WORCESTERSHIRE COUNTY COUNCIL

Covert Surveillance and Acquisition of Communications Data

PROCEDURE

1 INTRODUCTION

1.1 This Council is committed to working for the overall good of the people of Worcestershire, which will include carrying out appropriate investigationsinto allegations or concerns. Very occasionally, this will require us to gather information in respect of individuals who may be unaware of what we are doing (*eg*. for suspected offences) through covert surveillance or the acquisition of communications data. In doing so, we need to draw a fair balance between the public interest and the rights of individuals.

1.2 In order to achieve that balance, the Council wishes to take into account and comply with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Human Rights Act 1998. This Procedure sets out the Council's approach to covert surveillance and the acquisition of communications data issues falling within the framework of RIPA in order to ensure consistency, balance and fairness. This approach will provide additional protection and safeguards where these covert activities are likely to causeus to obtain what is called “private information” about individuals or wherewe go 'undercover' in certain circumstances. This Procedure also makes it clear to the public what checks and balances will apply.

2 SCOPE OF PROCEDURE

2.1 This Procedure applies to 3 areas of our information gathering (as defined in RIPA):

- "Directed Surveillance"
- The use of "Covert Human Intelligence Sources" (or “CHIS”)
- The acquisition of communications data

For the purposes of convenience in this Procedure, the first two areasabove can be referred to as “Covert Surveillance”.

2.2 Unless there is alternative legal authority, our approach to Covert Surveillance is to comply with this Procedure and RIPA, and also to have regard to the relevant statutory Codes of Practice.

3 COVERT SURVEILLANCE

3.1 "Directed surveillance" means surveillance which is:

- Covert (but not intrusive) *i.e.* calculated to ensure that persons who are subject to this surveillance are unaware that it is or may be taking place;
- For the purposes of a specific investigation or specific operation;
- Undertaken in a way which is likely to result in the obtaining of private information about any person. This includes informationabout any person's private or family life, including private or personal relationships with others;
- Not an immediate response to events where it would not bereasonably practicable to follow the formal procedures.

3.2 The use of Covert Human Intelligence Sources ("CHIS") means obtaining information through someone who:

- establishes or maintains a personal or other relationship withsomeone for the covert* purpose of using that relationship to obtain information or provide access to information to other persons (therelationship may involve communication online as well as in person). or
- covertly discloses information obtained by the use of such a relationship or as a consequence of its existence.

* *a relationship is only covert only if it is conducted in a manner, or the information disclosed, where one person in the relationship is unaware of its purpose.*

3.3 If the proposed actions do not fall within these definitions, or there is alternative legal authority for their use, then there is no requirement to follow this Procedure. Nothing in this Procedure permits the authorising of "Intrusive Surveillance" as defined in RIPA (*i.e.* in respect of anything takingplace on residential premises or in a private vehicle, involving the presence of an investigator on those premises/vehicle or carried outthrough a surveillance device).

3.4 From 1st November 2012 (under regulation 7A SI2010 / 521 as inserted by SI2012 / 1500) an officer of appropriate rank of a County or District Council has only been able to authorise Covert Surveillance if it is to prevent or detect conduct which constitutes a criminal offence which is either:

- ► punishable (whether on summary conviction or on indictment) by a maximum term of at least 6 months of imprisonment; or
- ► is an offence under any of sections 146, 147, 147A of the Licensing Act 2003 (sale of alcohol to children), or section 33 Children and Young Persons Act 1933 (sale oftobacco to children).

4 ACQUISITION OF COMMUNICATIONS DATA

4.1 Acquisition of Communications Data is also now permissible for a Local Authority under Part 4 of the Investigatory Powers Act 2016 which allows an authorised person to obtain communications data from Telecoms Services Operators (TSO's) or a Postal Service and places obligations on operators to make disclosures in certain circumstances. They do not authorise interception of communications during the course of transmission.

4.2 The definition of Communications Data is summarised below. It doesnot include the actual content of a communication, *i.e.*

- Traffic Data attached to a communication identifying any person or location to or from which the communication is transmitted; or data identifying apparatus through which a communication is transmitted.

- Information held by a TSO or Postal Service which relates to a person receiving a service.

Examples – Mobile phone bills; cookies; records of dates and times of communications and the location of that communication; the identity of theperson sending and receiving the communication.

4.3 Unless there is an alternative legal power enabling you to acquire communications data, you should follow the procedure set out in this Procedure, the Act and the relevant Code of Practice. Under this Procedure, there are two methods of acquiring communications data: Designated persons may either authorise the Local Authority to go and obtain communications in person from the Operator, under an Authorisation or, more usually, serve a Notice on the Postal Service or TSO requiring the provider to disclose the data. From 1st November 2012 both processes will require Judicial Approval by a Justice ofthe Peace (see paragraph 8). The Notice places a duty upon the service provider to comply as far as is reasonably practicable. If the operator does not already have the data in his possession, the notice may require him to obtain it. The notice may be enforced by civil proceedings for an injunction orother appropriate relief. The designated person must believe that it is necessary to obtain the communications data for the purpose of preventing or detecting crime or for preventing disorder.

4.4 The Home Office has issued a Code of Practice about the acquisition of communications data. The Code of Practice recommends the appointment of a Single Point of Contact (SPoC) within authorities. The Code of Practice also recommends the appointment of a Senior Responsible Officer (SRO) who is to be responsiblefor the integrity of the process in place within the public authority to acquire communications data. The SPoC deals with acquisition of communications data and all authorisations should be channelled from the Authorising Officerthrough the SRO to the SPoC. At this point the SRO will ensure the Authorising Officer makes available to the SPoC the information the SRO considers necessary to ensure the integrity and efficiency of any request for Communications Data. This should include information prepared by the Authorising Officer which will permit the authorisation to be made and allow any necessary cross-referencing.

The SPoC's appointment does not affect the procedures for covert surveillance.

4.5 There are times when an error may occur in the process of acquiring Communications Data. When this occurs the SRO should be informed, who will investigate and establish the facts surrounding the error who will, in turn,report the error to the IOCCO in written or electronic form within five workingdays of the discovery of the error.

5 CONSIDERATION BY AUTHORISING OFFICERS

5.1 The purpose of this Procedure is to ensure that potential interference withan individual's right to privacy is considered at a senior level to be justifiable and to provide the checks and balances and protection that flows from RIPPA for properly authorised actions. Once agreement has been received from the authorised officer, no RIPA activity can be undertaken unless and until that action has received Judicial Approval by a Justice of the Peace (see paragraph 8). The requirement for Judicial Approval does not alleviate the Authorising Officer from a level of scrutiny previously existed before November 2012 when Judicial Approval was not required.

It must be noted that where a person/organisation is acting under the Direction of the County Council and acting, essentially, as their agent then any actions which meet the definitions of directed surveillance must be dulyauthorised.

5.2 Covert Surveillance and acquisition of communications data within the scope of this Procedure needs to be properly authorised and recorded. An application for authorisation must be in writing and be authorised personally by a specified Senior Manager/postholder within each Directorate (called "Authorising Officers"). The list of Authorising Officers may be revised in writing by the relevant Chief Officer from time to time. The Authorising Officers may authorise covert surveillance and or acquisition of communications data. However, in the case of acquisition of communication data, the procedure must be channelled by the SPoC through the SRO as well as the Authorising Officer in all cases.

5.3 Applications to the Authorising Officer must use the relevant standard application form, and the Authorising Officer must also record any authorisation in writing by filling inthe appropriate details upon the application.

5.4 Authorising Officers have the responsibility for deciding whether to grant Support to an authorisation in accordance with this Procedure. Authorisation support will only be given where the Authorising Officer believes that the Covert Surveillance or acquisition of communications data is necessary and a proportionate response in all the circumstances, is a justifiable interferencewith an individual's Article 8 rights and meets the statutory criteria set out in Section 28 or 29 of RIPA 2000 (for covert surveillance) or Part 4 of IPA 2016 (for communications data). Due regard must be had to the relevant Code of Practice. The necessity and proportionality of the application will be considered further by the Justice of the Peace who will not approve the use of RIPA unless satisfied on all these counts.

5.5 An Authorising Officer must also take into account any 'secondary' or 'collateral' intrusion that may result from activity under an authorisation. Thisis the risk of intrusion into the privacy of persons not connected with the surveillance. Measures should be taken to minimise such intrusion, and the possibility of its occurrence should be a factor in the decision as to whether the surveillance is proportional. It must be noted that, because CHIS relates to the manipulation of a relationship and not, as with directed surveillance, the collection of private information, that officers must be aware that a CHIS could arise within an investigation whether or not intended by the Local Authority and its use must be approved accordingly.

5.6 Consideration will need to be given about the need for Directed Surveillance or CHIS authorisation when using the Internet/Social Media to gather information. It is unlikely that the use of search engines and accessing publicly available information on Facebook *etc*. will require authorisation. At the other end of the spectrum the use of covert communication by electronicmeans with a specific individual will almost certainly require authorisation. If information on social media is accessed regularly to ascertain a change in aperson's circumstances, or if a 'private' profile is accessed on Facebook *etc*. careful consideration will need to be given in each circumstance to decide ifauthorisation is required.

5.7 Material which is obtained through surveillance authorised under RIPA is admissible in criminal proceedings and any authorisation should also further consider the general admissibility of any evidence under section 78 of the Police and Criminal Evidence Act 1984.

5.8 In addition, for CHIS authorisation, satisfactory arrangements should be in place for managing the source as required by Section 29(5) of RIPA. Then, if the use of the CHIS is necessary, the Authorising Officer must believe that the use of a source is proportionate to the purpose of authorising the CHIS. The officer should balance the intrusiveness of the use of the source on the target and others who might be affected against the need for the source. Theuse of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

5.9 In general, the Authorising Officer or SPOC should not be directly involved in the investigation or operation in question.

5.10 Unless renewed or cancelled, written authorisations will cease to have effect after:

Directed Surveillance - 3 months
CHIS - 12 months (4 months for a juvenile source – until July 2018 this was 1 month)
Communications Data - 1 month

6. REVIEWS OF AUTHORISATIONS – DIRECTED SURVEILLANCE

6.1 The Authorising Officer should determine how often the authorisation should be reviewed. This needs to be as frequently as is necessary andpracticable but in any event not less than monthly during the life of the authorisation for Directed Surveillance.

6.2 The likelihood of obtaining confidential information or 'collateral' private information relating to someone other than thesubject will be borne in mind when setting the review period.

7. RENEWALS

7.1 Authorisations may be renewed for a further period of:

Directed Surveillance - 3 months
CHIS - 12 months (4 months for a juvenile source – until July 2018 this was 1 month)
Communications Data - see paragraph 7.5 below

provided an Authorising Officer is satisfied they continue to meet the criteria. The renewal must receive Judicial Approval - *but the Court will not play a part in the review process*. In relation to CHIS renewals should consider the use of, the tasks given to and the information obtained from the CHIS.

7.2 Authorisations can be renewed more than once.

7.3 Each review must be given Judicial Approval. The date of renewal must be considered in advance to ensure that the Court will be sitting on that date. If not an earlier application should be considered (see paragraph 8 for Judicial Approval).

7.4 Records of renewals are required to be retained (see paragraph 10 below).

8. JUDICIAL APPROVAL

The Application

8.1 From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 will commence. This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewalof an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he will issue an order approving the grant or renewal for the use of the technique as described in the application.

8.2 The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessityand proportionality, completing the RIPA authorisation/application form and seeking approval from an Authorising Officer will remain the same.

8.3 Following approval by the Authorising Officer/ the first stageof the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the Magistrates' Court to arrange a hearing.

8.4 The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. For communications data requests the IPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

8.5 The original RIPA / IPA authorisation or notice should be shown to the JP but willbe retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy.

8.6 In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Section 10).

8.7 Although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

8.8 The order section of the form will be completed by the JP and will be the official record of the JP's decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations/applications and renewalsand the local authority will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

The Hearing

8.9 The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

8.10 The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form.

8.11 Local authorities will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The local authority may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations or notices. This does not, however, remove or reduce in any way the duty of the Authorising Officer to determine whetherthe tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the Authorising Officer has considered and which are provided to the JP to make the case.

8.12 Officers presenting the matter, if not holding rights of audience, will need to be authorised under section 223 of the Local Government Act 1972. The skills of a legally trained personnel may not necessarily be required to makethe case to the JP which would likely, unnecessarily, increase the costs of the local authority's applications.

9. CANCELLATION

9.1 The Authorising Officer must cancel the authorisation if satisfied that the activity no longer meets the criteria upon which it was or could have been authorised or satisfactory arrangements for the source's case no longer exist. Where necessary, the safety and welfare of the CHIS should be considered after cancellation. At that point all directed surveillance must cease.

9.2 Authorisation should be formally cancelled upon completion of the operation where it is no longer needed.

9.3 Judicial approval is not required for a cancellation.

9.4 Records of cancellation are required to be kept (see paragraph 7 above).

10. RECORDS

10.1 A centrally retrievable record of all authorisations, notices, Judicial Approvals *etc.* under this Procedure will be held by the Head of Legal and Democratic Services. This record must be regularly updated whenever an authorisation is granted, renewed or cancelled. This will be achieved by the Authorising Officer forwarding a copy of the approved application, Judicial Approval renewal or cancellation to the Head of Legal Services for the centrally retrievable record which will be retained for at least 5 years.

10.2 It is the responsibility of the relevant Authorising Officer to (a) forward all relevant information and documentation in each case to the Head of Legal and Democratic Services, as soon as they have been executed, and b) to have systems in place to ensure compliance with this procedure, RIPA, IPA together with any relevant Regulations and or Code of Practice.

10.3 The operational Directorate concerned will retain the original forms of authority, renewal, cancellation or Judicial Approval and in addition will hold:

- Any supplementary documentation given to or by the Authorising Officer;
- Any separate notification of approval given by the Authorising Officer;
- A record of the period over which surveillance has taken place;
- The frequency of reviews decided by the Authorising Officer in the case;
- A record of the result of each such review;
- Any supporting documentation provided for a renewal of authorisation;
- The date and time of any instruction given by the Authorising Officer Records of the use of a particular CHIS, any risk assessment in relation to the source, the value of the source, the circumstances inwhich tasks were given to the source and any other record requiredby Regulations.

11. CONFIDENTIAL INFORMATION

11.1 Although RIPA does not provide any special protection for confidential information, particular care should be taken where confidential information (*i.e.* confidential personal information, confidential journalistic material, or information subject to legal privilege) might be obtained. Further guidanceis available in the relevant Code of Practice.

11.2 Where it is likely that such confidential information will be acquired through Covert Surveillance, the Surveillance must be authorised by the Chief Executive (or another Chief Officer in his absence). In general, legal advice should be obtained prior to Covert Surveillance that is likely to acquire confidential information.

12 DATA SAFEGUARDS

12.1 The Council must ensure that any information it obtains through surveillance is handled in accordance with the safeguards the Council has put in place, any relevant frameworks (such as data protection), and the Home Office Codes.

12.2 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes.

12.3 As set in this document and within the Home Office Codes, regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained.

12.4 All information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss.

12.5 Information obtained through surveillance should be held separately so that it is easily identifiable, scheduled for deletion or destruction in line with the Council's Retention Policy, and securely destroyed as soon as they are no longer needed for the authorised purpose. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

13 **GENERAL**

13.1 This Procedure is a public document and will be available for public inspection at County Hall and upon the Council's internet website. Copies of this Procedure will be held in all Directorates and made accessible to allAuthorising Officers and those who may need to seek authorisation. The Procedure will be reviewed and updated from time to time.

13.2 Oversight of RIPA Covert Surveillance procedures is provided by the Investigatory Powers Commissioner's Office who may be contacted atPO Box 29105, London SW1V 1ZU, info@ipco.gsi.gov.uk .

13.3 Complaints concerning the way in which the Council has operated thisPolicy may be made to the Chief Executive at County Hall, Spetchley, Road, Worcester WR5 2NP.