UNCLASSIFIED

Procedural Guidance: RIPA Covert Surveillance & Covert Human Intelligence Sources

(Regulation of Investigatory Powers Act 2000)

Status/Version: Approved v3.0 May 2018

1 Introduction

1.1 This document sets out the procedures that need to be followed to ensure compliance with the law and the national codes of practice issued by the Home Office, Investigatory Powers Commissioner's Office (IPCO), formerly the Office of Surveillance Commisoners (OSC) and the Information Commissioner's Office (ICO).

1.2 In the document the Data Protection Legislation means the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) as amended, replaced or superseded from time to time. This definition includes any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then any successor legislation to the DPA or the GDPR, and all guidance, standards and codes of practice published by the ICO, or any replacement body, which relate to data protection.

1.3 The Data Protection Legislation, Human Rights Act 1998 (HRA), and the Regulation of Investigatory Powers Act 2000 (RIPA) together with published codes of practice, define what surveillance is lawful.

1.4 All Council surveillance must be lawful and approved by an appropriate officer, ie by an Authorising Officer for RIPA covert surveillance activities. The Council's remit is also ***restricted to conducting surveillance to prevent or detect crime and to prevent disorder for core functions,*** eg in order to support enforcement functions when there is no other alternative and not for 'ordinary functions' such as employment issues, eg the disciplining of an employee (please see paragraph 2.1 of this procedural guidance, below). Disciplining of employees is not a 'core function' (although related criminal investigations may be – in such cases seek guidance from the Solicitor for information governance).

1.5 Evidence obtained without appropriate authorisation is likely to be challenged in any subsequent legal proceedings, and may leave the Council open to criticism.

2 Scope of Procedural Guidance

2.1 Only core functions within Coventry City Council are authorised to use ***directed surveillance***, under RIPA, in order to prevent and detect criminal offences that are either punishable by a maximum term of at least 6 months' imprisonment OR criminal offences relating to the underage sale of alcohol, tobacco and e- cigerettes.

2.2 This procedural guidance covers directed surveillance for:

i) Core functions, eg enforcement activities undertaken by Trading Standards;
ii) Directed surveillance that is likely to result in obtaining private information about a person,

including the use of internet and social networking sites; and

iii) Use of Covert Human Intelligence Sources (CHIS).

3 Types of Surveillance

3.1 Surveillance takes many forms. It can include monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other activities and/or communications, including the use of internet and social networking sites. It can also include recording such observations and also surveillance by and/or with the assistance of appropriate surveillance devices. Surveillance can be **overt** or **covert.**

3.2 **Overt surveillance** is what is typically carried out by the Council. There will be nothing secretive, clandestine or hidden about it. In many cases, Council officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly (eg an environmental health officer inspecting food premises).

3.3 Surveillance may also be overt if the subject has been told it will be happening (eg where a noise maker has been warned that details will be recorded if the noise continues; or where an entertainment licence is issued subject to conditions and the licensee is told that officers may visit without notice or identify themselves to the owner/proprietor to check that license conditions are being met).

3.4 Such overt surveillance, which includes the open and transparent use of CCTV, does not normally require authorisation. However, if a camera is to be used for a specific purpose, such as prolonged surveillance on a particular individual, authorisation will be required. More information regarding the use of CCTV can be found in the Council's CCTV Code of Practice and Procedures Manual, a copy of which can be found at the following link (this document is in the process of being updated to reflect GDPR):

https://coventrycc.sharepoint.com/:w:/r/_layouts/15/WopiFrame.aspx?sourcedoc=%7B6A4BAE65-3271-41C4-9865-B3B71D759D6D%7D&file=CCTV%20Code%20of%20Practice%20and%20procedure%20manual.docx&action=default&DefaultItemOpen=1

3.5 **Covert surveillance** is intended not to alert the subject to the fact that they are being watched. The legislation also covers **'covert human intelligence sources'** (commonly referred to as CHIS – these are people who establish or maintain a relationship with someone in order to covertly obtain information without telling the subject that they are doing this).

3.6 Covert surveillance must be within the law and can only start after authorisation has been provided.

3.7 In terms of monitoring the use of Council ICT, it is important to recognise the important interplay and overlaps with the Council's information security polices and standards covering computers, internet, email and telephones etc.

3.8 Surveillance is **directed surveillance** if the following apply:

i) It is covert, but not intrusive surveillance;
ii) It is conducted for a specific investigation or operation;
iii) It is likely to result in the obtaining of ***private information*** about a person (whether or not a person has been specifically identified for the purposes of the investigation); and
iv) It is planned and conducted otherwise than as an immediate response to a situation, the nature of which is such that it would not be reasonably practicable for an authorisation (please see paragraph 6.1 (iii) of this procedural guidance, below for further guidance).

3.9 **Intrusive surveillance** is covert surveillance of activity taking place on residential premises or in a private vehicle, when the investigator is inside the building or vehicle, or if they are using a surveillance device. It also includes surveillance from outside if it consistently provides information of the same quality and detail as may be expected to be obtained from a device inside. **Local authorities are not permitted to conduct intrusive surveillance - to do so would be unlawful** and may result in the prosecution of individuals and civil claims including claims under the Human Rights Act 1998.

4 Types of Information

4.1 **Private information** includes any information relating to a person's private or family life. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in obtaining private information.

4.2 **Confidential or Privileged Information** is that which would normally attract an even higher expectation of privacy, eg information subject to legal privilege, confidential medical information etc. The probability of the Council undertaking an operation where there is likelihood that knowledge of confidential information will be acquired is extremely low. However, should such a situation arise, authorisation must be obtained from the Chief Executive Officer prior to the operation being undertaken.

5 Necessity and Proportionality

5.1 Authorising Officers have to be satisfied that there is a **necessity** to use covert surveillance in a proposed operation, ie there must be an identifiable offence to prevent or detect before an authorisation can be granted. For example, in relation to planning enforcement and noise nuisance there is no offence before service of an enforcement notice. This does not prevent the use of covert surveillance but such unauthorised activity should not be afforded the protection of RIPA.

5.2 Prior to an Authorising Officer granting an authorisation for directed surveillance, they must believe that the request is proportionate to what is sought to be achieved. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. No activity should be considered proportionate if the information which is sought could reasonably be obtained by less intrusive means. The following elements of proportionality should therefore be considered:

i) Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
ii) Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others and that where there might be intrusion on the subject and others such intrusion is proportionate to what is sought to be achieved;
iii) Considering whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
iv) Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

6 General Best Practice

6.1 The following procedural guidance should be considered as best working practice with regard to all applications for directed covert surveillance and/or use of a CHIS:

i) Applications should avoid any repetition of information or simply copying and pasting from previously authorised applications;
ii) Information contained in applications should be limited to that required – refer to section 5 of Home Office Code of Practice for Covert Surveillance and Property Interference, a copy of which can be found at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716458/CCS207_CCS0618781142-1_Covert_Surveillance___Property_Interference_Code_of_Practice_Web_Accessible.pdf ;
iii) Applications must be authorised by an Authorising Officer;
iv) Where other agencies will be involved in carrying out the surveillance, these agencies must be detailed in the application - the 'lead organisation' should raise the required application form;
v) Authorisations should not generally be sought for activities already authorised following an application by the same or a different public authority;
vi) **Oral authorisations are prohibited in all circumstances** (even in urgent situations). Local authorities no longer have the power to make oral authorisations under s43 (1A) RIPA, inserted by the Protection of Freedoms Act 2012.

7 Authorisation procedures

7.1 The Council's Senior Responsible Officer for RIPA Part II is responsible for:

i) The integrity of the Council's processes for managing directed covert surveillance and use of a CHIS;
ii) Supporting the Cabinet Member (Policing and Equalities) and the Audit and Procurement Committee in ensuring the Council's use of RIPA are compliant with Council procedural guidance and the law.

7.2 The practice of using a **vulnerable person as CHIS** rarely, if at all happens in the Council. However, if such a request arose authorisation must be sought from the Chief Executive Officer, or in their absence, their deputy.

7.3 If any person is unsure as to whether the activity they are proposing constitutes surveillance that requires authorisation, they should seek advice from an Authorising Officer or the Information Governance Team before commencing the activity.

7.4 It is vital that all reasonable alternative methods (such as test purchases, obtaining statements, interview, or changing methods of working or levels of security) are exhausted before covert surveillance is considered. The outcome of such considerations must be recorded and any application for covert surveillance must clearly demonstrate why alternative methods are inadequate or not appropriate.

7.5 The disciplining of an employee would typically fall under 'ordinary functions' of the Council and not 'core functions', eg an officer is suspected by their manager of failing to maintain accurate time recording sheets. The manager wishes to undertake covert surveillance of when the employee starts and finishes work. Such activity, even if it is likely to result in obtaining of private information, does not constitute directed surveillance under RIPA - it relates to carrying out ordinary functions (ie employment matters) which are common to both public and private sector. Activities of this nature are covered by the Data Protection Legislation and the Information Commissioner's Employment Practices Code. An exception may be where the employee's activities are suspected of being part of a criminal investigation, eg selling counterfeit goods while at work. Anyone considering covert surveillance of an

employee must seek guidance from the Council's Solicitor for information governance in order to ensure any activities remain lawful.

7.6 For any covert surveillance activities that are deemed **necessary**, the Authorising Officer granting the authorisation must believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. **The activity will not be proportionate if it is deemed to be excessive in the circumstances** of the case or if the information which is sought could reasonably be obtained by alternative and less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

7.7 All requests to conduct, extend or discontinue covert surveillance must be made on the appropriate forms available on the Information Governace Handbook.

7.8 All requests must be submitted to an Authorising Officer (a list of Authorising Officers can be found by using the link shown above) who will consider and either authorise or reject the application in writing. This will take place prior to covert surveillance commencing and also applies where contractors or outside agencies are employed to carry out covert surveillance on behalf of the Council.

7.9 **The Authorising Officer can only grant permission when they believe directed surveillance is necessary and proportionate**. No one else can grant, extend or discontinue authorisations - thus ensuring independence and consistency. Authorising Officers will ensure a review date is set at the same time as authorising an application. Where applications are rejected, the Authorising Officer will include reasons why. This may result in further work on the application or outright refusal for the operation to proceed (eg insufficient evidence that all other reasonable measures have been exhausted etc).

7.10 **The Council's use of directed surveillance is subject to judicial approval by the Coventry Magistrates' Court**. The date for commencement of the authorisation (and therefore the surveillance activity) is the date that judicial approval is obtained. The Authorising Officer and / or the the Council officer attending Court should take the original hardcopy authorisation and show this to the magistrates but retain the original to keep with the Authorising Officer's records. It is recommended that the Authorising Officer should attend the Magistrates Court rather or in addition to the Council officer making the application. The Authorising Officer **must** be in attendance in the event of any unusual authorisations including any which involve a CHIS.

7.11 Written authorisation for covert surveillance is valid for a maximum of three months. Written authorisation for a CHIS is valid for a maximum of twelve months. Both periods run from the date of the original authorisation or renewal.

7.12 Judicial approval may be renewed for a further three or twelve months for covert surveillance and a CHIS respectively. Renewal must take place prior to expiration and takes effect from the date authorisation would have ceased. The Authorising Officer must be satisfied that the activity is still necessary and proportionate.

7.13 The Authorising Officer must review all authorisations (including renewals) at least monthly (sooner if the circumstances of the case are such that a review is required).

7.14 All authorisations with judicial approval must be formally cancelled and not left to expire. The operative of the activity should notify the Authorising Officer if the activity is no longer necessary and proportionate and the authorisation should thereafter be cancelled and the activity cease immediately. The Authorising Officer should complete a cancellation form detailing the information obtained and whether or not the objectives were achieved.

7.15 Applications for Council **covert surveillance** must be **carefully planned** so that the necessary consultations about **risk assessment**, **insurance** and **health and safety** can be carried out, and the necessary provision made **before surveillance commences**.

7.16 Surveillance that is unforeseen / iunplanned and undertaken as an immediate response to a situation, which is not reasonably practicable to obtain authorisation, falls outside the definition of 'directed surveillance' - therefore, authorisation is not required.

7.17 **Surveillance equipment** can only be installed (**or a CHIS** used) after judicial approval has been obtained. Equipment will only be installed (or a CHIS used) in residential premises if a member of the public has requested help, has agreed to equipment being installed in order to assist the Council with an operation, or referred a complaint to the Council and investigation is only possible using covert surveillance techniques after all the following has been considered:

i) Sufficient **evidence** has been documented to warrant the exercise
ii) Surveillance is shown to be both the **least harmful** means of meeting that purpose and **proportionate** to what it seeks to achieve

NB: This does not apply where residents are asked to keep diary sheets recording incidents of noise nuisance.

7.18 There may be occasions where the Council needs to consider asking a member of the public to assist with an operation. Tasking a person to obtain information covertly may result in an authorisation of a CHIS being required, however this may not be true in all circumstances. **If the task does not require the member of the public to establish or maintain a relationship with another person in order for the Council to obtain the information, they will not be a CHIS.** For example:

> *The Council has received a number of complaints regarding fly tipping on land. While notices have been put up to warn the public that overt surveillance may take place, because of the location and technical limiting factors (eg inadequate or no power supply for the cameras and/or the field of view), the Council may approach a local resident to obtain approval to install a camera in their home looking out on the affected area. In addition to demonstrating the necessity and proportionality of such an application, the requester must address issues such as the security of both the equipment and recorded information, and take into account the risk of obtaining private information about persons who are not subjects of the surveillance. The resident in this instance is not a CHIS as they are not establishing or maintaining a relationship with another person in order for the Council to obtain information.*

7.19 **A person who** establishes**, maintains and uses a personal or other relationship for the covert purpose of obtaining information is a CHIS**. For example:

> *A local resident who provides information about miscreant neighbours may be a CHIS if he has acquired the information as an "insider", rather than by mere observation from behind his net curtains. He may be vulnerable to reprisals if and when the Council takes action, and there is a risk of the Council being found in breach of its duty of care to him.*

7.20 NB: Special rules apply **if a person under 18** is to be authorised as a CHIS (refer to Section 4 of the Covert Human Intelligence Sources Revised Code of Practice, dated August 2018, which can be found at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_da

ta/file/733220/20180802_CHIS_code_reformatted_for_publication__002_.pdf). No **person under 16** can be authorised as a CHIS to give information against their parents or any person having parental responsibility for them. A person under 18 can only be authorised to act as a CHIS for one month.

7.21 A **vulnerable individual** is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of themselves, or be unable to protect themselves against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases authorisation **must** be obtained from the Council's Chief Executive Officer, or the person acting in that capacity.

7.22 In authorising a CHIS, the Authorising Officer should ensure a risk assessment has been undertaken to safe guard the individual from exploitation and protect their safety and identity.

7.23 A central record of surveillance requests and authorisations for covert surveillance will be maintained by the Information Governance Team (IGT). Authorising Officers are required to maintain an electronic copy and the original hard copy for their records, and send electronic copies (electronic copies only) to IGT within three working days: to infogov@coventry.gov.uk. Reasons why any requests were denied and a note of any recorded material handed to third parties, eg the police, must also be maintained by the Information Governance Team.

7.24 **All records must be marked Official Sensitive**, in line with the Council's Standard for Information Classification and must be kept securely.

7.25 All records will be kept for a period of 3 years following the end of the authorisation.

7.26 Authorising Officers must keep a **register of all reviews of material recorded and collected** covertly.

7.27 Recordings must be on high quality media and identified uniquely. Authorising Officers must keep a register of all recordings (please see paragraph 10.2 of this procedural guidance).

8 Covert surveillance of Social Networking Sites (SNS)

8.1 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

8.2 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example).

8.3 Where privacy settings are available and not used, the information is therefore publicly available and may be considered “open source”; therefore an authorisation is not usually required. However privacy implications still apply. This is because although the information has no protection by way of privacy settings, the intention when making such information available was not for it to be used for a covert purpose (such as investigative activity). This is regardless of whether a user of SNS has sought to protect such information by restricting its access by activating privacy settings.

8.4 Repeat viewing of SNS may constitute directed surveillance on a case by case basis and this

should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council Officer or by a person acting on the Council's behalf (i.e. the activity is more than mere reading of the site's content).

8.5 It is not unlawful for a member of a Council Officer to set up a false identity. A false identity could be used for occasional viewing of information but it is inadvisable for the officer to set up a false identity for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. Officers should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person.

8.6 For more information, please refer to the specific Use of Social Media in Investigations Guidance.

9 Interception of Communications

9.1 Interception of Communications takes two forms:

i) the collection and monitoring of **communications data** (e.g. records of who contacted whom, when, from where and for how long);
ii) the interception of the **content** of the communications themselves.

9.2 It is a criminal offence to intercept the **content** of communications (whether by post, email or telephone) without lawful authority. The circumstances in which the Council can intercept the content are rare.

9.3 The Council may intercept the content of communications if one party to the communication has consented to the interception and the surveillance of the communication (eg a telephone call) has an authorisation as detailed at Section 7 of this procedural guidance.

9.4 The Council is also permitted to record calls made to its Contact Centre for the purpose of ensuring that staff comply with standard procedures when dealing with the public. The Council must notify callers that monitoring and recording may take place and explain the purpose concisely.

9.5 The Council can only apply to access communication data for for the prevention and detection of crime or prevention of disorder.

9.6 Access to communications data includes identifying:
i) the devices called from and to;
ii) location of communicating parties;
iii) nature and service being used;
iv) duration of the communication;
v) other details held by the Communications Service Provider (CSP) about the subscriber to the service (e.g. their address).

9.7 Access to communications must be authorised by an Authorising Officer.

10 Monitoring

10.1 To ensure that the Council is using its powers under RIPA consistently and in line with the

authority's procedural guidance, quarterly reports on its use will be presented to the Information Management Strategy Group and an annual report to the Cabinet Member (Policing & Equalities) and the Audit and Procurement Committee. They will also be responsible for endorsing the authority's procedural guidance at least once per year and ensuring it remains 'fit for purpose'. Neither the Cabinet Member nor the Audit and Procurement Committee will be involved in making decisions on specific investigations.

10.2 During a covert operation, **recordings and information collected must be stored and transported securely, i.e. in line with the protective marking of "Official" or "Official-Sensitive"**. It must be reviewed monthly (or sooner if required) and access to it restricted. Access will generally only be allowed to limited and prescribed parties, including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (except where disclosure would prejudice any criminal enquiries or proceedings or breach privacy laws, eg Data Protection Legislation). Recordings must be on high quality media and identified uniquely. Recordings should not be kept for any longer than needed. Authorising Officers must keep a register of all recordings in order to control the retention period before wiping or securely destroying when no longer needed (such as if they are not required for evidence or the court case / investigation the recording is required for is completed).

11 Acknowledgements

11.1 This document has drawn on the key areas within the Home Office Codes of Practice for 1) Covert Surveillance and Property Interference, Draft Revised Code of Practice, dated June 2018 (Code of Practice for Covert Surveillance) and 2) Covert Human Intelligence Sources, Revised Code of Practice, dated August 2018. Officers should refer to the codes for more detailed guidance if necessary. Please note that at the time of writing this procedural guidance the Home Office has closed a consultation in relation to revision of its codes of practice under Parts II and III of RIPA. The Code of Practice for Covert Surveillance is still in draft form. Feedback from the consultation is being analysed and the final Code of Practice for Covert Surveillance has not yet been published. This RIPA Procedural Guidance will be updated as and when the final version is published.

12 Notes

12.1 Enquiries regarding this document should be directed to the Information Governance Team at: infogov@coventry.gov.uk or phone: (024) 7683 3323.

13 Document Control: Version History

Version	Status	Date	Author	Summary of changes
1.0	Approved	September 2010	J Hutchings	Minor amendments from Technical review have been incorporated
2.0	Approved	October 2010	S Gilbert	Minor amendments to web links and contact addresses
2.1	Draft	April 2017	R Kotonya	Amendments from OSC Inspection recommendations and included covert surveillance of social media sites
3.0	Approved	May 2018	S Harriott	Minor amendments including reference to GDPR, how to deliver authorisations to InfoGov and hyperlink to separate Social Media in Investigations Guidance

Technical Review

Name	Role	Business Area
A Harwood	Trading Standards and Consumenr protection Manager	Place Directorate

Management Approval

Name	Role	Date
J Newman	Legal Services Manager and Acting Monitoring Officer	August 2018
Information Management Strategy Group	Information Governance	May 2018

Management Approval

Name	Organisational Department	Format
All	**Coventry City Council**	**PDF via intranet/IG Handbook**