Regulation of Investigatory Powers Act 2000

Partnership Policy

March 2024 to February 2027

Contents

1 Introduction

There is a strategic partnership in place between the three sovereign councils of Boston Borough Council, East Lindsey District Council and South Holland District Council called the South and East Lincolnshire Councils Partnership. This is referred to throughout this Policy as 'The Councils'.

The Councils can make use of a limited range of investigatory powers: directed surveillance, covert human intelligence sources (CHIS) and the acquisition of communications data (CD).

The Councils powers is controlled by two key pieces of legislation:

i. Investigatory Powers Act 2016
ii. Regulation of Investigatory Powers Act 2000

This Policy sets out The Councils position in relation to the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000 (RIPA), which established a statutory framework for the regulation of covert surveillance by, amongst others, The Councils. The Act is designed as a mechanism to provide the correct balance between an individual's right to privacy and proper use of data and surveillance, having due regard to human rights as defined in the Human Rights Act 1998.

The procedures and guidance set out in this policy are based on the provisions of RIPA; Home Office Codes of Practice and guidance issued by the Investigatory Powers Commissioner's Office. Links to Guidance and documentation links can be found at the end of this Policy.

Officers of The Councils should be aware of the scope and extent of activities covered by RIPA.

As a company separate from the 'The Councils' (albeit one that is wholly owned by The Councils) employees or Agents of Public Sector Partnership Services Ltd (PSPS) cannot authorise covert surveillance but can seek such authorisation from The Councils in adherence to this Policy.

The Councils is a public body for the purposes of the European Convention on Human Rights and Human Rights Act 1998.

2 Policy Aim

The requirements of the:

- European Convention on Human Rights
- Human Rights Act 1998
- Investigatory Powers Act 2016 and
- Regulation of Investigatory Powers Act 2000,

impact on any officers of The Councils who undertake investigatory or enforcement

activities. This policy requires that all officers undertaking covert investigative activities only do so in accordance with the requirements set out in the Investigatory Powers legislation and its associated codes of practice.

2.1 The right of action for breach of convention rights is available in English law by the Human Rights Act 1998. However, there are times when public bodies can override this right and carry out covert investigative activities.

The Regulation of Investigatory Powers Act 2000 allows local authorities to carry out such Directed Surveillance (surveillance of an individual/s without their knowledge for a specific purpose), or use a Covert Human Intelligence Source (use of informants or undercover officers). The Investigatory Powers Act 2016 permits limited access to communications data (obtaining subscriber information of a telephone number or internet user, etc.) provided the investigatory activity is lawful, necessary, proportionate and non-discriminatory.

2.2 Everyone has a fundamental right to privacy. This means amongst other things, a right not to be watched, have your mail opened or have your personal space invaded. This right is contained in Article 8 of the European Convention on Human Rights:

"Everyone has the right to respect of his private and family life, his home and his correspondence."

The aim of this policy is to ensure that The Councils and their officers comply with the requirements of the European Convention on Human Rights, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000 when undertaking any covert investigative activities which may interfere with a person's right to respect for private and family life, home and correspondence.

3 Policy Statement

The Councils are committed to building a fair and safe community for all, by ensuring the effectiveness of laws designed to protect individuals, businesses, the environment and public resources.

The Councils recognise that the vast majority of individuals comply with the law. For those that choose not to, The Councils has a responsibility to ensure firm but fair enforcement action is taken which may include authorised covert surveillance in order to gather evidence of illegal activity.

Where any such surveillance is contemplated by officers it must be authorised under the Act to ensure it is lawful and does not infringe a person's human rights.

3.1 The Councils will not use covert surveillance unless it is absolutely **necessary** to achieve the desired aims and only so long as it is **proportionate** to do so and

that it is done with adequate regard to the rights and freedoms of those who are not the subject (s) of the covert surveillance.

When using covert surveillance, The Councils will give due regard to the following legislation:

Human Rights Act 1998,
Regulation of Investigatory Powers Act 2000
Investigatory Powers Act 2016
Protection of Freedoms Act 2012
Data Protection Act 2018
UK General Data Protection Regulation

3.2 The Councils **will**

- actively monitor its use
- have due regard to the Home Office Codes of Practice
- ensure authorisations are granted by the appropriately trained and designated officers
- ensure staff and (contractors) are appropriately trained to carry our surveillance activity
- properly investigate any complaints about its use
- assist, support and comply with the requirements of the Investigatory Powers Commissioner's Office (IPCO) who oversee the use of covert investigatory powers by public authorities.

3.3 The Councils will **not**:

- routinely use Covert Human Intelligences Sources (CHIS), any such proposal to deploy a CHIS must initially be authorised by the Authorising Officer
- carry out intrusive surveillance within the meaning of RIPA
- use covert surveillance (regulated by RIPA) unless judicial approval has been obtained.

4 Purpose

This Policy sets out the practice to be followed before any covert surveillance is undertaken when carrying out investigations.

4.1 The Policy will cover the procedural considerations The Councils must consider when undertaking either Covert or Overt directed surveillance and it will assist officers in understanding:

- when surveillance is regulated by RIPA
- when authorisation criteria are met
- RIPA procedures
- implications of the Codes of Practice
- non-RIPA surveillance
- how to complete forms.

This Policy will cover the procedures which must be followed when authorising, managing, recording the actions of, and ultimately using information obtained through a Covert Human Information Source.

4.2 **Roles**. The Councils Senior Responsible Officer (SRO) has overall responsibility for ensuring that the Council complies with RIPA.

The SRO will:

- inspect authorisations on a quarterly basis
- oversee training requirements for appropriate staff
- participate in IPCO inspections
- provide an annual report to the relevant Committee of each Council on the use of RIPA.

4.3 The SRO maintains the Central Records, carries out quality assurance checks on all authorisations submitted, arranges training, provides day-to-day advice on surveillance issues and produces information as required.

Central records - Records kept by the SRO will be used to:

- remind Authorising Officers of the expiry of authorisations
- check that surveillance does not continue beyond the authorised period
- remind Authorising Officers to regularly review current authorisations
- remind Authorising Officers and applicants to consider the destruction of the results of surveillance operations and associated paperwork in line with retention and destruction guidelines
- at the sixth anniversary of each authorisation, remind Authorising Officers that the forms of authorisation, renewal or cancellation held locally and in the Central Record are due to be destroyed unless there is a reason they should be retained for longer
- receive and investigate complaints by members of the public who reasonably believe that they have been adversely affected by surveillance activities carried out by The Councils
- commission and provide training in the law relating to surveillance for appropriate officers.

Authorising Officers (AO) – are trained, experienced managers who assess and authorise RIPA applications.

5 Definitions

Surveillance

5.1 Surveillance, for the purpose of the Regulation of Investigatory Powers Act 2000, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

5.2 Surveillance under RIPA may be classed as Directed or Intrusive.

- Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances) such that it is not reasonably practicable to seek authorisation under the 2000 Act. This may be authorised and undertaken by The Councils.

- Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises, or in the vehicle or is carried out by a means of a surveillance device).

The Councils does not have power to carry out intrusive surveillance, only the police, and other law enforcement agencies, can carry out intrusive surveillance.

5.3 Confidential information – includes confidential personal information such as medical records or spiritual counselling, confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

5.4 Private information - The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information can include any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

5.5 All Directed, covert surveillance shall be set out in accordance with the procedures in this Policy.

Directed Surveillance - Process

5.5.1 The following documents must be maintained:

- copies of applications and authorisations and any supporting documents and the approval of the Authorising Officer (AO)
- copy of any authorisation made by the judiciary

- a record of the period of surveillance
- the frequency of reviews by the AO and a record of that review
- a copy of any renewal of any authorisation (by AO or Judiciary)
- date, time and details of any instructions given by the AO.

5.5.2 Prior to the investigation:

- clear rules must be set up limiting the disclosure and access to any information obtained
- the number of people with knowledge of a covert monitoring exercise should be limited
- the surveillance must be strictly limited to obtaining evidence within a set time frame and it should not continue after the investigation is complete
- if using audio or video equipment, this should not normally be used in places such as toilets or private offices
- information obtained through covert monitoring should only be used for the prevention or detection of criminal activity or serious Gross Misconduct
- other information collected while monitoring should be disregarded and, where feasible, deleted - unless it reveals information that no employer could reasonably be expected to ignore.

6 Approved Forms

Once the need for surveillance has been established, the appropriate form should be completed and sent to the Authorising Officer for approval.

Forms can be downloaded here along with appropriate guidance for each application:

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

Helpful additional links are available at the end of this Policy.

7 Central Register

A central register must be kept by the SRO (RIPA Co-ordinator) detailing the following information.

1. Date and type of any authorisation.
2. Date any order made by a Justice of the Peace.
3. Name and grade of AO.
4. Unique ref number of the investigation. These are obtained from the Investigating Officer.
5. Brief description and names of subjects of investigation.
6. Whether any urgency provisions were used and why.
7. Exactly what is authorised.
8. Details of any renewal.
9. Whether confidential information is likely to be obtained.
10. Confidential information (if any).

11. Date of cancellation.
12. Self-authorisation.
13. Reviews.
14. Original copies of any documents.

8 Records Retention

Retention and Destruction of material obtained through Directed Surveillance.

All documents should be marked as Official-Sensitive and the SRO (RIPA Co-ordinator) is responsible for their retention, security and destruction in accordance with The Councils Data Retention Policies and the RIPA Codes of Practice.

8.1 Any material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained. This includes not only material that supports the prosecution's case, but that which may cast doubt on it or supports the case for the defence.

8.2 Unless the surveillance is recorded by means of electronic surveillance equipment, e.g., CCTV, sound recording equipment etc., then written logs must be kept of the surveillance activity.

8.3 All material shall be retained for six years.

8.3.1 All material that may be relevant to the investigation must be kept until a decision has been taken whether to instigate proceedings.

8.3.2 If proceedings are instigated, all material that may be relevant must be kept until either the accused is acquitted or convicted or the prosecution decides not to proceed with the case.

8.3.3 Where the accused is prosecuted, all material that may be relevant must be retained until, in the case of a custodial sentence being imposed, the convicted person is released from custody or the expiry of six months, whichever is the longer period, or six months from the date of conviction in all other cases.

8.3.4 Where an appeal is in progress that material must be kept until the conclusion of the appeal. Covert investigations conducted under Non-RIPA powers must be retained as directed by the relevant Assistant Director in consultation with Head of Legal.

8.4 Authorising and Investigating Officers must also ensure compliance with the appropriate data protection requirements and any relevant procedures produced by the authority in the handling and storage of material.

Much of the information obtained will amount to personal information within the meaning of the Data Protection Act 2018 and therefore, the requirements of that Act

must be adhered to when processing that information. Please refer to The Councils Data Protection Policy.

8.5 Please note that material that is obtained, particularly evidence, shall be stored securely both for data protection purposes and to avoid any accusation of tampering with evidence if court proceedings follow.

8.6 Material obtained from properly authorised directed surveillance can be used in other investigations where appropriate. The Councils legal advisor can assist further regarding the use and disclosure of such information.

9 Training and review

9.1 All The Councils officers undertaking covert surveillance shall be appropriately trained to ensure they understand their legal obligations. Authorising Officers shall attend appropriate, recorded training for that role at least every three years.

9.2 This Policy will be reviewed every three years by the SRO, who will make an annual report to the Audit and Governance Committee at The Councils on any amendments to the Policy and any surveillance carried out within the previous year.

9.3 The SRO (RIPA Co-ordinator), Authorising Officers and all officers who are involved in investigation duties who may wish to consider covert powers available to The Councils must receive appropriate training every three years.

9.4 The relevant Committee of each Council should be given training on RIPA powers to assist their annual review.

10 Activity Requiring Authorisation

10.1 The following types of activity will require authorisation.

- Directed Surveillance
- The conduct and use of a CHIS.

Directed surveillance is any activity undertaken covertly for the purpose of a specified investigation, in such a way that it is likely to obtain information about a person's private life.

A covert human intelligence source (CHIS) is an inside informant or undercover officer (including someone who develops or maintains a relationship with the subject of the authorisation) having a covert purpose of obtaining or accessing information for the investigator.

11 Applying for Authorisations

11.1 Only Authorising Officers (AO's) can enable an application under the Act. These persons are listed in **(Appendix 1)**.

11.2 AO's may authorise for any service at any Council (however see **12.4** regarding departmental leads).

11.3 To apply, the investigator should select and complete the appropriate application form from the link above and send securely to the AO. Guidance and documents can be found at the end of this Policy.

11.4 All information should be marked as Official-Sensitive when sent to the AO.

11.5 The investigator should include all steps taken so far in the investigation and any steps to be taken if the authorisation is made so that it is clear what the authorisation is for.

12 Granting of Authorisations by AO

Section 28 of RIPA states:
"*a person shall not grant an authorisation for directed surveillance unless he believes that authorisation is:*

- *necessary for the purpose of preventing or detecting crime, or of preventing disorder involving a crime; and*
- *the authorised surveillance is proportionate to what is sought to be achieved by it."*

12.1 There is a **crime** threshold to be reached, i.e., the criminal offence;

- is or would be punishable (whether on summary conviction or on indictment) by a maximum term of at least 6 months of imprisonment, or
- it arises from the underage sale of alcohol, tobacco, or nicotine inhaling products.

12.2 Use of recording or enhanced sight devices

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted.

12.3 Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used. (See R v Johnson (Kenneth) 1988 1 WLR 1377.

12.4 Authorisations must be given in writing

It is possible that Authorising Officers may face cross-examination in court about the authorisation some length of time after it is granted, and memories fade. It is therefore important that a full written record of what they are being asked to authorise, appears on the application form. If in doubt, Authorising Officers should ask for more detail.

12.5 Authorising Officers should not be responsible for authorising their own activities or that of their own service areas.

All RIPA authorisations must be approved by a Magistrate before an authorisation becomes effective and directed surveillance is undertaken, or a CHIS deployed.

12.6 Implementation

- Senior Responsible Officer, Line Managers and Service Managers will be responsible for ensuring that the requirements of the Regulation of Investigatory Powers Act 2000 are complied with.

- The Accountable Officers will be Managers, Assistant Directors, Deputy Chief Executives and Chief Executive.

- All officers will need to be informed and made aware of the existence of this policy, but more particularly those officers involved in enforcement activities or undertake or sanction investigatory activities, including Fraud, Community and Neighbourhood Services, Environmental Health, Licensing, Housing, HR, Planning and Internal Audit.

12.7 Duration of Authorisations and Reviews

RIPA authorisations are only valid for 3 months. If a renewal is required, it must be applied for prior to the three-month deadline. Renewals must be authorised by The Councils Authorising Officer and a Magistrate. An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect, e.g., an authorisation starting 1st January would come to an end on 31st March.

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on the appropriate form and a copy filed on the central record of authorisations and any paper copies are to be held in CCTV Control Room, Boston. This will be the repository for all three Councils. If the surveillance provides access to confidential information or involves collateral intrusion, more frequent reviews will be required. The Authorising Officer should determine at the time of giving the initial authorisation, how often a review should take place (and this may also be subsequently reviewed).

12.8 Renewals

12.8.1 While an authorisation is still in force, the Authorising Officer can renew it if he considers this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired, but for the renewal, and can be for a period up to 3 months, however AOs may impose a shorter review period if applicable. Magistrates' approval is also required on the renewal of any such applications.

12.8.2 Applications requesting renewal of an authorisation are to be made on the appropriate form and submitted to the Authorising Officer.

The renewal must be granted before the original authorisation ceases to have effect.

12.8.3 Applications for renewal will record whether it is the first renewal; and if not, every occasion on which the authorisation has previously been renewed. Applications must also detail;

- the significant changes to the information in the initial 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
- the results of regular reviews of the investigation or operation.

When a directed surveillance authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation.

12.9 Cancellations

The person who granted or last renewed the authorisation (or other person with Authority under this policy) **MUST** cancel it if s/he is satisfied that the directed surveillance no longer meets the criteria for authorisation.

Requests for cancellation will be made on the appropriate form and submitted to the Authorising Officer for authorisation of the cancellation. All directed surveillance cancellations must include directions for the management and storage of any surveillance product.

12.10 Granting of authorisation for the use of Covert Human Intelligence Sources (CHIS) See **Appendix 3**

12.11 Monitoring of personal information online

The study of an individual's on-line presence may engage privacy considerations requiring RIPA authorisation. The attached **Appendix 4** gives guidance on the monitoring of information online, such as social media.

13 Maintenance of Records

13.1 The SRO (RIPA Co-Ordinator) shall keep in a dedicated place;

- a record of all authorisations sought
- a record of all authorisations, whether granted or refused
- applications for the granting, renewal and cancellation of authorisations.

The records will be confidential and will be retained for a period of six years from the ending of the authorisation.

13.2 Each Authorising Officer shall send original copies of all applications/authorisations, reviews, renewals and cancellations to the SRO (RIPA Co-coordinating Officer), who will maintain a central record of all authorisations.

13.3 The SRO and Authorising Officers will ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling, access and storage of covert investigation documents and obtained information.

13.4 Where material is obtained by surveillance or a CHIS which is;

- wholly unrelated to a criminal or other investigation, or
- to the person subject of the surveillance, and
- there is no reason to believe it will be relevant to future civil or criminal proceedings,
  it should be destroyed immediately.

The decision to retain or destroy material will be taken by the relevant Authorising Officer.

14 Training and awareness of the contents of the Act

It shall be the responsibility of each Service Manager, or an Authorised Officer for that service, to ensure that all staff involved or likely to be involved in investigations that require RIPA powers, are adequately trained in order that they will be aware of the requirements and implications of the Act.

15 Non-RIPA Surveillance

From time to time a local authority may wish to undertake covert surveillance,which is not regulated by RIPA. This is acceptable as RIPA is permissive legislation.

15.1 Where the matter being investigated falls outside of RIPA, the procedure in this part of the Policy can be followed. It is important to remember that The Councils actions could be challenged both by claiming that the evidence obtained through

non-RIPA surveillance is inadmissible, or that The Councils have infringed a person's civil liberties.

This could lead to action being taken against The Councils in the civil courts. An individual might also complain to the Local Government and Social Care Ombudsman about The Councils actions.

It is therefore very important that non-RIPA surveillance is only considered in appropriate cases and the appropriate non–RIPA authorisation is sought.

15.2 Authorisation under RIPA affords a public authority a defence under Section 27 i.e., the activity is lawful for all purposes. However, failure to obtain an authorisation does not make covert surveillance unlawful. Refer to **(Appendix 5)**

15.3 A local authority may wish to conduct "Non-RIPA Surveillance" for one of two reasons;

1. Crimes Not Carrying Six Months Imprisonment
2. Employee Surveillance.

Under RIPA legislation, Authorising Officers may not authorise directed surveillance unless;

i. It is for the purpose of preventing or detecting a criminal offence **AND**
ii. meets the 'crime threshold' set out in regulation 7A of the 2010 Order.

The 'crime threshold' is met if the purpose of the directed surveillance is to detect or prevent criminal offences for which the punishment on conviction is a term of imprisonment of not less than 6 months or the offences or the activity subject to directed surveillance constitute an offence under sections 146, 147 or 147A of the Licencing Act 2003 or section 7 of the Children and
Young Persons Act 1933 (offences involving sale of alcohol and tobacco to underage children).

15.4 Covert surveillance that does not meet the six-month Crime threshold test.

The Chief Surveillance Commissioner in his annual report (2010/2011) stated:

"The higher threshold in the proposed legislation will reduce the number of cases in which local authorities have the protection of RIPA when conducting covert surveillance; it will not prevent the use of those tactics in cases where the threshold is not reached but where it may be necessary and proportionate to obtain evidence covertly and there will be no RIPA audit trail.
Part I of RIPA makes unauthorised interception unlawful. In contrast, Part II makes authorised surveillance lawful but does not make unauthorised surveillance unlawful."

16 Surveillance of Employees

Most employee surveillance will not be authorisable under RIPA, if a previous decision by the Investigatory Powers Tribunal is to be followed. Refer to **Appendix 6**

16.1 It has been acknowledged that there may be occasions when during the course of an investigation that it may become necessary to conduct surveillance of individuals (including members of staff) in respect of matters that do not satisfy the crime threshold, therefore would not meet the RIPA process criteria, but would if proven amount to a serious breach of The Councils code of conduct, for example Gross Misconduct.

In these circumstances, the IPCO has stated that it would be good practice for the investigating officer to go through the RIPA authorisation process in terms of;

i. Why there is no other alternative to undertaking the directed surveillance;
ii. Why the surveillance is necessary; and
iii. How it is proportionate in the circumstances.

16.2 Where it is deemed that the above-mentioned criteria have been satisfied, the non-RIPA surveillance should be monitored and reviewed in accordance with this policy.

Any authorisation under the Non-RIPA process must meet the same levels of necessity and proportionality as the RIPA levels required.

17 What happens if any surveillance has unexpected results (RIPA and Non-RIPA)

Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly encounters the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (known as collateral intrusion).

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. In some cases, the original authorisation may not be sufficient and consideration should be given to whether a separate or updated authorisation is required.

18 Human Rights Compliance

Covert surveillance done without a RIPA authorisation will not have the protection of RIPA (i.e., the defence in section 27).

However, it may still be undertaken if it is done in accordance with the European Convention on Human Rights (ECHR) which is directly enforceable against public authorities pursuant to the Human Rights Act 2018. Article 8 of the ECHR which states:

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

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others."

To satisfy Article 8, the covert surveillance must be both necessary and proportionate. In deciding whether it is, the same factors need to be considered as when authorising surveillance regulated by RIPA.

19 Non-RIPA Data Protection Compliance – Surveillance of Employees

19.1 When carrying out covert surveillance of employees not regulated by RIPA, the Data Protection Act 2018 (DPA) will apply as personal information about living individuals will be processed e.g. their movements, photographs etc.

The Information Commissioner has published a Data Protection Employment Practices Code (available at The employment practices code (ico.org.uk)).

Part 3 of this code covers all types of employee surveillance from CCTV monitoring, vehicle informatic tracking, email and internet interception and surveillance. It gives guidance on how to perform employee surveillance in a way which complies with the DPA. Whilst the code is not law, it can be taken into account by the Information Commissioner and the courts in deciding whether the DPA has been complied with.

The code states that employee monitoring should take place for a clear justified purpose and employees should be aware that it is taking place. Regarding covert surveillance, it states that it will be rare for such monitoring to be justified. It should therefore only be used in exceptional circumstances e.g., prevention or detection of crime or serious Gross Misconduct.

19.2 One of the other main recommendations of the code is that senior management should normally authorise any covert monitoring of employees. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent Gross Misconduct. They should carry out an impact assessment and consider whether the surveillance is necessary and proportionate to what is sought to be achieved.

External advice from RIPA advisors and experts should be sought at this stage.

19.3 The code sets out other rules that local authorities (and others) need to consider when carrying out covert surveillance of employees:

Prior to the investigation, clear rules must be set up limiting the disclosure and access to information obtained;

- the number of people with knowledge of a covert monitoring exercise should be limited
- the surveillance must be strictly limited to obtaining evidence within a set time frame and it should not continue after the investigation is complete
- if using audio or video equipment, this should not normally be used in places such as toilets or staff changing areas
- information obtained through covert monitoring should only be used for the prevention or detection of criminal activity or serious Gross Misconduct
- other information collected while monitoring should be disregarded and, where feasible, deleted unless it reveals information that no responsible employer could reasonably be expected to ignore.

As in the formal RIPA process, it is important to have a proper audit trail through written records.

To demonstrate compliance, the same forms for a RIPA authorisation need to be completed for a non-RIPA authorisation. The difference is that is does not need Judicial approval (no need to go to the Magistrate's Court)

19.4 Non-RIPA Authorisation Form

Application for authorisation to conduct Covert Surveillance which is not regulated by RIPA.

All forms should be completed by an officer of the local authority seeking authorisation to carry out surveillance which does not fall within the definition of Directed Surveillance in section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA). This could include surveillance where the subject is doing something which is not a criminal offence (or which does not carry a term of imprisonment of six months or more), misusing the work e-mail/internet system or breaching a legal agreement (e.g. tenancy agreement).

Before completing any of the forms contained in the links below, you should consult:

- The ICO Employment Practices Code: Part 3 (Staff Surveillance)
- The Councils SRO (RIPA Co-Ordinator)

19.5 Application for authorisation to conduct surveillance not regulated by RIPA

Consideration should be given to:

- who is going to do it
- when they are going to do it
- where they are going to do it and
- how they are going to do it.

Other points to address here include:

- how long will the surveillance last
- specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times
- any risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion)
- which premises are to be used and/or targeted
- which vehicles are to be used, are they public or private
- what type of equipment is to be used e.g., covert cameras, audio devices
- what is the capability of the equipment to be used? e.g., zoom lens, remote controlled etc.
- who else will be involved in the operation and what will be their role? e.g., private detectives, police
- what is the aim or an acceptable result of the surveillance
- evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented
- whether external RIPA advice and expertise is required.

In order to comply with the above, you need to address the following points:

- why the surveillance necessary
- how is the surveillance proportionate to the aims
- can you get information using less intrusive means/overt methods?
- indicate the likelihood of acquiring any confidential information and why it is necessary to continue with the surveillance.

20 Collaborative working

The Councils may on occasion work with partners and other organisations in such tasks as joint operations between Environmental Health or Licensing and the police. In such cases there may be confusion around who should obtain the authorisation under RIPA.

20.1 If The Councils service is acting on behalf of another organisation e.g., CCTV operatives or Licensing officers are acting on behalf of the Police, the Police should provide the RIPA authorisation. In such cases, the application and authorisation will be completed by the Police and not The Councils.

20.2 If The Councils are carrying out their own investigation but it is clear from the outset that operational support will be required as part of the investigation this should be stated in the authorisation.

20.3 In joint operations only one authorisation is required. In a case when each party to the investigation has completed an authorisation, the lawfulness of the activities will not be affected.

21 Member Involvement

The relevant Committee of each Council should consider (sanitised) reports on the use of RIPA and Non-RIPA powers under the Act on an annual basis to ensure that it is being used consistently with this policy. The relevant Committee of each Council will also consider reports from the IPCO.

Note: no personal data involving subjects etc. shall be included in these reports or disclosed at any point.

Members of The Councils will not however be involved in making decisions on specific authorisations.

The relevant Committee members should be given training on RIPA powers to assist their annual review.

22 Surveillance Equipment held by The Councils

This policy applies to covert surveillance activities carried out by, or on behalf of the Councils and includes, but is not limited to, the following:

- the taking of photographs of someone in a public place or
- the recording by video cameras of someone in a public place (not routine use of The Councils' CCTV system)
- the use of recording equipment or photographic equipment in respect of activities in a house, provided the equipment is kept outside the house and the equipment gives information of less quality and detail than devices which could have been placed in the house itself
- the taking of photographs of staff in the workplace or
- the recording by video cameras of staff in the workplace.

22.1 Any equipment (for example recording equipment or video/photographic equipment) should be stored, when not in use, in a locked cabinet under the control of the relevant Service Manager.

22.2 Any Officer of The Councils considering using the Equipment for covert surveillance in a public place must make a written request to the SRO (RIPA Co-ordinating Officer), who will consider and decide whether the proposed use of the Equipment is appropriate, bearing in mind the provisions of RIPA and the associated codes of practice.

22.3 Any Officer who uses the Equipment to record digital images may only view

such images once captured and shall not download them on to a computer or other electronic storage facility unless this is first agreed by the Senior Responsible Officer.

Note: Staff personal devices (mobile phones etc.) should not be used to record any activity during any RIPA operations.

23 CCTV consideration

The routine use of overt, unconcealed CCTV cameras for the purpose of generally observing activity in a particular area as used by The Councils on a daily basis is not surveillance as defined by the RIPA legislation.

23.1 There are specific, existing provisions regulating the use of CCTV cameras in public places and buildings and The Councils has a CCTV Policy which officers must comply with. However, if CCTV cameras are being used in a way that the definition of covert directed surveillance is satisfied, for example to follow or watch specific subjects who are the focus of any pre-planned operations, RIPA authorisation should be obtained.

23.2 The use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation. Conversely, the use of the same CCTV system to conduct planned surveillance of an individual and record his movements is likely to require authorisation.

23.3 Agreement must be in place with any external agencies requesting use of The Councils CCTV system. Such agreements ensure that The Councils can be confident that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

23.4 A copy of the RIPA authorisation should be requested (redacted as necessary) from the external agency who is requesting the use of The Councils CCTV system.

24 Acquisition and Disclosure of Communications Data

Communication Service Providers ("CSPs"). CSPs are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Councils must obtain communications data from CSPs in strict compliance with RIPA.

24.1 Types of Communications Data

Communications data is the 'who', 'where', 'when' and 'how' of a communication such as a letter, phone call or e-mail but not the content, not what was said or written. There are three types of communication data:

- **Service Use Information** data relating to the use made by any person of a

postal or telecommunications,
  - internet service, or any part of it. This could be itemised telephone call records,
  - itemised records of connection to internet services,
  - itemised timing and duration of calls, connection/disconnection/reconnection data, use of forwarding or re-direction services,
  - additional telecom services and records of postal items.
- **Subscriber Information** is information held or obtained by the CSP about persons to whom the CSP provides or has provided a communications service:
  - subscribers of email and telephone accounts, account information including payment details, address for installing and billing,
  - abstract personal records and sign up data.
- **Traffic Information** – this is data that is comprised in or attached to a communication for the purpose of transmitting it and which identifies a person or location to or from which it is transmitted.

The Council is not permitted to access the content of any communications but can access cell location of telephone and internet traffic.

25 Authorisations and Notices

25.1 Section 73 of the Investigatory Powers Act 2016 provides that The Councils, as a local authority, is a relevant public authority for the purposes of Part 3 of this Act (Authorisations for Obtaining Communications Data).

25.2 Subsection (3) provides that local authorities may only acquire communications data for the purpose of preventing or detecting crime or of preventing disorder.

25.3 Local authorities are only able to obtain communications data if they are party to a collaboration agreement as certified by the Secretary of State. The Councils currently uses the National Anti-Fraud Network (NAFN) as a shared Single Point of Contact (SPoC) service.

25.4 The Councils authorisations to obtain communications data can only take effect if approved by the Office of Communications Data Authorisations (OCDA) once all the internal authorisation processes have been completed, including consultation with a NAFN Single Point of Contact (SPoC), but before the SPoC requests the data from the Telecommunications Provider (i.e. Internet Service Provider (ISP) or a Telecommunications Operator (TO)

25.5 Authorisation Procedures

The introduction of the Office for Communications Data Authorisations (OCDA) means
the acquisition of communications data by local authority officers is no longer subject

to
judicial approval by a magistrate.

25.6 Designated Senior Officers (DSO)

DSO's fulfil a similar role in relation to applications to obtaining communications data, assessing and approving authorisations and notices. It is the responsibility of the Designated Senior Officer to ensure that when applying for authorisation the principles of necessity and proportionality are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

25.6.1 Any requests for amendments to the lists must be made in writing and sent to the Head of Legal. Section73 of the IPA 2016 prescribes the rank or position of such officers as being a "Director, Head of Service, Service Manager or equivalent")

The Head of Legal designates which officers can be DSO's. Only these officers can authorise the disclosure of communications data. All authorisations must follow the procedures set out in the Policy.

25.7 Single Point of Contact (SPoC)

SPoCs are responsible for advising officers within The Councils on how best to go about obtaining communications data, for liaising with CSPs, and advising whether applications and notices are lawful. As required under the latest Acquisition and Disclosure of Communications Data Code of Practice, The Councils has engaged the National Anti- Fraud Network (NAFN). NAFN's SPoC services relate only to communications data. For information on using NAFN, see 27.5.5 below.

Additional Requirements for Authorisation of Acquisitions and Disclosure of Communications Data

The rules on the granting of authorisations for the acquisition of communications data are slightly different from directed surveillance and CHIS authorisations and involve three roles within The Councils. The roles are:

- Applicant Officer
- Designated Senior Officer (DSO)
- Single Point of Contact (SRO)

25.8 Applicant

This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The application form must;

- set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of The Councils for the prevention or detection of crime or preventing disorder
- describe the communications data required i.e., the telephone number, email

address, the specific date or period of the data and the type of data required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted
- explain why the conduct is necessary and proportionate
- consider and describe any meaningful collateral intrusion. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation

The applicant therefore needs to consider what the impact is on third parties and try to minimise it.

26 List of Application forms and guidance documents

A. Application for Authorisation of Directed Surveillance

B. Review of Directed Surveillance Authorisation

C. Cancellation of Directed Surveillance Authorisation

D. Renewal of Directed Surveillance Authorisation

E. Application for Authorisation of a Covert Human Intelligence Source

F. Review of Covert Human Intelligence Source Authorisation

G. Cancellation of Covert Human Intelligence Source Authorisation

H. Renewal of Covert Human Intelligence Source Authorisation

I. Judicial and Magistrates Application form (Attached)

The Councils Judicial/Magistrates Approval Form.

Application for judicial approval for authorisation, to use a covert human intelligence source or to conduct directed surveillance.

Local Authority .....

Local Authority Department .....

Offence under investigation .....

Address of premises or identity of subject:

.....

.....

.....

Covert technique requested: (tick one and specify details)

☐ **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 use a covert human intelligence source or to conduct directed surveillance.

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:

Appendix 1

List of Officers Authorised under this Policy

POSITION	NAME
Senior Responsible Officer	Christian Allen
Authorising Officer	Andy Fisher
Authorising Officer	Duncan Hollingsworth
Authorising Officer	Donna Hall
Authorising Officer	Dee Bedford
Non-RIPA Authorising Officer	Matt Fisher
Non-RIPA Authorising Officer	Peter Hunn

Appendix 2

The RIPA Covert Surveillance Code of Practice contains detailed guidance on proportionality:

1 This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who might be affected) against the need for the activity in investigative and operational terms."

2 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.

3 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."

4 AOs must demonstrate that they have:

- balanced the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explained how and why the methods to be adopted will cause the least possible intrusion on the subject of the surveillance and others
- considered whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result
- evidenced, as far as reasonably practicable, what other methods had been consideredand why they were not implemented.

5 In order to comply with the above, you need to address the following points:

- can you get information using less intrusive means/overt methods ?
- are you likely to obtain any Confidential information during the surveillance
- indicate the likelihood of acquiring any confidential information and any mitigating factors why you should continue with the activity.

The Home Office Code of Practice on Covert Surveillance and Property Interference should be considered on the issue of proportionality (paragraphs 4.5 and 4.6):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Appendix 3

Granting of authorisation for the use of Covert Human Intelligence Sources (CHIS)

The Councils is permitted to use a CHIS subject to Section 29 of the Regulation of Investigatory Powers Act

The use of a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be considered to be a tool of last resort, to be used only when all other less intrusive means have been used or considered.

The times when the Councils will use a CHIS are very limited.

The use of Section 29 authorisations by local authorities in England and Wales is subject to judicial approval. Local authorities do not have the power to grant Criminal Conduct Authorisations.

1 A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:

(a) covertly using the relationship to obtain information or provide access to information to another person, or
(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

A person who reports suspicion of an offence or incident is not a CHIS, nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

2 Test purchasers
Where a test purchaser is tasked to make a single purchase, any relationship with the supplier is likely to be too limited to require a CHIS authorisation. On the other hand, if the test purchaser has to become acquainted with the vendor in order for him to make a sale, a relationship will have been established and the test purchaser will be treated as a CHIS. If there is any doubt whether authorisation is required in relation to a particular operation, then the Investigating Officer should seek advice and may require formal RIPA authorisation.

3 The Councils need to obtain an order approving the grant or renewal of a Section 29 authorisation from a Justice of the Peace before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use or conduct is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the CHIS as described in the application. This amendment also means that local authorities in England and Wales are no longer able to grant a Section 29 authorisation orally.

A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a The Councils officer or any another person who is asked to act as a CHIS on The Councils's behalf.

4 Authorisation for a CHIS can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder."

5 Duration of authorisations
A written authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect, except in the case of juvenile CHIS.

The duration of authorisation for juvenile CHIS is four months from the time of grant or renewal (instead of twelve months).

The authorisation for the use of juvenile CHIS should be subject to at least monthly review.

For the purpose of decisions about authorisation, the age test is applied at the time of the grant or renewal.

6 All authorisations must be cancelled when they are no longer necessary or proportionate.

7 Officers considering the use of a CHIS under the age of 18, and those authorising such activity must be aware of the additional safeguards identified in The Regulation of Investigatory Powers (Juveniles) Order 2000 and its Code of Practice.

8 A CHIS aged 16 or 17 years old should only be deployed to gather evidence against their parents or any person who has parental responsibility for them where careful consideration has been given to whether the authorisation is justified in light of that fact. In such instances the rationale must be documented by the public authority.
Note: On no occasion should a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Juveniles Order are satisfied.

9 **Confidential Material.** Where the likely consequence of the directed surveillance or conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of a CHIS should be subject to special authorisation. In these cases, the proposed course of conduct must be referred to the SRO (RIPA Co-Ordinator) for a decision as to whether authorisation may be granted.

Wherever knowledge of confidential information is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be

made by the Chief Executive (or in their absence whoever deputises for this role)

10 The same requirements of necessity and proportionality exist for the granting of these authorisations as with directed surveillance.

11 Additionally, the Authorising Officer shall not grant an authorisation unless he /she believes that arrangements exist which satisfy the following requirements:

- there will at all times be an officer with day-to-day responsibility for dealing with the CHIS and the source's security and welfare
- there will at all times be an officer who will have general oversight of the use made of the source
- there will at all times be an officer with responsibility for maintaining a record of the information supplied by the source
- records which disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available.

12 Similarly, before authorising the use or conduct of the source, the Authorising Officer must be satisfied that the conduct/use is proportionate to what the use or conduct of the CHIS seeks to achieve, considering the likely degree of intrusion into the privacy of those potentially effected, and for the privacy of persons other than those who are directly the subjects of the operation or investigation.

13 Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

14 Particular care is required where people would expect a high degree of privacy, or where, as a consequence of the authorisation, 'confidential material' is likely to be obtained.

15 Consideration is also required to be given to any adverse impact on community confidence that may result from the use or conduct of a CHIS or information, obtained from that source.

16 Additionally, the Authorising Officer should assess any risk to a source, in carrying out the conduct in the proposed authorisation.

17 Authorisation for the use of a CHIS must be given in writing

Only the Chief Executive (or in his/her absence the person who is formally nominated to act as the Chief Executive) may authorise the use of CHIS where knowledge of confidential information is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS.

18 Ideally, the Authorising Officers should not be responsible for authorising their own activities e.g., those in which they themselves are to act as a source, or in tasking a source.

19 Authorisations must be approved by a Magistrate

The Solicitor employed by The Councils will arrange the appointment before the Magistrate(s) and explain the procedure to the Authorising Officer. The Solicitor employed by The Councils and the investigating officer will be required to attend before the Magistrate(s) to seek the Magistrate's approval to the authorisation.

20 CHIS Application Process

An application for authorisation for the use or conduct of a CHIS will be made on the appropriate form and must record:

- details of the purpose for which the source will be tasked or deployed
- the reasons why the authorisation is necessary in the particular case and the grounds on which authorisation is sought (e.g., for the purpose of preventing or detecting crime or disorder)
- where a specific investigation or operation is involved, details of that investigation or operation
- details of what the CHIS would be tasked to do
- details of potential collateral intrusion and why the intrusion is justified
- details of any confidential material that might be obtained as a consequence of the authorisation
- the reasons why the authorisation is considered proportionate to what it seeks to achieve
- the level of authorisation required.

A subsequent record of whether authorisation was given or refused by whom and the time and date.

21 Duration of Authorisation of a CHIS

A written authorisation, unless renewed, will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect except

The duration of Authorisations for juvenile CHIS is four months from the time of grant or renewal (instead of twelve months),

22 Renewal of a CHIS

As with authorisations for directed surveillance, authorisations for the conduct and use of CHIS can be renewed, the same criteria applying. However, before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS and that the results of the review have been considered.

23 Applications for renewal must be made on the appropriate form and submitted to the Authorising Officer. An application for renewal should not be made until

shortly before the authorisation period is coming to an end.

24 An authorisation may be renewed more than once provided it continues to meet the criteria for authorisation.

When CHIS authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation.

25 Review

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on the appropriate form and a copy filed on the central record of authorisations.

26 If the surveillance provides access to confidential information, or involves collateral intrusion, frequent reviews will be required. The Authorising Officer should determine how often a review should take place.

27 Before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of:

- the use made of the source during the period authorised
- the tasks given to the source
- the information obtained from the use or conduct of the source.

28 If the Authorising Officer is satisfied that the criteria necessary for the initial authorisation continue to be met, he may renew it in writing as required.

29 When CHIS authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation.

30 Cancellations

The officer who granted or renewed the authorisation **MUST** cancel it if he/she is satisfied that:

- the use or conduct of the CHIS no longer satisfies the criteria for authorisation, or
- that the arrangements for the source's case no longer exist

31 Requests for cancellation will be made on the appropriate form and submitted to the Authorising Officer for authorisation of the cancellation.

All CHIS cancellations must include directions for the management and storage of any surveillance product.

32 Management Responsibility

The day-to-day contact between The Councils and the CHIS is to be conducted by the handler, who will usually be an officer below the rank of the Authorising Office

33 Security and Welfare

A risk assessment considering the security and welfare of the CHIS must be carried out by an AO to determine the risk to the CHIS of any tasking by the investigating officer, and the likely consequences should the subject of the surveillance know the role of the CHIS.

Appendix 4

Guidance on the use of Social Networking Sites for investigations

It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for The Councils's staff carrying out investigations. These investigations may relate to the various enforcement roles within The Councils – for example Fraud, Planning Enforcement, Licensing or Environmental Health, but will equally apply to some non-enforcement teams, such as Debt Collection or Housing.

The use of internet and social networking sites may fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

1 Social Networking Sites

There is a fine line between general observation, systematic observation and research and it is not sufficient to rely on a perception of a person's reasonable expectations or their ability to control their personal data.

2 Guidance for officers in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

- officers must not 'friend' individuals on social networks as part of undertaking their roles
- officers must not use their own private social networking accounts to view the social networking accounts of other individuals as part of their professional role
- officers viewing an individual's profile on a social networking site should do so on one occasion only, to obtain evidence to support or refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must take place on only one occasion when RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

The purpose of this guidance note is to provide clarity on The Councils position.

3 It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise.

This might include but is not limited to sites such as 'Facebook', X (Twitter) and 'LinkedIn.' Sites used to advertise goods and services should be included within the

definition.

As the definition of 'private information' under RIPA includes:
'any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships'

4 Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any enforcement proceedings.

5 If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile on one occasion in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.

The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

6 In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing.

However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

7 Each single viewing of an individual's social networking site must be recorded on the investigation file stating who viewed it, when and why. This is to enable scrutiny and reporting to IPCO if necessary as well as to evidence on the investigation file that there has been no misuse of RIPA.

8 If it is considered that there is a need to further monitor an individual's social networking site with a view to gathering evidence then authorisation must be obtained from an Authorising Officer.

9 If the offence being investigated falls within the threshold levels under RIPA, a formal RIPA application must be completed, authorised by one of The Councils' Authorising Officers and then approved by a Magistrate.

10 If the offence being investigated falls outside of RIPA (for example if the offence does not carry a custodial sentence of at least 6 months imprisonment or is not a core function of The Councils) a non-RIPA form must be completed. Guidance is available in the links at the end of this document.

Appendix 5 – Non-RIPA surveillance

S.80 states:

"*Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner,shall be construed –*

- *as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;*
- *as otherwise requiring:*
- *the issue, grant or giving of such a warrant, authorisation or notice, or*
- *the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice, before any such conduct of that description is engaged in; or*
- *as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.*"

This point was explained more fully by the Investigatory Powers Tribunal in the case of:

C v The Police (Case No: IPT/03/32/H 14th November 2006):

"Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful."

Appendix 6 – Non-RIPA surveillance

Consider

C v The Police and the Secretary of State for the Home Department (14th November 2006, No: IPT/03/32/H),

C, a former police sergeant, retired in 2001 having made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an enhanced pensiondue to the injuries.

In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming they had carried out directed surveillance without an authorisation. The Tribunal first had to decide if it had jurisdiction to hear the claim. The case turned on the interpretation of the first limb of the definition of directed surveillance i.e., was the surveillance "for the purposes of a specific investigation or a specific operation?"

The Tribunal ruled that this was not the type of surveillance that RIPA was meant to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers."

The Tribunal also stated that it would not be right to apply RIPA to such surveillance for a number of reasons:

- RIPA does not cover all public authorities, and there was no sense in police employee surveillance being conducted on a different legal footing than, for example, the Treasury, which does not have the same surveillance rights under RIPA.

- The Tribunal has very restrictive rules about evidence, openness and rights of appeal. The effect of these would lead to unfairness for employees of RIPA authorities when challenging their employers' surveillance, as compared to those who were employed by non-RIPA authorities.

This case study suggests that, even where employee surveillance is being carried out on one of the grounds in section 28(3), the question has to be; is it for a core function linked to one of the authority's regulatory functions?