Herefordshire Council

Reference number
Approved by: cabinet
Date approved: June 2014
Version: 2.0
Last revised: 5 April 2018
Review date: April 2020
Category
Owner: Legal services
Target audience: council officers

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

After the Review Date has expired, this document may not be up-to date. Please contact the document owner to check the status after the Review Date shown above. If you would like help to understand this document, or would like it in another format or language, please contact the document owner.

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

GENERAL STATEMENT OF POLICY

This policy document explains how Herefordshire Council will comply with the Regulation of Investigatory Powers Act 2000 ('RIPA') in relation to directed surveillance, use of covert human intelligence sources and the acquisition of communications data. This Policy is supplementary to the:

Regulation of Investigatory Powers Act (RIPA) 2000 -
http://www.legislation.gov.uk/ukpga/2000/23/contents

Guidance on the use of covert surveillance or human intelligence sources by public authorities under part 2 of the Regulation of Investigatory Powers Act (RIPA) 2000.-
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance -
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

1.0 BACKGROUND

1.1 The primary function of central and local government regulation and enforcement is to protect the individual, the environment, and a variety of groups such as consumers and workers. At the same time, carrying out regulatory functions in an equitable, practical and consistent manner helps to promote a thriving national and local economy, and to prevent and detect crime and disorder.

1.2 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. RIPA sets out a regulatory framework for the use of covert surveillance techniques by public authorities. If such activities are conducted by council officers then RIPA regulates them in a manner which is compatible with the European Convention on Human Rights (ECHR), particularly Article 8 (the right to respect for private and family life).

1.3 Sections 37 and 38 of the Protection of Freedoms Act 2012 (the Act) came into force on 1 November 2012. Under the Act, local authority authorisations and notices for the use of particular covert techniques (direct surveillance, covert human intelligence sources (CHIS) and the acquisition of communications data) can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

1.4 In addition amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco.

1.5 Herefordshire Council will on occasion need to use covert surveillance in order to carry out its enforcement functions effectively. Examples of enforcement activities which may

require the use of RIPA include trading standards, community and fire safety, fraud investigations and child protection.

1.6 The council takes seriously its responsibilities as a regulatory authority and will at all times act in accordance with the law, ensuring that any regulatory and enforcement action it takes is lawful, necessary and proportionate.

2.0 SCOPE AND DEFINITIONS

2.1 This policy applies to all Herefordshire Council services.

2.2 The main purpose of RIPA is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

- interception of communications
- acquisition of communications data (e.g. billing data)
- intrusive surveillance (on residential premises/in private vehicles)
- directed surveillance in the course of specific operations
- use of covert human intelligence sources (informants etc)
- access to encrypted data

2.3 By working in conjunction with other, pre-existing legislation, the Act ensures the following points are clearly covered:

- purposes to which relevant powers may be used
- which authorities can use the powers
- authorisation of the use of the powers
- the use that can be made of material gained
- independent judicial oversight
- a means of redress for the individual where powers are breached

2.4 RIPA limits local authorities to using 3 covert techniques for the purposes of the prevention or detection of crime or prevention of disorder. These techniques are:

- **Directed surveillance** - surveillance which is covert but not intrusive, and which is undertaken for the purposes of a specific investigation or a specific operation, in such a manner as is likely to result in obtaining information about a person – whether or not the target of the investigation/operation.

- A **covert human intelligence source (CHIS) -** undercover officers, public informants and people who make test purchases.

- **Communications data (CD)** - is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into 3 parts:

    - 'traffic data' (which includes information about where the communications are made or received);
    - 'service use information' (such as the type of communication, time sent and its duration); and
    - 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).

2.5 The council must be satisfied that there is an identifiable offence before authorising any covert surveillance. In addition the key tests in any application for authorisation are:

- Necessity
- Proportionality and
- Risk of collateral intrusion

3.0 DIRECTED SURVEILLANCE

3.1 Directed surveillance is defined in Section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

- for the purposes of a specific investigation or specific operation;

- in such a manner as it is likely to result in the obtaining of **private information** (Section 13) about the person (whether or not one specifically identified for the purposes of the investigation or operation); and

- otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practical for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance

3.2 The Council will only use directed surveillance to investigate a crime and where the criminal offence being investigated meets one of the following conditions:

- The offence is punishable, whether on summary conviction or on indictment to a maximum term of at least 6 months of imprisonment, or
- Section 146, 147 or 147A of the Licensing Act 2003 or
- Section 7 of the Childrens and Young Persons Act 1933

3.3 The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD.

3.4 No officer of the council will undertake intrusive surveillance. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.5 Surveillance operations will only be carried out by officers who have received appropriate training in human rights and the Act.

3.6 No officer within the council will undertake directed surveillance without prior or emergency authorisation (see section 7).

3.7 The use of directed surveillance under RIPA will not be authorised to investigate matters that do not involve criminal offences or to investigate low-level offences that do not meet the threshold test.

4.0 COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

4.1 A CHIS is defined by section 26(8) of RIPA as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within the following points;

- covertly uses such a relationship to obtain information or to provide access to any information to another person: or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship and
- authorisations will only be given to officers who have undergone appropriate training in human rights and the Act.

4.2 The authorisation for the conduct and use of a CHIS may include:

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

4.3 Vulnerable individuals (a person who is in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care or protect himself against significant harm or exploitation) may be authorised to act as a CHIS **only in the most exceptional circumstances.** Authorisation must be given by the chief executive or in his/her absence the director adults and wellbeing and he/she will only do so after taking advice from the solicitor to the council.

4.4 Authorisation will only be given for the use of a covert human intelligence source, when the activity is necessary:

- to prevent or detect crime,
- in the interests of public safety,
- for the economic well-being of the UK,
- the purposes of national security
- for protecting public health.

Or is revenue related or specified by the Secretary of State.

5.0 COMMUNICATIONS DATA

5.1 The term ‘communications data’ embraces the ‘who’, ‘when’ and ‘where’ of a communication but not the content, not what was said or written. It is information about a communication - not the communication itself.

5.2 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data such as service use and subscriber information. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.

5.3 In the case of communications data the RIPA authorisation or notice will be scrutinised by a single point of contact (a 'SPoC'). The SPoC is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and Communication Service Providers (CSPs). An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requests for CD are made

5.4 Under RIPA it is against the law for a business to intercept any electronic communication on its, or anyone else's, system. There are some exceptions to this:

- Interception is authorised under a warrant (this does not apply to local authorities)
- where the interception takes place with consent
- where the interception is connected with the operation of the communications service itself

5.5 Interception for business related workplace monitoring may be applicable in certain circumstances by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The regulations are designed to meet the legitimate needs of businesses to manage their information systems, making use of the capabilities of modern communications technology, but in a way that is consistent with high standards of privacy.

5.6 Interception of Council telecommunications will only be made in accordance with the Regulations, and following procedures agreed by the Assistant Director Governance. Interception may be carried out in the following circumstances:

- To establish the existence of facts or to ascertain compliance with regulatory or self-regulatory practices (e.g. to keep records of communications where the specific facts are important, such as being able to prove that a customer has been given certain advice).

- To check the standards are being achieved or ought to be achieved (e.g. to check the quality of e-mail responses sent by members of staff to customer enquiries or for staff training).

- To prevent or detect crime (e.g. to check that employees or others are not involved in defrauding the Council).

- To investigate or detect unauthorised use of the telecommunications system. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised.

- To ensure the security of the system and its effective operation (e.g. to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

5.7 The Council will make all reasonable efforts to inform potential users that interceptions may be made.

6.0 COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

6.1 The use of the internet and, in particular, social networking sites[1], can provide useful information for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – 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 the internet and social networking sites may potentially 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).

6.2 In using social media for the gathering of evidence:

- officers must not 'friend' individuals on social networks
- officers should not use their own private accounts to view the social networking accounts of other individuals
- officers viewing an individual's profile on a social networking site should do so only once in order 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 only take place once 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.

6.3 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 once 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.

6.4 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.

6.5 If there is a need to monitor an individual's social networking site, authorisation must be obtained. 5. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by an Authorising Officers and then approved by a Magistrate.

7.0 AUTHORISATION

7.1 At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique

[1] 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 sites such as 'Facebook' and 'Linked-In'. Sites used to advertise goods and services should be included within the definition. 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.

and at the point it is decided whether or not to authorise its use, it must be clear that the threshold is met and that it is necessary and proportionate to use it.

7.2 The applicant will complete a written RIPA authorisation or notice form (appendix 1) setting out for consideration by the authorising officer or, for communications data the designated person; why use of a particular technique is necessary and proportionate in their investigation. This authorising officer or designated person will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.

7.3 In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. The chief executive or in his/her absence director economy, communities and corporate will authorise surveillance activity where confidential information is likely to be acquired, he or she will do so only after taking advice from the solicitor to the council.

7.4 "Confidential information" is defined for the purposes of RIPA as matters subject to legal privilege, confidential personal information or confidential journalistic material. Confidential material must not be copied or retained unless for a specific purpose – e.g. use in evidence in proceedings and may only be disseminated following advice from the Assistant Director Governance.

7.5 After the form has been countersigned the local authority will seek judicial approval for their RIPA authorisation or notice. The Justice of the Peace (JP) will decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP.

7.6 The time limits for authorised applications are three months for directed surveillance and twelve months for a CHIS (one month if the CHIS is under 18). Authorisations and notices for communications data will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

8.0 RESPONSIBILITIES

8.1 **Corporate Directors** to:

- ensure all regulatory staff are aware of and trained in the Act
- delegate the task of authorising surveillance operations
- provide procedures to be adopted in the application for, granting etc of, and recording of authorisation
- ensure copies of the Codes of Practice for Covert Surveillance, The Use of Covert Human Intelligence Sources, and Acquisition and Disclosure of Communications Data are available for public reference at council offices or by post or e-mail on public request
- ensure that details of the complaints procedure involving the Investigatory Powers Tribunal are readily available for public reference purposes at council offices or by post or e-mail on public request

8.2 **Director Economy, Communities and Corporate** to:

- Fulfil the role of senior responsible officer for RIPA and will be responsible for:
  - the integrity of processes for the management of CHIS
  - compliance with Chapter II of Part I of RIPA (acquisition and disclosure of CD)
  - compliance with Part II of RIPA (surveillance and CHIS)
  - oversight of the reporting of errors to the Investigatory Powers Commissioner's Office, identification of the cause(s) of errors and the implementation of processes to minimise repetition of errors
  - engagement with the commissioners' inspectors when they conduct their inspections
  - oversight of the implementation of post-inspection action plans approved by the commissioner.
  - maintaining a log of all RIPA applications, authorisations etc including copies of all completed forms, and reviewing the quality of applications, authorisations etc.
  - ensuring that all authorising officers are of an appropriate standard in light of any recommendations made by inspectors' reports
  - ensuring that cabinet members and members of the audit and governance committee have sufficient understanding of human rights and RIPA to be able to discharge their responsibilities under this policy

8.3 **Head of law and governance** to:

- maintain a record of all authorisations granted in the council
- report to audit and governance committee annually so that the committee can ensure that RIPA use is consistent with the policy and that the policy remains fit for purpose
- hold copies of all authorisations, extensions to and cancellations of authorisations and carry out an annual review of authorisations.

8.4 **Head of Regulatory and Development Management Services** to:

- act as the authorising officer or for communications data the designated person to consider applications, and issue, renew, cancel or refuse authorisations relating to investigations of council employees, in accordance with the criteria set out in the Act and in the Investigatory Powers Commissioner's Office office procedures and guidance - https://www.ipco.org.uk/docs/OSC%20Procedures%20&%20Guidance%20-%20%20July%202016.pdf
- ensure applications are complete and are made out on the appropriate *pro forma*, except in the case of emergency applications

- maintain a record of applications and authorisations, and provide copies to the head of law and governance within 5 working days of the application, irrespective of whether the authorisation is granted, and copies of all cancelled authorisations within 5 working days of the cancellation.

- ensure all staff involved in surveillance operations have access to the relevant codes of practice detailed below.

- review authorisations at least weekly and record the review on the authorisation and ensure that authorisations are cancelled as soon as they have either served their original purpose or no longer meet the criteria for issue, whichever is the earlier

- ensure that the forms and procedures detailed in the Trading Standards Investigations Manual are kept up to date and comply with RIPA and the codes of practice

- in the case of communications data to act as a single point of contact (a 'SPoC').

7.6 **All staff involved in surveillance operations** to:

- be familiar with Act, the relevant codes of practice, and the investigatory powers commissioner's office procedures and guidance - https://www.ipco.org.uk/docs/OSC%20Procedures%20&%20Guidance%20-%20%20July%202016.pdf

- ensure that the authorising officer is provided with all relevant information available to the investigation to enable an informed decision to be made

- advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance.

- cease the surveillance operation immediately it no longer meets the authorisation criteria

Appendix 1 to
Regulation of Investigatory Powers Act 2000 (RIPA)
Policy and Procedures

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

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Sourc ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

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

Address of applicant department:.....

.....

Contact telephone number:.....

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

Local authority reference:.....

Number of pages:.....

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

Magistrates' court:.....

Having considered the application, I (tick one):

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

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Document Classification

Author Name and Role	Erica Hermon, Head of law and governance
Date Created	June 2014
Date Issued	June 2014
Description	RIPA Policy
File Name	
Format	Microsoft Word / 2010
Geographic Coverage	Herefordshire
Master Location	Legal Services
Publisher	Herefordshire Council
Rights Copyright	Copyright of Herefordshire Council
Security Classification	
Status	
Subject	
Title	

Consultation Log

Date sent for consultation	
Consultees	

Approval Log

		Date
Impact assessment by		
To be agreed by		
To be approved by	Cabinet	12 Jun 2014
Finally to be ratified by		
To be reviewed by	Audit and governance committee	Annually

Version Log

Version	*Status*	*Date*	*Description of Change*	*Reason For Change*	Pages affected
2.0	*Published*	*5 April 2018*	*Updated logo, job titles, links and social media requirements*	*Job title changes and previous recommendation from inspection*	*All (with exception of appendix 1)*