MID DEVON DISTRICT COUNCIL

RIPA POLICY

USE OF DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES REGULATION OF INVESTIGATORY POWERS ACT 2000

1.0 INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert investigative techniques by public authorities. It provides for the application for and granting of authorisations for those techniques covered by the Act.

1.2 Article 8 of the European Convention on Human Rights provides a right to private and family life. This is not an absolute right; it may be infringed in certain circumstances. The RIPA is designed to provide a statutory regulatory framework, which will meet the requirements of the European Convention on Human Rights.

2.0 PURPOSE

The purpose of this policy is to ensure that the Council complies with the requirement of RIPA and that appropriate authorisations are given for covert surveillance, the use of covert human intelligence sources and the acquisition and disclosure of communications data.

3.0 ASSOCIATED DOCUMENTS

3.1 Background documents

Report to the Council's Policy and Development Committee –15.02.01

3.2 Statutes and Statutory Instruments

(a) Regulation of Investigatory Powers Act 2000
(b) Human Rights Act 1998
(c) Police and Criminal Evidence Act 1984
(d) Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
(e) Protection of Freedoms Act 2012

3.3 Guidance

(a) Explanatory Notes to RIPA
(b) Code of Practice for covert surveillance and property interference
(c) Code of Practice for the use of covert human intelligence sources
(d) Code of Practice for the acquisition and disclosure of communications data
(e) Home Office Web Site https://www.gov.uk/guidance/surveillance-and-counter-terrorism#local-authority-use-of-ripa

All Codes of Practice are available on the Home Office Web Site https://www.gov.uk/government/collections/ripa-codes

4.0 SCOPE

The Act provides a regime of primary legislation and Codes of Practice, which divide covert investigation techniques into categories distinguished to an extent by the degree of intrusion involved. This procedure applies to all investigation and surveillance that may be subject of an authorisation under RIPA.

4.1 The Act covers the following investigatory powers:

(1) Part I (Chapter II) - the acquisition of communications related data e.g. telephone billing data

(2) Part II deals with:

- intrusive surveillance on residential premises or in private vehicles
- directed surveillance i.e. covert surveillance in the course of a specific operation
- the use of covert human intelligence sources e.g. agents, informants, undercover officers

(3) Part III - deals with the power to seize electronic keys giving access to encrypted computer material

(4) Part IV - provides for scrutiny, complaint procedures and codes of practice

4.2 This policy document relates to the **use of directed surveillance** and **covert human intelligence sources**. It does not cover the acquisition and disclosure of communications data as it is not anticipated that this power will be used by the Council. If authorisation is however sought for this type of activity, guidance must be sought from Legal Services before any operation or investigation is undertaken. It does not cover intrusive surveillance because local authorities are not allowed to do this. Intrusive surveillance is the covert (i.e. secret) surveillance of anything taking place in residential premises or a private car and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

4.3 RIPA sets out the purposes for which each of these powers may be used, the Agencies and authorities that can use them and who should authorise the use. Authorisation under RIPA gives lawful authority for the use of these methods of obtaining information provided there is compliance with the statutory requirements and procedures. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the Human Rights Act 1998.

4.4 For district councils, the Act does not allow directed surveillance or CHIS at all except for the purpose of preventing or detecting crime or preventing disorder. For example, this means that you cannot carry out these covert activities prior to the service of a

statutory notice, unless you believe an offence may have been committed, may be about to be committed, or there could be public disorder. Your only option in other cases will be to carry out overt – open, non-secretive – surveillance.

4.5 Services likely to conduct investigations covered by this Act are Planning, Environmental Health, Housing and Audit. However, any officer of the Council if he or she conducts an investigation using methods or techniques covered by this Act is required to seek the necessary authorisation, provided always that the purpose of the investigation is the one which the Act says can justify covered surveillance – see 4.4 above.

5.0 ACTIVITY REQUIRING AUTHORISATION

5.1 The following types of activity will require authorisation:

- directed surveillance
- the conduct and use of covert human intelligence sources
- obtaining communications data

5.2 Directed surveillance is, in essence, any activity undertaken covertly for the purpose of a specific investigation in such a way that is likely to result in obtaining information about a person's private life.

5.3 A covert human intelligence sources (CHIS) is effectively an inside informant or undercover officer, i.e. someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator. Council officers may act as CHIS when undertaking social media research. For a more detailed definition see section 26 of the Act.

6.0 APPLYING FOR AUTHORISATIONS

6.1 Subject to the provisions of paragraphs 6.3 and 8.7 the Directors are authorising officers for the Council. In the absence of the nominated authorising officer, applications for authorisation should be submitted to Chief Executive who also has the delegated authority to issue authorisations in relation to any service of the Council. Authorising officers may authorise for any service within the Council.

6.2 Any officer intending to use directed surveillance or a CHIS shall apply for authorisation from the authorising officer or in their absence from the Chief Executive as Head of Paid Service or in his absence a Director who is an authorising officer by completing the appropriate application form as set out at **Appendix DS/1 or CHIS/1**.

6.3 Special care needs to be taken with **confidential personal information**. This is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. This also includes legally privileged material, journalistic materials and information given to a Member of Parliament. Owing to the very sensitive nature of this type of information authorisations potentially involving confidential personal

information must always be made by the **Chief Executive** or in his/her absence the person who is formally nominated to act as the Chief Executive.

6.4 When completing the application always include a full account of the steps to be taken in the investigation which require authorisation.

7.0 GRANTING OF AUTHORISATIONS FOR DIRECTED SURVEILLANCE

7.1 Section 28 provides that a person shall not grant authorisation for *directed surveillance* unless he believes that the authorisation is necessary on one of the statutory grounds and the authorised surveillance is proportionate to what is sought to be achieved by it. The applicant and the authorising officer must both consider whether it is necessary to use covert surveillance in the investigation. From 5 January 2004, only one ground applied to district councils and it is therefore the only one which can be used to justify an authorisation.

That ground is

- for the purpose of preventing or detecting crime or of preventing disorder

7.2 The authorising officer in determining whether the surveillance is proportionate will give particular consideration to any collateral intrusion on or interference with the privacy of persons other than the subject(s) of the surveillance. The Home Office Code of Practice has the following to say on the issue of proportionality:

> "**4.5** if the activities are deemed necessary on…the statutory grounds, the person granting the authorisation… must also believe that they are proportionate to what is sought to be achieved by carrying them out. 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 and operational terms.
> 4.65 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. 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.." Home Office Code of Practice on Covert Surveillance and Property Interference.

A useful prompt is to ask yourself " Is there any other way of obtaining the evidence?". There is a need to consider the following:
(i) Whether the use of covert surveillance is proportionate to the mischief being investigated, and
(ii) Whether it is proportionate to the likely intrusion on the target and others, and
(iii) Whether all other reasonable means of acquiring the evidence have been considered.
(iv) What other methods had been considered and why they were not implemented.

7.3 Authorisations must be given in writing. It is possible that authorising officers may face cross-examination in court about the authorisation some time after it is granted and memories fade. It is therefore important that a full written record of what you are

being asked to authorise appears on the application form. If in doubt ask for more detail.

7.4 Authorising officers should not be responsible for authorising their own activities.

7.5 All RIPA authorisations must be approved by a Magistrate before an authorisation becomes effective, directed surveillance is undertaken, communications data is obtained or an application is made for a Covert Human Intelligent Source. Directed surveillance can only be authorised where the following conditions apply;

(1) The first condition is that the authorisation under section 28 is for the purpose of preventing or detecting conduct which—

(a) constitutes one or more criminal offences, or
(b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

(2) The second condition is that the criminal offence or one of the criminal offences referred to in the first condition is or would be—

(a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment or

are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

7.6 **Duration of Authorisations and Reviews**

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. So 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 **Appendix DS/2** and a copy filed on the central record of authorisations. If the surveillance provides access to confidential information or involves collateral intrusion more frequent reviews will be required . The Authorising Officer should determine how often a review should take place.

7.7 **Renewals**

7.7.1 While an authorisation is still effective 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.

7.7.2 Applications requesting renewal of an authorisation are to be made on the appropriate form as set out at **Appendix DS/3** and submitted to the authorising officer. The renewal must be granted before the original authorisation ceases to have effect.

7.7.3 Applications for renewal will record:

- whether this is the first renewal, if not, every occasion on which the authorisation has previously been renewed

- 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.

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

7.8 **Cancellations**

The person who granted or last renewed the authorisation **MUST** cancel it if he is satisfied that the directed surveillance no longer meets the criteria for authorisation. Requests for cancellation will be made on the appropriate form as set out at **Appendix DS/4** 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.

8.0 GRANTING OF AUTHORISATION FOR THE CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

8.1 The same requirements of necessity and proportionality exist for the granting of these authorisations as are set down for directed surveillance.

8.2 Additionally the authorising officer shall not grant an authorisation unless he /she believes that arrangements exist for the source's case which satisfy the following requirements:

- there will at all times be an officer with day to day responsibility for dealing with the source 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 source will not be available to persons except to the extent that there is a need for access to them to be made available

8.3 Similarly before authorising 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 source seeks to achieve, taking into account the likely degree of intrusion into privacy of those potentially effected for the privacy of persons other than those who are directly the subjects of the operation or investigation. Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

8.4 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.

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

8.6 Additionally, the authorising officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

8.7 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 a juvenile or vulnerable CHIS.

8.8 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. However it is recognised that this will not always be possible especially in the case of small departments. Authorisations must be approved by a Magistrate, see paragraph 7.5. The Solicitor employed by the Council will arrange the appointment before the Magistrate(s) and explain the procedure to the Authorising Officer. The Solicitor employed by the Council and the Authorising Officer will be required to attend before the Magistrate(s) to seek the Magistrate's approval to the authorisation.

8.9 An application for authorisation for the use or conduct of a source will be made on the appropriate form as set out at **Appendix CHIS/1** 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 on 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 source 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.

8.10 **Duration of Authorisations**

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 in the case of a juvenile CHIS which has a duration of one month. Oral authorisations will, unless renewed, last 72 hours.

8.11 **Renewals**

As with authorisations for directed surveillance authorisations for the conduct and use of covert human intelligence sources 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. Applications for renewal must be made on the appropriate form as set out at **Appendix CHIS/3** and submitted to the authorising officer. However an application for renewal should not be made until shortly before the authorisation period is coming to an end.

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

8.13 When covert human intelligence source authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

8.13 **Reviews**

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on **Appendix CHIS/2** and a copy filed on the central record of authorisations. 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.

8.14 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

8.15 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. When covert human intelligence source authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

8.16 **Cancellations**

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

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

8.17 Requests for cancellation will be made on the appropriate form as set out at **Appendix CHIS/4** 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.

8.18 **Management Responsibility**

The day to day contact between the Council and the source is to be conducted by the handler, who will usually be an officer below the rank of the authorising officer. No vulnerable person or young person under the age of 18 should be used as a source.

8.19 **Security and Welfare**

Account must be taken of the security and welfare of the source. The authorising officer prior to granting authorisation should ensure that an assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the target know the role of the

8.20 **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 source should be subject to special authorisation. In these cases the proposed course of conduct must be referred to the Head of Paid Service or (in his absence) a Director for a decision as to whether authorisation may be granted.

8.21 **Monitoring of personal information online**

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

9.0 **MAINTENANCE OF RECORDS**

9.1 Each Service shall keep in a dedicated place

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

9.2 The records will be confidential and will be retained for a period of 3 years from the ending of the authorisation.

9.3 Each authorising officer shall send original copies of all applications/authorisations, reviews, renewals and cancellations to the RIPA Co-ordinating Officer when drafted who will maintain a central record of all authorisations. The report will include details of the level of compliance with the requirements for authorisation.

9.4 Authorising officers will ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

9.5 Where material is obtained by surveillance which is wholly unrelated to a criminal or other investigation or to the person subject of the surveillance and 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.

10.0 AWARENESS OF THE CONTENTS OF THE ACT AND TRAINING

It shall be the responsibility of each Service Manager or other Authorised Officer to ensure that all staff involved or likely to be involved in investigations receive a copy of the training document, and are aware of the requirements and implications of the Act. It shall be the responsibility of the Senior Responsible Officer with the assistance of the RIPA Co-ordinating Officer to ensure that all relevant officers have received appropriate training and are aware of the requirements and implications of the Act.

11.0 CODES OF PRACTICE

A copy of each Code of Practice shall be kept in the reception area and be available to members of the public during usual working hours.

12.0 SENIOR RESPONSIBLE OFFICER AND RIPA CO-ORDINATING OFFICER

The Monitoring Officer is the Senior Responsible Officer for the Council whose role is:

(i) to be responsible for RIPA training throughout the Council;
(ii) to ensure that all authorising officers are of an appropriate standard; and
(iii) to be responsible for heightening RIPA awareness throughout the Council.

The Senior Responsible Officer will nominate a Solicitor employed by the Council is the RIPA Co-ordinating Officer for the Council whose role is:

(i) to collate all original applications/authorisations, reviews, renewals and cancellations;

(ii) to keep the Central Record of Authorisations; and

(iii) to notify the Leader of the Council of the receipt of authorisations from Authorising Officers.

13.0 MEMBER INVOLVEMENT

Members of the Community Wellbeing PDG should review this policy annually to ensure that it remains fit for purpose. Cabinet will consider reports from the OSC. The Cabinet should also consider reports on the use of the powers under the Act on a regular basis which shall be at least every year to ensure that it is being used consistently with this policy. Members of the Council will not however be involved in making decisions on specific authorisations.

Inventory of Surveillance Equipment held by MDDC

None as at 1 August 2019

Standard Operating Procedure for use of Surveillance Equipment

1. The Council operates the surveillance equipment (Equipment) as set out in the Inventory.
2. The Equipment should be stored, when not in use, in a locked cabinet under the control of the Senior Responsible Officer .
3. Any Officer of the Council considering using the Equipment for covert surveillance in a public place must make a written request to the Senior Responsible Officeror the 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.
4. 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 and/or the RIPA Co-ordinating Officer.

Mid Devon District Council

Annex 1 to the Council's RIPA Policy

Open Source Internet Research and RIPA

Background

The internet enables access to a vast amount of information which can be useful to the Council in carrying out its statutory functions as well as engaging with the public.

Open Source Internet Research (OSIR) is the name given to viewing, collecting processing and analysing publicly available personal information stored on the internet including on Social Media. Social Media in this Annex means social networking websites such as Twitter, Facebook, YouTube, content communities and blogs.

This Annex to the Council's RIPA Policy covers the use of OSIR in investigations. Advice should be taken from HR should an investigation involve a member of staff. Where officers are carrying out OSIR they must be aware of the Council's RIPA Policy and the information contained in this annex.

Using OSIR raises the issue of whether RIPA authorisation must be obtained. This policy indicates when RIPA authorisation should be obtained. If RIPA authorisation is required the Council's RIPA policy must be complied with.

Investigatory techniques governed by RIPA

RIPA regulates the use of covert investigative techniques such as directed surveillance and CHIS, which are described in more detail in the Council's RIPA policy. RIPA requires that the use of these techniques must be authorised and judicial approved. The Council's RIPA policy sets out the process to obtain such authorisation and judicial approval.

Categories of using OSIR

This Annex focuses on four broad categories of OSIR to give an indication when RIPA authorisation is required.

Category 1

Category 1 is viewing publicly available postings or websites where the person viewing does not have to register a profile answer a question or enter correspondence in order to view e.g. a trader's website. There must be a low expectation of privacy and no RIPA authorisation would normally be required to view or record these pages.

However, repeated visits over time which amount to monitoring an individual's on line presence will require RIPA authorisation. How a person runs his/her business can be private information even if they do so in the public domain. No monitoring of a person's on line presence can take place without RIPA authorisation. The exception to this is where prior notification is given to the person that the Council is monitoring that person's on line presence. This would then be overt monitoring and would not require RIPA authorisation.

All visits to such websites for the purposes of any investigations must be recorded and be available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer-see Part 12 of the RIPA Policy for more details about these roles.

Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to. Using test purchases in an investigation does not necessarily trigger the need for RIPA authorisation but in each case advice must be sought beforehand from the Co-ordinating Officer

Category 2

Category 2 is viewing postings on social networks where the viewer has to register a profile but there is not otherwise a restriction on access. This would include Facebook where there is no need to be accepted as a "friend" to view. E.g. a trader has a "shop window" on Facebook advertising business and products

There are differences between this and Category 1. The person who posts information or runs such a website may reasonably expect viewers to work within the terms and conditions of the website. Viewings using a fictitious

identity or “covert account” require RIPA authorisation. No such viewings may take place without RIPA authorisation.

Viewing conducted in an overt manner do not require RIPA authorisation. Viewings can be conducted in an overt manner via an account profile which uses the officer’s correct name and email address (which should be a middevon.gov.uk).

All viewings for investigations regardless of whether RIPA authorised or not will need to be recorded and available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer. Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to.

Category 3

Category 3 is viewing postings on social networks which require a “friend” or similar status to view. Viewings using a covert account or fictitious identity will require RIPA authorisation. No such viewings may take place without RIPA authorisation.

Viewing conducted by using the officer’s correct name and email address (which should be a middevon.gov.uk) to acquire “friend status” may still require a RIPA authorisation. It may be that such a status is given by default on the part of the person posting or website owner. Officers will need to be sure that their access is being granted as a representative of the Council.

If officers are not sure that access is being granted to the officer as a representative of the Council then RIPA authorisation must be obtained before such viewings take place.

All viewings for investigations regardless of whether RIPA authorised or not will need to be recorded and available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer. Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to.

Category 4

Category 4 is the use of sophisticated OSIR tools and techniques including active search, reverse engineering and/or tools or filters etc to obtain information on an individual on the wider web. The use of such tools is likely to involve monitoring an individual and RIPA authorisation must be obtained before use

Covert Facebook accounts and similar covert social media accounts

Use of such covert accounts requires RIPA authorisation. Even with RIPA authorisation use of such covert accounts may be judged to be unlawful because the companies' terms and conditions do not allow such covert accounts. RIPA authorisation is not in itself sufficient to permit in law breaching a company's terms and conditions. Advice must be sought from the Co-ordinating Officer.

Procedures/instructions

Senior managers may issue instructions and procedure notes to provide further safeguards in using OSIR