East Northamptonshire Council

Policy & Resources Committee – 9 September 2013

Covert Surveillance Policy

Purpose of report: To inform Members of the impact of the Protection of Freedoms Act 2012 and to update the Council's Covert Surveillance Policy accordingly

Attachment(s)

Appendix One – Covert Surveillance Policy

1.0 Background

1.1 In September 2011, this Committee approved a revised version of the Council's Covert Surveillance Policy in anticipation of the changes that would come into force as a result of the Protection of Freedoms Act 2012 (the Act), which was, at that time, progressing through Parliament.

1.2 This paper sets out the implications for the Council of the Act, and attaches as an appendix a revised version of the Covert Surveillance Policy now that the Bill has been enacted.

2.0 Protection of Freedoms Act 2012

2.1 The Act came into force in November 2012 and changed the procedure for the authorisation of local authority surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA). The revised policy reflects the updated Guidance to Local Authorities.

2.2 As a result of the Act, local authorities may only authorise directed surveillance (covert surveillance on individuals in public places) or use a covert human intelligence source (CHIS) when the following conditions are met:

- The authorisation is for the purpose of preventing or detecting conduct which constitutes a criminal offence; and
- The criminal offence is one which is punishable by a maximum term of at least six months' imprisonment or is an offence under:-
    - s146 of the Licensing Act 2003(a) (sale of alcohol to children);
    - s147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
    - s147A of the Licensing Act 2003(b) (persistently selling alcohol to children);
    - s7 of the Children & Young Persons Act 1993 (c) (sale of tobacco etc to persons under 18)

2.3 In addition to restricting the use of directed surveillance and CHIS, both types of activity will require subsequent authorisation by a JP.

2.4 The Council has made limited but effective use of its RIPA powers, for example in relation to fly-tipping hot spots, and when it does so the use has been proportionate. However, the limitations imposed by the Act mean that use of covert surveillance will almost always have to be replaced by other forms of activity, as indicated in the Policy. It should be noted that these may be less effective.

2.5 This update ensures that the Council's policy reflects the changes brought in by the new legislation.

3.0 Equality and diversity implications

3.1 Applying the investigatory powers given to the Council in accordance with the Human Rights Act is designed to ensure that there should be no equality and diversity implications to the use of the powers.

4.0 Legal implications

4.1 Failure to obtain a RIPA authorisation where a person's rights under the European Convention of Human Rights are interfered with may leave the Council open to civil action for damages under the Human Rights Act 1998.

5.0 Risk management

5.1 As noted in the legal implications above, the Council could be open to civil action for damages if the appropriate authorisation is not sought. This is covered by risk reference 259 (non-compliance with legislation) on the Council's risk register.

6.0 Financial implications

6.1 There may be additional resource and cost implications arising from the changes in legislation if the Council needs to employ alternative surveillance techniques which involve more officer time than previously. If the Council does make use of the RIPA provisions in future, there will be resource implications involved in seeking a magistrate's consent to an authorisation. Any additional costs would need to be considered along with the overall financial position of the Council as part of its medium term financial plans.

7.0 Corporate outcomes

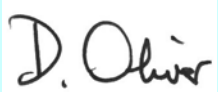
7.1 The revised policy links to the following corporate outcomes:

- Effective partnership working
- Effective management
- Councillors and staff with the right knowledge, skills and behaviours

8.0 Recommendation

8.1 The Committee is recommended to approve the revised Covert Surveillance Policy

(Reason – to ensure that East Northamptonshire Council is compliant with the Protection of Freedoms Act 2012)

Legal	Power: Regulation of Investigatory Powers Act 2000; Protection of Freedoms Act 2012				
	Other considerations: Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance				
Background Papers:					
Person Originating Report:	Emma Gadsby, Policy & Performance Manager, 01832 742099, egadsby@east-northamptonshire.gov.uk				
Date:					
CFO		**MO**		**CX**	

(Committee Report Normal Rev. 22)

East Northamptonshire Council

Covert Surveillance Policy

September 2013

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

Author (Post holder title)	Policy & Performance Manager
Type of document	Policy
Version Number	V2.1
Document File Name	
Issue date	
Approval date and by who (SMT / committee)	
Document held by (name/section)	
For internal publication only or external also?	Internal and external
Document stored on Council website or Eunice?	Website
Next review date	

Change History

Issue	Date	Comments
2.1	September 2013	Revised following changes introduced by the Protection of Freedoms Act 2012 and changes to regulations under RIPA

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)

Distribution List

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)

Links to other documents

Document	Link
Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance	https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

Additional Comments to note

Contents

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 (RIPA) 2000 are used in accordance with the Human Rights Act, the Protection of Freedoms Act 2012 and the amendments to the regulations under RIPA that came into force on 1 November 2012.

2.0 Scope

2.1 Local authorities have a number of powers of covert surveillance which are covered by RIPA which allows local authorities to authorise the use of three covert techniques:

- Covert surveillance on individuals in public places – **directed surveillance** using cameras and other methods such as covert following of individuals
- **Communications data** (such as telephone billing information)
- **Covert human intelligence sources** (CHISs) where individuals interact with suspected offenders in order to investigate crime

2.2 Following the amendments to the RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, **directed surveillance** under RIPA may only be used in certain circumstances and the additional authorisation of a Justice of the Peace (magistrate or district judge) will be needed for all three forms of surveillance covered by RIPA.

2.3 Local authorities will no longer be able to use **directed surveillance** in some cases where it was previously authorised. However, this does not mean it will not be possible to investigate these areas in order to stop offending behaviour. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

2.4 This policy forms part of the Council's overall Benefits Counter Fraud Strategy.

3.0 Policy outcomes

3.1 The outcomes to be delivered by this policy are:

Corporate Covert Surveillance Policy outcomes	**Links to corporate outcomes**
• The Council meets its duties under the relevant legislation • Staff are aware of the need to balance the use of covert surveillance with the rights of those who may be subject to it • The Council's processes are transparent	• Effective partnership working • Effective management • Councillors and staff with the right knowledge, skills and behaviours

4.0 Corporate Covert Surveillance Policy

4.1 Like any other public body which is able to investigate criminal offences, the Council is able to make use of covert surveillance in order to gather information. Information obtained in this way can be valuable and can often be used as evidence in legal proceedings or as intelligence to identify or prevent offending.

4.2 It is important that the Council uses all the tools available to it to make the best use of council tax payers' money. However, the Council is committed to using these techniques only when it is proper to do so and proportionate to the offence suspected.

4.3 The use of covert techniques may, in certain circumstances, interfere with a person's rights under the European Convention on Human Rights (ECHR). Article 8 provides a right to respect for private and family life, home and correspondence. As covert techniques are generally used to obtain information about a person without their knowledge, there is a clear likelihood of interference with the Article 8 rights of those subject to covert techniques.

4.4 Any interference with Article 8 rights will be lawful provided a public authority can demonstrate that the following three tests are met:

- Is the proposed interference proportionate to what it seeks to achieve?
- Is the proposed interference necessary in pursuit of a legitimate aim?
- Is the proposed interference permitted in law?

4.5 RIPA offers a statutory framework to ensure that the three tests are met. Failure to obtain a RIPA authorisation where Article 8 interference does occur may leave the Council open to civil action for damages under the Human Rights Act 1998.

4.6 This policy sets out the individual and collective responsibilities relating to the use of covert surveillance, making sure that the techniques are used in accordance with the relevant legislation, that the Council meets the professional standards expected of it and that the risks to the Council are minimised.

4.7 Process

4.8 RIPA authorisation is required only where the use of directed surveillance, the conduct or use of a covert human intelligence source or the acquisition of communications data is likely to result in the interference of a person's Article 8 rights. Authorisation is therefore more likely to be appropriate in circumstances and in locations where a person has a heightened expectation of privacy.

4.9 Identifying the appropriate technique

4.10 At the start of an investigation where officers intend to use **directed surveillance**, they will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use, it must be clear that the threshold is met and that it is necessary and proportionate to use it.

4.11 The Council is only permitted to authorise directed surveillance where the following conditions apply:

- The authorisation is for the purpose of preventing or detecting conduct which constitutes a criminal offence; and
- The criminal offence is one which is punishable by a maximum term of at least six months' imprisonment or is an offence under:-
    - s146 of the Licensing Act 2003(a) (sale of alcohol to children);
    - s147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
    - s147A of the Licensing Act 2003(b) (persistently selling alcohol to children);
    - s7 of the Children & Young Persons Act 1993(c) (sale of tobacco etc to persons under 18)

4.12 The need to complete the RIPA authorisation/application form and seek approval from an authorising officer/designated person within the Council remains the same as before the new provisions were introduced.

4.13 Authorisation by a JP

4.14 All three covert techniques will now require subsequent authorisation by a JP once the approval from the authorising officer/designated person within the Council has been given. No surveillance falling under the provisions of RIPA shall take place without authorisation by the Authorising Officer and approval by a JP.

4.15 The application should be made in writing on the standard Home Office form (available on EUNICE). The application should describe the precise nature and scope of the proposed activity and the likely interference with Article 8 rights and set out the case for the interference on the grounds of necessity and proportionality.

4.16 Authorising officers for this Council are shown in Appendix A. It is good practice for the authorisation to be granted by a person who is not directly involved in taking operational decisions in relation to the matter under investigation.

4.17 A checklist is included at Appendix B to help determine whether the techniques should be used and whether authorisation is required.

4.18 Once the Authorising Officer is satisfied that such surveillance is proportionate to the offence being investigated, the authorisation may be granted and an application for judicial approval must then be made to the Magistrates' Court.

4.19 An authorisation will run for three months for directed surveillance and 12 months for a CHIS (or one month if the CHIS is aged under 18 years). Authorisations and notices for communications data will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

4.20 In certain situations of urgency, for example where a delay would damage the investigation, RIPA authorisation can be sought and granted verbally (see Appendix C for how to deal with requests outside usual office hours)

4.21 The need for an authorisation should be kept permanently under review, usually by the Authorising Officer. If at any point the grounds for authorisation cease to exist (particularly with directed surveillance, for example where the surveillance has achieved its objective and is no longer necessary or where the activity is no longer proportionate), it should be submitted to the Authorising Officer for cancellation. Authorisations should never simply be allowed to lapse.

4.22 An authorisation can also be renewed, and should be submitted to the Authorising Officer for consideration. If granted, this is also subject to judicial approval and an application for renewal must be made to the Magistrates' Court in the same way as the original authorisation.

4.23 Record keeping

4.24 A central record should be held by each Service to assist the Office of Surveillance Commissioners during its periodic statutory inspection visits to the Council. The central record should be kept for a minimum rolling period of three years from the end of each authorisation, and should include the following information:

- The type of authorisation (i.e. directed surveillance, CHIS or communications data);
- The date the authorisation was granted;
- The name and grade of the authorising officer;
- The frequency of reviews set by the authorising officer and a record of the result of any reviews;
- The operational identifier or unique reference number for the investigation or operation;
- The identities of subjects, where these are known;
- Whether the urgency provisions have been used and, if so, the reasons for their use;
- Whether the relevant deployment is likely to result in obtaining confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- Details of any renewal of the authorisation including the name and grade of the Authorising Officer granting the renewal;
- The date the authorisation was cancelled;
- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the authorising officer.

A copy of all documentation produced while the authorisation was in place should also be retained in the central record held by the Democratic & Electoral Services Manager.

4.25 In addition, the information obtained through the deployment of covert techniques must be retained, used and shared strictly in accordance with the Data Protection Act 1998 and any other relevant legislation, because of the possible interference with Article 8 rights.

4.26 It should be retained for no longer than is necessary in the circumstances, used only for the purposes for which it was obtained and shared only where specifically allowed by law. Officers should familiarise themselves with the legislation, and seek guidance from the Council's Data Protection Officer.

4.27 Other considerations

4.28 If the use of covert surveillance or the conduct or use of a covert human intelligence source is likely to result in the Council obtaining **confidential information** (defined in the glossary), authorisation can only be granted by the Chief Executive or Executive Director. Due consideration must be given to the additional legal and ethical issues this raises.

4.29 Requests for access to, and disclosure of, **communications data** may only be made via the Council's Accredited Officer or Single Point of Contact (see Appendix A).

4.30 Officers may occasionally be involved in a **joint covert surveillance operation** with another public authority such as the Department for Work & Pensions or the Environment Agency. It is important, in these circumstances, that Council officers satisfy themselves as to the existence and extent of any RIPA authorisation related to that operation. It is good practice for a signed copy of the authorisation from the lead agency to be provided to the Council ahead of the surveillance operation.

5.0 Next steps

5.1 This policy will be reviewed in three years or sooner if required by changes to legislation.

6.0 Glossary of terms

Term	Definition
Communications data	The 'who', 'when' and 'where' of a communication but not the 'what' (i.e. the content of what was said or written). This consists of: • Traffic data (which includes information about where the communications are made or received) – local authorities are **not** authorised to obtain this data • Service use information (such as the type of communication, time sent and its duration) • Subscriber information (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services)
Confidential information	Falls into three categories: • Matters subject to legal privilege • Confidential personal information (e.g. relating to a person's physical or mental health, or to spiritual counselling or assistance) when held in confidence in accordance with a profession, trade or vocation. Communications between an MP or Councillor and a constituent are also likely to fall within this category • Confidential journalistic material If any confidential information is likely to be obtained by using a covert technique then authorisation must be given by the Chief Executive.
Covert human intelligence source (CHIS)	Undercover officers, public informants and people who make test purchases
Covert surveillance	Surveillance which is carried out with the aim that those who are subject to it are unaware that it is taking place
Directed surveillance	Covert surveillance which is not intrusive and carried out in places other than residential premises or private vehicles
Intrusive surveillance	Covert surveillance carried out in residential premises or private vehicles – local authorities may not do this

Appendix A – Authorising Officers

Service	Authorising Officer
All services or where the authorisation is likely to obtain confidential information or the deployment of a CHIS under the age of 18 or vulnerable person	Chief Executive Executive Director
All services where access to and disclosure of communications data is involved	Democratic & Electoral Services Manager (the Council's Accredited Single Point of Contact – SPOC)
Customer & Community Services • Benefits • Communications • Community Partnerships • Customer Services • Land Charges • Revenues	Head of Customer & Community Services
Environmental Services • Environmental Protection • Health Protection • Waste Services	Head of Environmental Services
Financial Services • External Funding • EnCor Financial Services • Internal and external audit • Procurement	Chief Finance and s151 Officer
ICT Services • Applications • Technical • Support	Head of ICT Services
Planning Services • Building Control • Development Control • Housing Strategy • Planning Admin • Planning Policy & Conservation	Head of Planning Services
Resources & Organisational Development • Amenities • Democratic & Electoral Services • Human Resources • Policy & Performance	Head of Resources & Organisational Development

Appendix B – checklist

Council staff must:

Action	✓
Read the Covert Surveillance Policy and be aware of any other relevant guidance	
Determine whether directed surveillance, a CHIS or the acquisition of communications data is required	
Assess whether the authorisation will be in accordance with the latest legislative requirements and be able to demonstrate that the suspected offence is subject to a custodial sentence of six months or more (for directed surveillance)	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly	
Consider whether surveillance will be proportionate	
Consider all less intrusive options which may be available and practicable and use those first if possible	
Ensure that measures are taken to avoid or minimise intrusion into the privacy of anyone who is not the direct subject of the surveillance	
If authorisation is necessary and proportionate, prepare and submit an application to carry out the appropriate technique to an Authorising Officer	
Review regularly and submit to Authorising Officer on date set	
If operation is no longer necessary or proportionate, or fulfils its objective, complete a cancellation form and submit to Authorising Officer	

Authorising Officer must:

Action	✓
Consider in detail whether all options have been duly considered, including taking into account the Covert Surveillance Policy and any other relevant guidance	
Confirm that the offence is subject to a custodial sentence of six months or more (for directed surveillance)	
Consider whether surveillance can be considered to be in accordance with the law and is necessary and proportionate to the offence being investigated	
Authorise **only if** an overt or less obtrusive option is not practicable	

Ensure the relevant judicial authority has made an order approving the grant of the authorisation	
If surveillance is still necessary and proportionate: • Review authorisation • Set an appropriate further review date	
Cancel authorisation when it is no longer necessary or proportionate for it to continue	

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

Yes

No

• Complete RIPA authorisation/ notice form, and seek approval of authorising officer/designated person as per current arrangements.
• Complete application part of the judicial application/order form for JP.

Outside usual office hours:

A JP may consider an authorisation out of hours in **exceptional** circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
• Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
• If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
• Attend hearing as directed with two copies of both the counter- signed RIPA authorisation form or notice and the accompanying judicial application/order form.

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

No

Yes

Within Office Hours Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
-Section 7 of the Children and Young Persons Act 1993.

No

Yes

Attend court with:
• counter-signed RIPA authorisation/ or notice (for CD authorisations/ notices the signatures may be electronic signatures).
• the accompanying judicial application/order form.
• any other relevant reference or supporting material.

Outcome

Investigator may **not** use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met **if** further of fences come to light as the case progresses.

Refuse to approve the grant or renewal and quash the authorisation or notice.

Refuse to approve the grant or re-newal of an authorisation or notice.

Approve the grant or re-newal of an authorisation or notice.

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.

The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may **not** use the covert technique. Local authority may wish to address, for example, a technical error and reapply.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

Obtain signed order and retain original RIPA authorisation/notice.
For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.
If out of hours, a copy of the signed order to be provided to the court the next working day.