- 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*

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 and RIPA. 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

4.5 The standard forms for authorisation relating to communications data can be found on the following link: https://www.gov.uk/government/collections/ripa-forms--2
Alternatively, copies can be found within this Manual at Section 10.

4.6 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 thePeace (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.

5.10 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 tha Tc 0.074Tw 5.094 0 Td[(a)]TJ-7.204)-0r9.199Tc(i)-7.19 0.004bouw ([t)3s)-)Tj0

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

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

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 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 Po80.003 Tc -01.14-10.5 (t)-7.2 (ec)-4 (t)-7.3 7 (pr)-4eno (ak)0

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