity of the process and for ensuring compliance; and
3) are intended to provide greater clarity on:
    i) when the use of RIPA techniques is likely to be proportionate;
    ii) when public authorities do/do not need to use RIPA authorisations; and
    iii) collateral intrusion.

The intended objective is that with increased and intensified monitoring activity, the balance between supporting law enforcement and respecting privacy will be more effectively achieved.

These changes were followed in 2012 by further amendments to RIPA contained in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and the Protection of Freedoms Act 2012. The former contains provisions which limit the use of RIPA powers to the investigation of offences which carry a 6 month custodial sentence and to offences connected with the sale of tobacco or alcohol to children, while the latter contains a requirement for judicial approval of RIPA authorisations for Directed Surveillance and use of a Covert Human Intelligence Source.

3.1 General Policy Statement - Steps Taken to Achieve Compliance

A forum comprising legal advisers, authorising officers and operational staff known as the Enforcement Officers' Working Group (EOWG) meets regularly to monitor procedure and performance and note any developments in the law.

The Councils have agreed for the present to implement Directed Surveillance ("DS") only and not to use Covert Human Intelligence Sources ("CHIS") which carries greater risk and is more complex. This policy is to be kept under review based on the need for CHIS within the Councils. There has not previously been a significant demand for use of CHIS. The EOWG, the SROs and the Councils' Committees will regularly review the need for CHIS, which requires specialist training for a relevant officer.

The Councils will only use DS as a last resort. Wherever practicable, the Councils will use overt surveillance techniques, thereby keeping the need for authorisation under RIPA to a minimum. Any surveillance is only to be carried out where it is both necessary and proportionate, having properly considered the human rights of the subject **and others**.

The Councils have produced guidance on DS for officers which forms part of this document. The guidance on CHIS is limited to enable officers and members to identify what constitutes CHIS and very broadly, what authorisation would involve.

Central Registers of RIPA authorisations for both Councils are held by Legal Services together with copies of authorisations given.

The Committees of both Councils will regularly monitor policy, practice and procedure.

The Councils will ensure that records pertaining to DS are retained for a minimum of 7 years.

3.2 Policy Statement on Surveillance – RIPA Part II

The Councils will ensure that all surveillance undertaken by officers will be conducted in accordance with the Codes of Practice issued by the Home Office and practical advice from the Office of Surveillance Commissioners (OSC). By adopting this approach the Councils are endeavouring to ensure that there are no breaches of the Human Rights Act 1998 or of the Regulation of Investigatory Powers Act 2000 itself. The implications of not observing the legislation, failing to put in place adequate procedural safeguards or to provide clear guidance for officers are:

Damage to the public's perception of the way the Councils conduct themselves in investigatory activities (e.g. possible abuse of statutory powers) leading to loss of public confidence

- Possibility of increased complaints and compensation claims to the Councils
- Loss of, or challenge to evidence in a prosecution
- Adverse commentary from the OSC and potential withdrawal of powers)
- Possibility of complaints to the Investigatory Powers Tribunal and consequent judgements and penalties
- Actions against the Councils under the Human Rights Act.

This policy document has been designed to protect both residents of the Babergh and Mid Suffolk Districts and officers that are likely to be involved in statutory duties which involve investigation and/or enforcement.

4. Guidance and Procedure for Officers

4.1 RIPA Part II - Surveillance

Overt Surveillance does not require authorisation under RIPA

Overt surveillance is, as its name would suggest, surveillance which is open. In other words, there is nothing secretive or hidden about it, and the public are likely to be aware that it is taking place. Officers may carry out overt surveillance in the course of a normal day's work, and this does not require any prior authorisation.

Similarly, surveillance will be overt if the subject has been told it will happen, e.g. where a noisemaker has received advance written warning (within three months of the surveillance) that noise will be recorded if it continues, or where a Premises Licence authorising entertainment is issued subject to conditions, and the licensee is told that officers may visit without notice and/or without identifying themselves to the owner/proprietor to check that the conditions are being met.

Part II of the Act identifies three categories of covert (i.e. secret or hidden) activity which may be authorised if the correct procedure is followed and the established criteria are met. These are:

i) Intrusive Surveillance (this category may not be authorised by a local authority)
ii) Directed Surveillance
iii) Covert Human Intelligence Sources

Intrusive Surveillance ("IS")

A local authority may not authorise Intrusive Surveillance and the Councils therefore **may not** carry out intrusive surveillance under any circumstances. This is covert surveillance carried out on any residential premises or in any private vehicle. It involves a person actually on the premises or in the vehicle or is carried out by a surveillance device on the premises or in the vehicle. It can also include recordings made by a device not actually on the premises or in the vehicle but which give recordings of a quality equal to that which might be obtained from a device on the premises or in the vehicle. Authorisation may only be given by a Senior Authorising Officer or by the Secretary of State. Examples of Senior Authorising Officers are: within the police force - certain Chief Constables or Commissioners, within the National Criminal Intelligence Service and National Crime Squad - a Director-General and specially designated officers within HM Customs & Excise. In all but the most urgent cases approval from a Commissioner (at the Office of the Surveillance Commissioner – the body which oversees compliance with the Act) is required to be notified to the Senior Authorising Officer before an IS authorisation can take effect. As a local authority may not authorise IS, no further reference will be made to it in this Guidance.

4.2 Directed Surveillance ("DS")

This is **covert** but not intrusive (see below) surveillance, which is:

- undertaken for a **specific** investigation or operation (not as an immediate response to events or as part of a routine patrol) and
- in a way likely to obtain **private information** about a person.

Covert surveillance, according to RIPA s.26(9)(a), occurs if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place." If an officer's activities are not hidden from the subjects of the **surveillance**, then those activities are not within the RIPA framework, e.g. spot checks on dustbins in a recycling scheme. An example of covert surveillance would be the monitoring of the movements of a benefit fraud suspect, to determine whether the suspect had undeclared work, or an undeclared person sharing his or her property.

Private information in relation to a person includes any information relating to his private or family life. The glossary to the Covert Surveillance Code of Practice defines private information as:
"Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of the investigation" and also (at paragraph 2.4) says it should be taken to include

"…any aspect of a person's private or personal relationship with others, including family and professional or business relationships." It goes on to say that this can include personal data such as names, telephone numbers and addresses and that "family should be treated as extending beyond the formal relationships created by marriage or civil partnerships. E.g. a person observed running a commercial baking business from her home became subject to investigation. Such an investigation should be subject to the RIPA consideration/authorisation process as any surveillance could result in obtaining private information about her. Case law demonstrates that breaches of Article 8 can occur even in a public place (see the case of Peck -v- UK) and also that private life is widely interpreted by the courts, covering activities which take place at business premises. In the case of Ammam –v- Switzerland the court said "Respect for private life comprises the right to establish and develop relations with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature."

Limitation on the Use of Directed Surveillance

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI2012/1500) came into force on 1st November 2012. It restricts Authorising Officers in a local authority in England or Wales from authorising directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND the offence meets the following conditions:

1) that the criminal offence to be prevented or detected is punishable by a minimum term of six months' imprisonment; or
2) constitutes an offence under sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old) regardless of the length of prison term.

It is therefore essential that Investigating Officers consider the penalty attached to the criminal offence which they are investigating BEFORE considering whether it may be possible to obtain an authorisation for directed surveillance. They may wish to take advice from Legal Services in that regard.

How may Directed Surveillance be authorised?

The Act says that DS must first be authorised by an "authorised person". A list of authorised persons at the Councils can be found below in the section 5.5 entitled 'Authorising Officers'.

Following the amendments made to RIPA by the Protection of Freedoms Act 2012, the Council will subsequently be required to make an application to the Magistrates' Court for judicial approval before the authorised activity can be commenced.

Authorisations for DS do not have to be notified to the Office of the Surveillance Commissioner but must be available for review when Commissioners, Assistant Commissioners and Inspectors visit the authority.

Obtaining Judicial Approval of Authorisations

Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. Section 38 of the Protection of Freedoms Act 2012 amends RIPA to require that where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, judicial approval will be required. The relevant Council will have to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of grant of the authorisation or renewal of an existing authorisation if and only if, they are satisfied that:

(a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a CHIS was reasonable and proportionate and these grounds still remain;
(b) the "relevant conditions" were satisfied in relation to the authorisation. "Relevant conditions" include that:
    (i) the relevant person was designated as Authorising Officer.
    (ii) it was reasonable and proportionate to believe that using covert surveillance or a CHIS was necessary and the relevant conditions have been complied with.
    (iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA.
    (iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

No activity permitted by the authorisation granted internally by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained.

To ensure compliance with this requirement, any Authorising Officer who proposes to authorise an application for the use of directed surveillance or for the use of a CHIS must immediately inform Legal Services by telephone or email of the details of the authorisation, and provide a copy of the authorisation form. Legal Services will then make the necessary arrangements for an application for an order to approve the authorisation to be made to the Magistrates' Court. The Authorising Officer and the Investigating Officer may be required to attend the Magistrates' Court to support the application.

When do council officers need to get authorisation?

Anti-social behaviour activities, noise, violence, race etc.

(a) Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be considered a "CHIS", as they are not required to establish or maintain a relationship for a covert purpose. **However, regular review of the maintenance of the diary should be undertaken to ensure the diary is kept as the individual conducts everyday activities, rather than specifically observing, listening or monitoring, which might be construed as 'directed surveillance'**

(b) Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does **not** require authorisation.

(c) Recording sound (onto tape, CD, a hard drive etc.) on private premises could constitute intrusive surveillance, unless it is done overtly by for example writing to the alleged noisemaker to warn that this will occur if the level of noise continues. Therefore, (i) the occupant of the monitored premises must receive notice in writing that sound recording equipment may be installed on a neighbouring property (thus rendering the surveillance overt), and (ii) the surveillance must be carried out within a period of three calendar months from the date of the notice. At the end of the three month period, the surveillance must cease or, if surveillance is to continue, either a further notice must be served on the occupant of the monitored premises or an authorisation to conduct (covert) directed surveillance will be required.

(d) Any use of still camera or video recording equipment not notified to the subject 'on the day' should be DS authorised. Use of any 'hidden devices' should be considered carefully to ensure this does not constitute 'intrusive' surveillance. In case of doubt, seek specific guidance from Legal Services.

Use of Technical Equipment

Covert surveillance equipment should only be used by RIPA trained officers.

Covert surveillance equipment will only be installed with the authorisation of the Council's authorising officers. This will only be used in residential premises if a member of the public has made a complaint or requested help and the matter can only be investigated with the use of covert surveillance techniques. If a resident is requested to keep a video diary as part of an evidence gathering exercise, this will be regarded as directed surveillance on behalf of the Council, and as such would require authorisation.

4.3 Covert Human Intelligence Sources (CHIS)

The Councils will not authorise CHIS at present, but the need for CHIS will be kept under review. The guidance in this section should enable officers and councillors to identify what would constitute 'CHIS'.

This type of surveillance involves the use or conduct of someone who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information i.e. any informant, undercover agent or officer. CHIS activity involves covertly using such a relationship to obtain information or provide access to information or covertly disclosing information obtained by the use of such a relationship. A full explanation of what constitutes CHIS is covered by RIPA Section 26 (7)(8) and (9). As indicated above, the Councils no longer authorise CHIS. However, in order that Council officers do not inadvertently create or use a CHIS, the following guidelines are suggested to enable officers to identify and thereby avoid a CHIS:

- 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 calculated to ensure that one of the parties to the relationship is unaware of that purpose; and
- A relationship is used covertly, and information obtained 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.
- This clearly covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.
- Inducing anyone to act in a covert way (see also section 48 RIPA) that is covered by the above definitions would also count as use of a CHIS.
- It should be noted that a person overtly providing information to the Councils may in reality be a CHIS if he/ she has obtained that information in the course of, **or as a result of the existence of**, a personal or other relationship. A duty

of care would be owed to such a person, and great care should be taken before acting upon the information he/ she has provided.
- If in any doubt seek advice from Legal Services.

Authorisation of CHIS

Two elements need to be authorised with a CHIS: -

- Conduct – establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- Use – actions inducing, asking or assisting a person to act as a CHIS and the initial decision to use a CHIS

Special rules apply to juveniles and vulnerable people.

CHIS requires judicial approval in the same way as DS (see paragraph 4.2 above under the heading 'Obtaining Judicial Approval of Authorisations').

Properly managed use of a CHIS requires
- the maintenance of confidential source records
- Use of handlers and a controller
- A process for introducing intelligence to an investigation without revealing the source
- Regular review of conduct and use
- Risk assessment in relation to the safety of the CHIS, including undercover officers

4.4 RIPA PART I CHAPTER II (Communications Data)

Categories of Communications Data

There are three broad areas of communications data, only two of which can be accessed by the Councils. They are as follows:

1. Section 21(4)(c) Information about Communications Service users, such as:

    - Name of account holder/subscriber
    - Installation and billing addresses
    - Method of payment/ billing arrangements
    - Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to)

- Other customer information e.g. account notes, demographic information or sign up data (not passwords or personalised access information)

2. Section 21(4)(b) Information about the use of communications services

- Outgoing calls on a landline telephone or contract or prepay mobile phone
- Timing and duration of service usage
- Itemized connection records
- Internet logon history
- E-mails (sent)
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring
- Information about the provision and use of forwarding/redirection services (postal and telecom)
- Records of postal items e.g. records of registered/recorded/special delivery postal item, records of parcel consignment/delivery/collection

Organisations from which the Councils may access Communications Data

All Communications Data is accessed from Communication Service Providers (CSPs). These may be:

- **Telecom providers**,
  mobile phone service providers, landline phone service providers or International Simple Voice Resellers

- **Internet Providers**
  ISPs, Virtual ISPs and Portals

- **Postal Providers**
  Postal services

Applying for an Authorisation to Obtain Communications Data

Application must be made using the appropriate form. It must include the following information:

- Name or designation of the officer requesting the communications data
- The operation and person (if known) to which the requested data relates
- A description of the data requested

- Identification of which section of the Act the communications data is covered by
- Reasons why obtaining the data is considered to be necessary under Section 22(2) of the Act. **N.B. there is only one reason - for the prevention or detection of crime or preventing disorder.**
- An explanation as to why obtaining the data is proportionate to what it seeks to achieve
- An indication (where appropriate) that the matter of collateral intrusion has been considered.

Application forms are subject to inspection by the Interception of Communications Commissioner. Both the applicant and the Designated Person may be required to justify any decisions they have made.

All notices and Authorisations for Communications Data must be channelled through a "Single Point of Contact" (SPoC) at the National Anti-Fraud Network ("NAFN").

Section 37 of the Protection of Freedoms Act 2012 has amended section 23 of RIPA so that judicial approval must be obtained for the obtaining or disclosing of communications data. Judicial approval must be requested once **all** the Councils' internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. The authorisation must be provided by a Magistrate.

The Home Office Acquisition and Disclosure of Communications Data Code of Practice can be found on the Home Office website.

Ways of obtaining Communications Data

Under RIPA, there are two permissible ways of accessing Communications Data.

1. Notice under Section 22(4)
   A Notice is where a CSP collects data on behalf of the Council. The form of Notice must include the following information:

   - A description of the data required (and whether it is Communications Data under Section 21(4)(b) or Section 21(4)(c) of the Act.
   - The purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**
   - The name (or designation) and office, rank or position of the Designated Person
   - The manner in which the data should be disclosed
   - A unique reference number
   - If relevant, any indication of urgency

- A statement setting out that data is sought under the provisions of Part I, Chapter II of the Act
- Contact details

2. Authorisation under Section 22(3)

A section 22(3) authorisation is used by the Council collecting or retrieving the Communications Data itself. It may only be given in these circumstances:

- When the Postal or Telecommunications operator is not capable of obtaining or retrieving the communications data
- When it is believed that the investigation may be prejudiced if the Postal or Telecommunications Operator is asked to collect the data itself
- When there is a prior agreement in place between the Council and the Postal or Telecommunications Operator as to the appropriate mechanisms for the disclosure of Communications Data

Each Authorisation must include the following information:

- A description of the conduct that is authorised
- A description of the Communications Data required (identify whether it is Communications Data under Section 21(4)(b) or 21(4)(c) of the Act)
- Identify the purpose for which the data is required. **In relation to the Councils' cases this will always be for the prevention or detection of crime where the offence carries a minimum custodial sentence of 6 months or is one of the designated offences under the Licensing Act 2003 (see paragraph 4.2) .**
- The name (or designation) and office, rank or position of the Designated Person
- A unique reference number

Authorisations and notices are valid for one month, but can be renewed using the appropriate form. They must be cancelled as soon as they are no longer considered to be either necessary or proportionate.

It is the duty of a Designated Person to cancel Authorisations and Notices.

Designated Persons (Authorising Officers) and their Responsibilities

An Authorising Officer for Communications Data must be a Head of Service or above.

Authorising Officers must ensure that requests for Communications Data are both necessary and proportionate prior to granting an Authorisation or issuing a Notice.

They have a duty to consider various points, as follows:

- Whether the case justifies the accessing of Communications Data under Section 22(2)(b) i.e. that it is for the prevention or detection of crime or preventing disorder.
- Whether obtaining access to the data by the conduct authorised by the authorisation, or required of the CSP in the case of a Notice, is proportionate to what is sought to be achieved
- Whether the circumstances of the case still justify such access in cases where there is likely to be collateral intrusion
- Whether any urgent time scale is justified.

N.B. Communications data cannot be used in evidence without it being produced in a statement by the CSP involved.

4.5 Internal authorisation procedure and Authorising Officers

a) Authorisation procedures

Prior authorisation for directed surveillance or for use of a covert human intelligence source needs to be obtained from an Authorising Officer. All authorisations, reviews, cancellations and rejections will be filed in a central register kept in the Legal Services section of both Councils. All must be completed using the correct, current version of the RIPA forms.

How is an application for authorisation made?

An application for authorisation for Directed Surveillance must be made in writing. It should specify:

- The action to be authorised
- The identities, where known, of those to be the subject of Directed Surveillance
- An account of the investigation or operation
- The reasons why the authorisation is sought (i.e. the prevention or detection of crime or the prevention of disorder)
- Why the surveillance is considered to be proportionate to what it seeks to achieve
- An explanation of the information which it is desired to obtain as a result of the authorisation
- The potential for collateral intrusion, i.e. interference with the privacy of persons other than the subjects of the surveillance, and an assessment of the risk of such intrusion or interference
- The likelihood of acquiring any confidential material
- Where authorisation is sought urgently, reasons why the case is considered to be urgent

The Authorising Officer (see e) below) must give authorisations in writing,

b) Duration of Authorisations

A written authorisation will cease to have effect (unless renewed) at the end of a period of 3 months beginning with the date on which it took effect. However, authorisations must not be allowed to expire, but must be cancelled as soon as the activity is no longer necessary or proportionate. For example, the information has been obtained, the investigation has been completed, or the activity is no longer going to be undertaken.

c) Renewal of Authorisation

If at any time before an authorisation ceased to have effect the Authorising Officer considers it necessary for the authorisation to continue for the same purpose for which it was given, then he/she may renew it in writing for a further period beginning with the day when the authorisation would have expired but for the renewal. The renewal will normally be for three months in the case of DS. The request for a renewal of authorisation should record:

- whether this is the first renewal or on how many occasions it has been renewed
- the same information as outlined for an original application
- details of any significant difference in the information given in the previous authorisation
- the reasons why it is necessary to continue with the surveillance
- the content and value to the investigation or operation of the information so far obtained by the surveillance
- an estimate of the length of time the surveillance will continue to be necessary
- the results of any reviews

d) Reviews and Cancellations

The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the surveillance no longer meets the criteria for authorisation. A record should be made of the cancellation and the appropriate form completed.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded. Reviews should be more frequent where there may be collateral surveillance on persons other than those who are the subject of surveillance. 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.

As soon as a decision is taken to cease surveillance, an instruction must be given to those involved in the operation to stop listening, watching or recording

the activities of the subject. The date on which that instruction is given should also be recorded.

e) Authorising Officers

Since amendments were made under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 the seniority of Authorising Officers must be at Director/Heads of Service level, or above

The following are **Authorising Officers** for the purposes of Part II of RIPA: -

Head of Paid Service or, in his/her absence, the acting Head of Paid Service – But only for the authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer.

Head of Environment

Head of Law and Governance

Corporate Manager – Internal Audit

Authorisations may only be given to an **authority** by its own Authorising Officers. Authorising Officers should not give authorisations relating to their own service, e.g. the Head of Environment whose area includes the investigation of fly tipping cases should **not** authorise surveillance for a fly tipping matter.

4.6 Guidance for Authorising Officers

The role of an Authorising Officer is akin to that of a Magistrate or Judge considering an application to the court for a Warrant or similar. The Authorising Officer must have all the information she or he feels is necessary to make an independent assessment of the application. The Authorising Officer should assess, for example: the force of the complaint giving rise to the surveillance, the duration of the surveillance proposed, if recording devices are to be used, an indication of the expected quality should be given. Without examining such issues, an Authorising Officer will not be able to determine whether the surveillance is both 'necessary' and 'proportionate' and whether, therefore the authorisation should be given. An Authorising Officer should not hesitate to refuse an application on the grounds of insufficient information. If further details are required, comments may be made on the returned application as to the further information sought.

Application forms are subject to inspection by the Surveillance Commissioner. Both the applicant and the Authorising Officer may be required to justify any decisions they have made.

The primary consideration for an Authorising Officer is that authorisations for directed surveillance may only be granted if the Authorising Officer is certain that such authorisation is necessary **for the prevention or detection of criminal offence which carries a custodial sentence of a minimum of 6 months or is one of the specified offences under the Licensing Act 2003.**

Before signing an authorisation, an Authorising Officer needs to be satisfied that the authorisation is: -

- in accordance with the law
- necessary (consider - is there reasonably available another, overt, means of discovering the information desired?)
- proportionate (consider – is the proposed surveillance the **least intrusive** method available? Is it **excessive** in relation to the seriousness of what is being investigated? The Authorising Officer should be satisfied, prior to authorisation, that all other avenues for obtaining the necessary evidence have been explored.

The likelihood of "collateral intrusion" must also be considered. The Authorising Officer should ensure that intrusion to individuals who are not the intended subject of the investigation is avoided or at least minimised.

If the period of authorisation is not made clear on the authorisation form, then an authorisation will be effective for a period of three months, after which it ceases to have effect (unless renewed in the meantime). Reviews should be carried out periodically, to ensure that the authorisation continues to meet the criteria. If it does not, it should be cancelled using the appropriate form (please see forms attached). Even those authorisations where the time period is specified need to be cancelled using a cancellation form.

<u>Further Guidance on Criteria to be given Consideration in an application</u>

<u>Collateral Intrusion</u>
An Authorising Officer must give particular consideration to the potential for "collateral intrusion". Essentially, this is interference with the privacy of persons other than the subject(s) of surveillance. An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the Authorising Officer when considering the proportionality of the surveillance. Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way.

In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required. The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his/her home, or where there are special sensitivities.

Proportionality

Proportionality is a very important concept, and it means that any interference with a person's rights must be proportionate to the intended objective. Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus where surveillance is proposed that action must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary; and the impact on the individual or group of people concerned must not be too severe. The Human Rights Act defines a measure or action as proportionate if it:

- impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties)
- is carefully designed to meet the objectives in question and is not arbitrary, unfair or based on irrational considerations.

5. Keeping of Records

The following records must be kept:

- A copy of the application for the authorisation;
- A copy of the authorisation together with any supplementary documentation and notification of approval given by the authorising officer;
- A record of the period over which the surveillance is taking or has taken place (including any significant suspensions of coverage)
- A record of the frequency and results of periodic reviews of the authorisation
- A copy of any renewal of authorisation, together with the supporting documentation when the renewal was requested
- A copy of the judicial approval order
- The date and time when any instruction was given by the authorising officer

IN ADDITION a central register of authorisations will be kept in Legal Services. The register will be used to keep track of all the Councils' authorisations and record their status. The register may be used for inspection purposes by officers of the OSC. The register must be updated whenever an authorisation is granted, renewed or cancelled. This record should be retained for a period of at least 5 years from the ending of the authorisation and should contain the following information:

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

- the unique reference number (URN) of the investigation or operation
- the date the authorisation was approved by the Magistrates' Court
- the title of the investigation or operation, including a brief description and names of subjects, if known
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer
- whether the investigation or operation is likely to result in obtaining confidential information as defined by the Code of Practice
- the date the authorisation was cancelled

Where the product of the surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the established disclosure requirements (e.g. under the Criminal Procedure and Investigations Act 1996) for a suitable further period or until further review.

Who keeps the records/a central register of authorisations?

Copies of individual authorisations should be kept by the department carrying out the investigation. The original authorisations and the court orders approving them will be kept by Legal Services together with the Central Register of Authorisations. The authorisations and Court Orders will be held by Legal Services for 7 years. Any copy authorisations held by individual departments should be destroyed according to the retention policy for that type of file.

6. Breaches of RIPA, its Codes of Practice and the Human Rights Act

The Effect of a RIPA Authorisation

Although it is neither an express statutory requirement nor a stipulation of the Codes of Practice that acts of surveillance carried out by local authorities must be authorised under RIPA, the effect of a RIPA authorisation (correctly completed) is to make the action which is authorised (and the evidence obtained through that action) "lawful for all purposes" (Section 27(1)). Without such an authorisation, evidence obtained from DS or CHIS may be deemed unlawful and thus be ineffective in any prosecution. In addition, the authority may be exposed to civil or criminal liability for its conduct.

The Effect of the Codes of Practice

Section 72 of RIPA says:

(1) A person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, have regard to the provisions (so far as they are applicable) of every code of

practice for the time being in force under that section.
(2) A failure on the part of any person to comply with any provision of a code of practice for the time being in force under section 71 shall not of itself render him liable to any criminal or civil proceedings.
(3) A code of practice in force at any time under section 71 shall be admissible in evidence in any criminal or civil proceedings.
(4) If any provision of a code of practice issued or revised under section 71 appears to-

(a) the court or tribunal conducting any civil or criminal proceedings,
(b) the Tribunal,
(c) a relevant Commissioner carrying out any of his functions under this Act,
(d) a Surveillance Commissioner carrying out his functions under this Act or the Police Act 1997, or
(e) any Assistant Surveillance Commissioner carrying out any functions of his under section 63 of this Act,

to be relevant to any question arising in the proceedings, or in connection with the exercise of that jurisdiction or the carrying out of those functions, in relation to a time when it was in force, that provision of the code shall be taken into account in determining that question.

Human Rights Act 1998

If covert surveillance or use of a covert human intelligence source is not authorised under RIPA, then the authority will be exposed to the possibility of legal action under the Human Rights Act. The subject of the surveillance may be able to have the evidence obtained in an unauthorised investigation excluded. The articles most likely to be put forward are:

- Article 6 – the right to a fair trial
- Article 8 – the right to respect for private and family life, home and correspondence

7. Appendices – Forms and further information

The web address for the Office of the Surveillance Commissioners is:
https://osc.independent.gov.uk/

A full copy of RIPA 2000 can be found at:
http://www.legislation.gov.uk/ukpga/2000/23/contents

Orders relating to RIPA can be found at
https://osc.independent.gov.uk/advice-and-guidance/acts-legal-documents/

The Codes of Practice (which include flowcharts illustrating the authorisation process) can be found at:
https://www.gov.uk/government/collections/ripa-codes

RIPA forms can be found at:
https://www.gov.uk/government/collections/ripa-forms--2

Judicial Approval Forms and Guidance can be found at
https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

A copy of the Human Rights Act 1998 can be found at:
http://www.legislation.gov.uk/ukpga/1998/42/contents

Guidance on Human Rights can be found at
http://webarchive.nationalarchives.gov.uk/+/http://www.dca.gov.uk/peoples-rights/human-rights/publications.htmhttp://www.yourrights.org.uk/