



East  
Northamptonshire  
Council

## Policy and Resources Committee – 12 September 2011

### Covert Surveillance Policy - Regulation of Investigatory Powers Act 2000

**Purpose of report** To make changes to the council's Covert Surveillance Policy in the light of (a) the inspection report issued at the beginning of June by the Office of Surveillance Commissioners and (b) the effect of the Protection of Freedoms Act 2011, and (c) amendments to the officer delegation scheme approved in July 2011.

#### Attachment(s)

Appendix A – Revised Covert Surveillance Policy  
Appendix B – Member Briefing

#### 1.0 Introduction

- 1.1 Members will recall – from the Briefing issued in April 2011 - that the government was concerned about the misuse, by local authorities, of the covert surveillance provisions in the Regulation of Investigatory Powers Act 2000 and introduced changes in the Protection of Freedoms Bill. For the benefit of members not in office in April 2011, the briefing is attached as Appendix B.
- 1.2 The Bill has now been enacted. The effect of the new provisions is likely to be a cessation of the use, by the council, of the RIPA provisions. This is because every authorisation will now need to be agreed by a magistrates court and authorisations are only likely to be agreed if the offence will attract a prison sentence of six months or more. Whilst fraud benefits cases may, in certain circumstances, result in a prison sentence exceeding this period, covert surveillance operations have been carried out in partnership with the Department of Work and Pensions (DWP), and it is possible that the provisions will still be used by that government department, thus obviating the need for an authorisation sought by this council. Overt surveillance methods or alternative actions will be required for other activities where RIPA may previously have been used.
- 1.3 An inspection was undertaken by an inspector from the Office of Surveillance Commissioners (OSC) on 2 June this year (see section 2) One of the recommendations he made was that the council amend, slightly, its covert surveillance policy, even though the prospect of using the RIPA provisions in the future appears to be limited or unlikely.

#### 2.0 OSC Inspection

- 2.1 The Inspector's report was accompanied by a covering letter from the Chief Surveillance Commissioner, who commented:-

*"I am pleased to see that all the recommendations made following the last inspection 3 years ago have been discharged. You now have a well-oiled RIPA machine ready for use on the rare occasions when this is necessary. Your officers have a thorough understanding of what is expected and a level-headed and confident approach. I commend all involved".*

- 2.2 The Inspector made several recommendations, which are being implemented. In relation to the current policy, the Inspector stated that *"It is concise yet comprehensive and if read with care, tells an officer of the council all he needs to know on considering whether to make an application under RIPA"*. However three minor suggestions were made to improve it, and these are summarised in paragraph 2.3 below.

### 2.3 **Suggested changes to policy – Inspector’s report**

- Paragraph 2 – the discussion of *proportionality* needs to be replaced by the current, more helpful, revised Home Office Code of Practice.
- The description of CHIS (Covert Human Intelligence Sources) needs to have a provision that before using, the advice of the Solicitor to the Council should be sought. This council has never used a CHIS.
- The delegation to the Chief Executive in paragraph 10.3 to consult the Leader (or Deputy Leader) in cases where a juvenile or vulnerable person is being considered as a CHIS is not acceptable to the Inspector, who states “Such a decision is the non-delegable responsibility of the Chief Executive. Furthermore, the General Best Practice section of the Home Office Code of Practice states “They (elected members) should not be involved in making decisions on specific authorisations”. However remote the possibility of the council ever using a CHIS, this policy should be strictly adhered to, not least because of the serious security and safety issues surrounding CHIS’s.”

All changes as a result of the Inspector’s recommendations are shown in **red**.

### 2.4 **Other changes**

Changes as a result of the Protection of Freedoms Act 2011 are shown in **green**, and those as a result of changes to the delegation scheme are depicted in **purple**.

## 3.0 **Financial implications**

- 3.1 There are no significant financial implications. Clearly, however, if there is still some use of RIPA provisions in the future, there will be resource implications involved in seeking a magistrate’s consent to an authorisation.

## 4.0 **Legal implications**

- 4.1 The council has an obligation to follow the requirements of the Protection of Freedoms Act and obtain the consent of magistrates to any authorisation under RIPA.

## 5.0 **Risk implications**

- 5.1 There are no risk implications arising from this report.

## 6.0 **Equality and Diversity Implications**

- 6.1 There are no equality or diversity implications.

## 7.0 **Recommendation**

- 7.1 It is recommended that the revised Covert Surveillance Policy as set out in Appendix A be approved.

<b>Legal</b>	Power: Regulation of Investigatory Powers Act 2000; Protection of Freedoms Act 2011				
	Other considerations:				
<b>Background Papers:</b> Previous policy					
<b>Person Originating Report:</b> Keith Osborne, Democratic Services Manager 01832 742113					
<b>Date:</b> 28 June 2011					
<b>CFO</b>		<b>MO</b>		<b>CX</b>	

(Committee Report Normal Rev. 22)



**East Northamptonshire Council**

**Corporate Covert Surveillance Policy**  
September 2011

**DRAFT**

**If you would like to receive this publication in an alternative format (large print, tape format or other languages) please contact us on 01832 742000**

## Document Version Control

<b>Author (Post holder title)</b>	Democratic Services Manager
<b>Type of document (strategy/policy/procedure)</b>	Policy
<b>Version Number</b>	0.1/1
<b>Document File Name</b>	
<b>Issue date</b>	September 2011
<b>Approval date and by who (SMT / committee)</b>	
<b>Document held by (name/section)</b>	
<b>For internal publication only or external also?</b>	internal and external
<b>Document stored on Council website or Eunice?</b>	Eunice / Website
<b>Next review date</b>	2014 (if use is made of the RIPA provisions)

## Change History

Issue	Date	Comments
0.1	June 2011	Amendments to take account of the OSC Inspector's report; change in delegation scheme and change in legislation

*NB: Draft versions 0.1 - final published versions 1.0*

## Consultees

Internal	External
Heads of Service/affected staff	
CMT	
Neil Pritchard	

## Distribution List

Internal	External
All users or potential users of RIPA powers	

## Links to other documents

Document	Link
Data Protection Policy	
Enforcement Policies	

## Additional Comments to note

The reasons for updating the Policy are –

- the feedback received from the RIPA Inspection.
- The implications of the Freedom Act
- The change to the officer delegation

## Contents

	Page
1.0 Introduction	4
2.0 Interpretation	5
3.0 Pre surveillance visit and planning process	7
4.0 Unforeseen circumstances	7
5.0 Authorisation Procedures	7
6.0 Review of Authorisations	9
7.0 Review of Authorisations	9
8.0 Changes in Circumstance	9
9.0 Cancellation of Surveillance	9
10.0 Covert Human Intelligence Sources (CHIS)	9
11.0 Record of authorisations	10
12.0 Quality Assurance	11
13.0 Retention of material and security	11
14.0 Complaints procedure	11
<b>Annexe:</b> Authorised Officers	12

## 1.0 Introduction

- 1.1 The purpose of this policy is to ensure that the investigatory powers given to the Council under the Regulation of Investigatory Powers Act 2000 are used strictly in accordance with the Human Rights Act. The policy contributes to the following corporate outcomes:
- Effective partnership working (government departments and magistrates)
  - Effective management
  - Councillors and staff with the right knowledge, skills and behaviours.
- 1.2 Article 8 of the Human Rights Act protects an individual's rights to privacy. If there has been an intrusion into an individual's rights it must be clearly shown this was necessary to prevent or detect crime. Article 6 provides for the right to a fair trial, and evidence must have been gathered in accordance with the law.
- 1.3 Covert surveillance (which for the purpose of this policy includes accessing communications data) should not be undertaken unless it is necessary and proportionate to the alleged offence and been authorised by the appropriate officer.
- 1.4 An authorisation made by an officer named in the **Annexe to this policy and approved by a Magistrates Court** provides lawful authority for the Council to carry out covert surveillance **only for the prevention or detection of crime** but it is considered to be a power of last resort and to be used only after all other avenues have been explored
- 1.5 Covert surveillance falls into two categories, *directed* and *intrusive* surveillance. Intrusive surveillance is **not** available to local authorities and such use would be **ultra vires**.
- 1.6 This policy applies to *Directed Surveillance* and the use of *Covert Human Intelligence Sources* (within this policy collectively referred to as surveillance). However, CHIS will **not** be used in benefit investigations. Whilst it is unlikely that other Service areas will use them, this Policy highlights – in Section 10, the essential provisions which need to be observed.
- 1.7 The Council will only use surveillance where it judges such use to be proportionate (see box on page 6.).
- 1.8 Before authorising surveillance, authorising officers will take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion). Measures will be taken wherever practicable to avoid collateral intrusion.
- 1.9 In relation to benefit fraud, this policy must be read in conjunction with benefit fraud circular F4/2003. In all covert surveillance cases, the policy must be read in conjunction with the Home Office Code of Practice (a copy of which accompanies this Policy).
- 1.10 This policy together with the Home Office Code of Practice is available for public inspection in the Reception areas at East Northamptonshire House, Thrapston, The

Rushden Centre, and the TIC, Oundle, and can be accessed on the Council's website by using the link - <http://www.east-northamptonshire.gov.uk/pp/silver/viewsilver.asp?id=2264>.

## 2.0 Interpretation

2.1 For the purpose of this Policy:

**Authorising officer** means:

An officer who is designated as an officer responsible for authorising surveillance within the meaning of the Act.

**The Act** means:

The Regulation of Investigatory Powers Act 2000 as amended by The Protection of Freedoms Act 2011

**Collateral Intrusion** means:

Surveillance which indirectly intrudes into the privacy of anyone who is not the direct subject of the surveillance. This could be innocent bystanders, work colleagues, the children of the surveillance subject.

**Confidential Information** means:

Matters subject to legal privilege, confidential personal information or confidential journalistic information.

Where this type of information could possibly be acquired, the responsible person for authorising will be the Chief Executive, or in his absence, the appropriate Executive Director.

**Covert Surveillance** means:

Surveillance carried out in a manner calculated to ensure that those persons subject to the surveillance are unaware that it is or may be taking place.

**Covert Human Intelligence Source (CHIS)** means:

The use of a person to obtain or access private information **covertly** by establishing or maintaining a personal or other relationship with a suspect (in all cases the advice of the Solicitor to the Council must be sought at the earliest opportunity). The Act refers to persons being asked, induced or assisted to provide such private information (see definition on page 9) CHIS include agents, informants or officers working under cover.

CHIS does not apply to members of the public providing information out of public duty (without expectation of reward or payment) and who have information that is received by them in the normal course of their life.

**Directed Surveillance** means:

Surveillance which is covert, but not intrusive and undertaken:

- a) For the purpose of a specific investigation;
- b) In such a manner as is likely to result in obtaining private information about a person.

Private information in relation to a person includes any information relating to his private or family life.

**Intrusive surveillance** means:

Surveillance carried out in relation to anything taking place on residential premises or in any private vehicle; it involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

*Note: Local authorities are not authorised to carry out intrusive surveillance.*

**Communications data** means:

Information held by communication service providers (eg telecom, internet and postal companies - *csp s*) relating to the communications made by their customers, but **not the contents of the communications themselves.**

**Necessary**

To justify the intrusion surveillance will cause into an individual's rights the Authorising Officer must be satisfied that it is necessary for the reason specified on the application form headed **Authorisation** (For the purpose of preventing or detecting crime or of preventing disorder) given the circumstances of the particular case.

**Proportionality**

The activity must be proportionate to the likely outcome. This entails striking a balance between the intrusiveness of the activity on surveillance subjects and others likely to be effected against, the proposed activity, the circumstances of the case and the need for the activity.

For example, the activity would not be proportional if there was an alternative way of obtaining the information.

Basically, we should not be taking a hammer to crack a nut!

**The following elements of proportionality will therefore be considered:**

- **balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;**



- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods have been considered and why they have not been implemented.

## **Private information**

Is defined in s26 (9) of the Act as that in relation to a person and includes any information relating to his private life.

If observations will not result in obtaining of private information about a person, then it is outside the RIPA framework.

### **Subject(s) means:**

An individual or group of individuals in respect of whom surveillance has been authorised, and such observed contacts of that individual or group of individuals as come to notice during the course of the authorised surveillance.

## **3.0 Pre surveillance visit and planning process**

- 3.1 For the purposes of planning surveillance an investigator should visit the proposed location **once** to plan the surveillance.
- 3.2 The investigator will need to demonstrate both the necessity and proportionality of the permission sought.
- 3.3 Suitable background checks should be made from computer systems and other agencies where a legal gateway exists to exchange information.
- 3.4 The planning process must include identifying where observations will take place; how surveillance will be conducted and recorded (i.e. camera, visual observations with notes taken etc.); what resources are needed; whether the subject will be followed and over what distance; the duration of the surveillance.
- 3.5 Most importantly, the plan must identify any collateral intrusion and set out how this will be kept to a minimum.

## **4.0 Unforeseen circumstances**

- 4.1 Directed surveillance does not include covert surveillance carried out as an immediate response to events or circumstances which, by their nature, could not be foreseen.

- 4.2 Investigators witnessing an offence during the course of their normal duties should record as soon as possible their observations and make a referral in the normal way.
- 4.3 Where it is vital that surveillance should be continued, urgent oral authorisation (see paragraph 5.6) must be sought.

## 5.0 Authorisation procedures

### *Written authorisations*

- 5.1 No surveillance falling under the provisions of RIPA shall take place without authorisation by the Authorising Officer **and approval by a Magistrates Court.**
- 5.2 Wherever possible authorisation shall be in writing.
- 5.3 Before giving authorisations for surveillance, the authorising officer must give individual attention to each case and be satisfied that:
- (1) The surveillance is necessary and that there is no other way of providing the evidence.
  - (2) The test of proportionality has been undertaken.
  - (3) Measures are to be taken to avoid or minimise collateral damage.
  - (4) Surveillance has been properly planned in all its aspects including (3) above and that: the location of observations has been properly identified; that the method of surveillance is identified; the period (both dates and timings) over which surveillance is to take place has been stated.
- 5.4 Authorisations will be endorsed on the **Authorisation** application form and a copy returned to the investigator via the appropriate line manager (in the case of benefits, this is the Senior Benefit Officer). Original documentation will be retained in accordance with paragraphs 8 & 9. Alternatively, if authorisation is refused this, together with reasons, will be shown on the **Authorisation** form.
- 5.5 In urgent cases, oral authority can be given as outlined in 5.6.

### *Oral authorisations*

- 5.6 In extreme cases where delay would damage the investigation, oral authorisation may be given. However, the same considerations must be applied and great care taken before authorisation is given.
- 5.7 The Authorising officer shall record the authorisation in the Surveillance file and make a record on the control matrix.
- 5.8 The investigator will record the authorisation in a QB50 notebook.

## *Access to Communications Data*

- 5.9 Requests for access to, and disclosure of, communications data may only be made via the Council's Accredited Officer or Single Point of Contact (SPOC).
- 5.10 The SPOC will ensure that officers designated in the Council's scheme of delegation have applied tests of necessity and proportionality and the risk of collateral intrusion has been taken fully into account (see paragraph 1.8).
- 5.11 This policy must be read in conjunction with the Regulation of Investigatory Powers (Communications Data) Order 2003 and Home Office Code of Practice (a copy of which accompanies this Policy).

### **6.0 Duration of authorisations**

- 6.1 Once authorised, surveillance will normally start immediately and in the case of Benefit cases, must begin within 10 days. In the event that circumstances delay this, the reasons for delay must be documented on the investigation file to show there has been no unreasonable delay.
- 6.2 Written authorisations last for three months beginning with the day on which they took effect and may be renewed at intervals of not longer than three months.
- 6.3 Urgent oral authorisations last for seventy-two hours from the time they were given.

### **7.0 Review of authorisations**

- 7.1 The Authorising Officer will undertake a review at monthly intervals during the duration of surveillance (or shorter period if the circumstances of the particular surveillance justify). Authority to continue may be withdrawn as a result of the review if the activity fails to meet expectations.

### **8.0 Changes of circumstance**

- 8.1 In the event a change of circumstance occurs the investigating officer shall advise the Authorising Officer (using the **Review form**) within seventy two hours of becoming aware of the change.
- 8.2 Surveillance activity cannot commence in respect of the changed circumstances unless authorised.
- 8.3 The Authorising Officer shall reconsider if surveillance remains appropriate once again using the criteria employed in 5.0 above.
- 8.4 If authorised to continue, the Authorising Officer shall complete the **Review form**; otherwise, cancellation will be given orally followed by completion of the **Cancellation form**, setting out reasons for cancellation.

## 9.0 Cancellation of Surveillance

9.1 When surveillance operations have been completed, the Authorised Officer will cancel authorisations and they will not be allowed to expire automatically at the end of the three month (or 72 hour) period referred to in 6.0 above.

## 10.0 Covert Human Intelligence Sources (CHIS)

10.1 Whilst it is unlikely that Service areas will use CHIS (for Benefit investigations, there is a clear policy **not** to use them) it is recognized that a member of the public, or a Council Officer, might fulfil the role of a CHIS even though they have not been *specifically* asked to use a relationship for covert purposes. It is essential that the following provisions are observed. This is supplemented by the Home Office Code of Practice which accompanies this Policy (website link):

- A named officer (ie a “Handler”) will have day to day responsibility for dealing with the CHIS. That officer will –
  - fully recognize the Council has a duty of care to the CHIS, whose security, safety and welfare is paramount.
  - Undertake a risk assessment prior to the use of the CHIS to determine the risk to them and the likely consequences should their role become known.
  - Take fully into account, at the outset, whether there will be ongoing security and welfare considerations related to the Source, once the authorisation has been cancelled, and
  - Maintain a record of the use made of the CHIS, and regulate access to them, ensuring that the Regulation of Investigatory Powers (Source Records) Regulations 2000 are fully complied with
- A further named officer will have general oversight of the use made of the CHIS (ie a “Controller”).
- **Before approving a CHIS, the advice of the Solicitor to the Council must be sought at the earliest opportunity**

10.2 Officers conducting investigations shall clearly establish whether persons assisting the Council might fulfil the role of a CHIS. Possible examples are –

- The use of professional witnesses
- “Entrapment cases” – pretending to be a customer.

10.3 Only the Chief Executive (or his absence, an Executive Director), has the power to authorise a CHIS where it involves a vulnerable person or a juvenile, or where surveillance involves communications subject to legal privilege, confidential personal information or confidential journalistic material.

## 11.0 Record of authorisations

- 11.1 A record of all surveillance authorisations (including refusals) together with review documents shall be maintained by the Authorised Officer.
- 11.2 In addition, the Authorising Officer shall maintain a matrix controlling the authorisations, extensions, reviews and cancellations.
- 11.3 The Council's Democratic Services Manager shall hold a central, computerised, register with details of all authorizations and applications for access to communications data. Such records shall be available for inspection by officials from the Office of the Surveillance Commissioner and, for communications data, the Interception Commissioner. The central register shall contain the following information:-
- The type and date of authorisation
  - The name and rank/grade of the authorising officer
  - The date of magistrates' approval
  - A unique reference number for the investigation or operation
  - The title of the investigation/operation, and a brief description of the subjects, if known
  - If the urgency provisions were used, and why
  - If "self-authorisation" applies
  - If an authorisation is renewed, when and the name and rank of the authorising officer
  - If confidential information is likely to be a consequence of the investigation or operation
  - The date the authorisation was cancelled
- 11.4 Authorising officers shall ensure that the Democratic Services Manager is provided with the required information to maintain the central register.

## **12.0 Quality Assurance**

- 12.1 The Council's Democratic Services Manager and Solicitor to the Council shall jointly be responsible for internal quality assurance. This entails checking that all applications and authorizations have been satisfactorily completed in accordance with the appropriate Code of Practice, that there are subsequent timely reviews, renewals and cancellations, and that the process has regard to the critical areas identified by reports issued from time to time by the Office of the Surveillance Commissioner.

## **13.0 Retention of material and security**

- 13.1 Where there is reasonable belief that material relating to any surveillance could be relevant to pending or future criminal or civil proceedings, it should be preserved in accordance with the requirements, where appropriate, of the Criminal Procedure and Investigations Act 1996 and other relevant legislation.
- 13.2 Where surveillance has ceased or where surveillance has concluded and the material obtained is longer required, it shall be destroyed immediately.

13.3 Authorisations will be destroyed as confidential material. Central records will be destroyed after three years of the ending of authorisation. Counter fraud records shall be destroyed after five years provided the record is no longer required as evidence in support of legal action.

13.4 All material relating to surveillance and requests for access to communications data shall be kept securely.

**14.0 Complaints procedure**

14.1 The Council shall maintain the standards set out in this Policy.

14.2 Any complaint arising out of investigatory work shall be dealt with in accordance with the Council’s Comments, Complaints and Compliments Procedure ([website link](#)).

14.3 If the matter cannot be resolved at a local level the complainant has recourse to the Investigatory Powers Tribunal, PO Box 33220 London SW1H 9ZQ. (020 7273 4514).

**ANNEXE**

**AUTHORISING OFFICERS - RIPA**

*Regulation of Investigatory Powers Act 2000*

To authorise covert surveillance, Covert Human Intelligence Sources, and undertake investigations:

*All subject to the Council's Corporate Policy and appropriate Home Office Code of Practice and subject to approval by a Magistrates Court*

To authorise requests for access to, and disclosure of, Communications data:

*Requests for Communications data being channelled through the SPOC (Democratic Services Manager)*

**Covert Surveillance covering the following:-**

1. Crime and disorder and anti-social behaviour; Noise; Licensing; Food Safety; Littering; Dog Control; Flytipping; Refuse; Health & Safety; Abandoned Vehicles
2. Planning Enforcement
3. Benefit Fraud
4. Personnel Issues

**ALL - Chief Executive; Executive Director (prior to approval by a Magistrates Court)**

**Planning**

**Head of Planning Services**

**Environmental Health  
(Noise; Licensing; Food Safety; Littering; Dog Control; Flytipping; Refuse; Health & Safety; Abandoned & Nuisance Vehicles)**

**Executive Director ;  
Head of Environmental Services;  
Environmental Protection Manager;  
Commercial Health Manager;  
Waste Manager**

**Crime & Disorder - Anti-Social Behaviour**

**Executive Director (ML);  
Head of Environmental Services  
Commercial Health Manager;  
Environmental Protection Manager;  
Waste Manager**

**Anti Fraud and Corruption**

**Head of Revenue and Benefit**

**Strategy (Benefits)**

**Services**

**Other officers in absence of above -**

**Solicitor to the Council;  
Democratic Services Manager**

**Personnel**

**Head of Organisational Development**

Covert Human Intelligence Authorisations where surveillance involves communications with vulnerable people or juveniles or is subject to legal privilege, confidential personal information or confidential journalistic material.

Chief Executive, or in his absence, Executive Director ~~in consultation with the Leader of the Council (or in his absence the Deputy Leader)~~  
Prior to approval by a Magistrates Court



## APPENDIX B

<b>Date:</b>	1 April 2011
<b>Ref no:</b>	CMT-2011-016 RIPA

# Member Briefing

<b>Title:</b>	Changes to Local Authority Covert Surveillance Powers (RIPA)
---------------	--

**Summary:** The Protection of Freedoms Bill, published in February 2011, includes proposals to restrict councils' powers to conduct covert surveillance under what is termed the RIPA provisions.. In future – once the provisions are enacted and codes and orders are put in place – it will be necessary for councils to obtain the approval of a magistrate for the use or renewal of any one of the three investigatory techniques available. In addition, there will be a serious offence test; councils will only be able to authorise surveillance in cases where the offence being investigated carries a custodial sentence of six months or more.

### Further information:

#### 1. Communication

- 1.1 Once the changes have received the Royal Assent (expected Easter 2011), and the government has introduced orders and codes to “put the meat on the bones” (which may be up to a year), a further briefing will be issued. .
- 1.2 In the meantime, the implications for this council’s current covert surveillance policy and procedures and officer delegation will be examined and a report will be presented to the Policy and Resources Committee in June 2011.

#### 2. Current Surveillance Powers

- 2.1 Councils currently have the ability to use three different covert investigating methods for the purposes of preventing or detecting crime under the Regulation of Investigatory Powers Act 2000 (RIPA):-
  - Directed surveillance (ie watching premises or people to gain information).
  - Obtaining communications data, from telephone service providers, via a council SPOC (this council has never used this power)
  - Deployment of a Covert Human Intelligence Source (CHIS) (again the council has never used this provision).
- 2.2 The use of directed surveillance has only been as a last resort (where it is not possible to use other methods to obtain information). At East Northamptonshire, authorisations have been granted by a head of service or a senior manager for the following where it is suspected an offence has been committed:-
  - House to house collections



- Fly tipping
- Benefit fraud but authorisations are now granted by the Department of Work and Pensions (DWP)
- Noise nuisance
- Anti-social behaviour
- Hackney carriage licensing
- Houses in Multiple Occupation.

**2.3** The use of the powers is regulated by the Office of the Surveillance Commissioner, who undertakes council inspections and pinpoints any failings.

### **3. Effect of the new Provisions**

**3.1** The initial conclusion to the changes to the RIPA provisions is that it will no longer be possible for the council to use RIPA powers for all of the above areas - with the exception of benefit fraud – as compared to the current situation. The highest sanction for most of the offences would be a fine but house to house collections offences could result in a custodial sentence not exceeding six months. The DWP may continue to grant authorisations for benefit fraud where conviction may well result in a custodial sentence of six months or more.

**3.2** There may be new areas for which consideration would be given to authorisations in the future. However, in the – probably unlikely - event of RIPA powers being used, there would be additional costs and action may be delayed.

<b>Originator:</b>	Keith Osborne, Democratic Services Manager
<b>Contact details:</b>	01832 742113 kwosborne@east-northamptonshire.gov.uk
<b>Approved by CMT</b>	CMT 29 March 2011 – approved
<b>Approved by Leader</b>	4 April 2011