ANNEX 1

OXFORDSHIRE COUNTY COUNCIL
www.oxfordshire.gov.uk

POLICY ON COMPLIANCE WITH THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1 Introduction

1.1 Part II of this Act came into effect on 25 September 2000 and regulates the use of covert activities by Local Authorities. Special authorisation arrangements need to be put in place whenever the Local Authority considers commencing a covert surveillance or obtaining information by the use of informants or officers acting in an undercover capacity.

1.2 Local Authorities do operate a number of covert activities in a number of key areas, examples of which are highlighted in Appendix 1 to this policy. Activities can include covert surveillance in relation to internal audit and personnel where fraud, deception or gross misconduct by staff might be suspected. The legal requirements are now supplemented by codes of practice issued by the Home Office for certain surveillance activities, (covert surveillance activity and covert human intelligence sources) breaches of which can be cited in Court as evidence of failure to abide by the requirements of RIPA. This may mean that the evidence obtained by that surveillance is excluded.

1.3 The Council policy is that specific authorisation is required for any covert investigation. There are only a small number of authorised Officers who can give this permission and these are as follows:

- County Solicitor
- Designated authorised officer – Trading Standards

Before authorisation it will normally be necessary to consult with the relevant Head of Service.

1.4 Before seeking authorisation you should discuss with your Line Manager.

1.5 This Policy applies to all services except Trading Standards who have their own specific internal Directorate procedures for dealing with authorisations. However, copies of all authorisations including those for Trading Standards will be forwarded to the County Solicitor for retention in a central register, and Trading Standards will simply be exempt from the provisions of this policy concerning prior authorisation.

2 Definitions

Intrusive Surveillance – Local authorities may not use hidden officers or concealed surveillance devices within a person's home or vehicle in order to directly observe that person.

Covert Surveillance – This is a non-intrusive operation or investigation calculated to ensure the person is unaware of the covert surveillance undertaken which is likely to result in the obtaining of private information about

a person (targeted or otherwise) e.g. checking staff are making claimed visits, time spent etc.

Covert Human Intelligence Source (CHIS) – This is an undercover operation whereby an informant or undercover officer establishes or maintains some sort of relationship with the person in order to obtain private information e.g. test purchasing, telephone calls where the identity of the caller is withheld.

Head of Service – this also includes Business Managers and those authorised to act on behalf of the Head of Service as set out in clause 7.4.

3 RIPA Requirements

3.1 Basically the surveillance must be authorised prior to it taking place and must subsequently be shown to be necessary and proportionate.

3.2 All non-intrusive covert surveillance and CHIS requires prior authorisation by the appropriate Local Authority officer (as set out in this policy) before any surveillance activity takes place. The only exception to this is where covert surveillance is undertaken by way of an immediate response to events that means it was not foreseeable and not practical to obtain prior authorisation.

3.3 There is no direct sanction against Local Authorities within the Act for failing to seek or obtain authorisation within the organisation for surveillance, nevertheless such activity by its nature is an interference of a person's right to a private and family life guaranteed under Article 8 of the European Convention on Human Rights. The consequences of not obtaining authorisation may mean that the action is unlawful by virtue of Section 6 of the Human Rights Act 1998 i.e. a failure by the Authority to conduct this work in accordance with human rights conventions. Obtaining authorisation will ensure the Local Authority's actions are carried out in accordance with the law and satisfy the stringent and necessary safeguards against abuse.

4 Grounds of Necessity

The authorisation by itself does not ensure lawfulness, as it is necessary also to demonstrate that the interference was justified as both necessary and proportionate. **The statutory grounds of necessity must apply for the purposes of preventing or detecting crime or of preventing disorder.**

5 Proportionality

5.1 Once a ground for necessity is demonstrated, the person granting the authorisation must also believe that the use of an intelligence source or surveillance is proportionate, to what is aimed to be achieved by the conduct and use of that source or surveillance. This involves balancing the intrusive nature of the investigation or operation and the impact on the target or others who might be affected by it against the need for the

information to be used in operational terms. Other less intrusive options should be considered and evaluated. All RIPA investigations or operations are intrusive and should be carefully managed to meet the objective in question and must not be used in an arbitrary or unfair way.

5.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion i.e. the risk of intrusion into the privacy of persons other than those directly targeted by the operation. Measures should be taken wherever practicable to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

6 Confidential Material

Where an investigation may reveal sensitive and confidential material this requires special authorisation by the Chief Executive or his or her delegated Authorised Officer (Assistant Chief Executive).

7 Implementation Procedure

7.1 Heads of Service will be the officers who are responsible for seeking authorisation for surveillance. They have operational responsibility for ensuring compliance with the requirements of RIPA and Home Office Codes of Practice (Covert Surveillance and Covert Human Intelligence Services) in relation to covert surveillance and covert human intelligence source for their service. The Codes of Practice can be downloaded from the following link:

http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/?view=Standard&pubID=518844

7.2 All applications for authorisation and authorisations must be made in accordance with the procedure and on the appropriate forms: (download forms from the links below)

RIPA Form 1 – Authorisation Directed Surveillance
RIPA Form 2 – Review of a Directed Surveillance Authorisation
RIPA Form 3 – Renewal of a Directed Surveillance Authorisation
RIPA Form 4 – Cancellation of a Directed Surveillance Authorisation
RIPA Form 5 – Application for Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)
RIPA Form 6 – Review of a Covert Human Intelligence Source (CHIS) Authorisation
RIPA Form 7 – Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation
RIPA Form 8 – Cancellation of an Authorisation for the use or conduct of a Covert Human Intelligence Source (CHIS)
RIPA Form 9 – Application request for Communications Data

7.3 All requests for authorisation must be forwarded to the County Solicitor who will maintain a central record for inspection. The County Solicitor will monitor the central register periodically and produce an annual report to CCMT. Renewals of authorisations will be for a maximum of 3 months and cancellation of authorisation should be requested as soon as possible i.e. as soon as the surveillance is no longer considered necessary.

7.4 The Authorised Officers may authorise a person to act in their absence, who will be a Senior Manager and who will have overall management responsibility for the operation/investigation. A list of all current named Authorised Officers and named substitutes will be included in the central register and appended to this Policy (Appendix 2). The County Solicitor will approve all proposed Authorised Officers for inclusion in a central register. The annual report to CCMT will also include a review of the appropriate designated Authorised Officers.

7.5 All Managers have responsibility for ensuring that they have sufficient understanding to recognise when an investigation or operation falls within the requirements of RIPA. Authorised Officers will keep up to date with developments in the law and best practice relating to RIPA.

7.6 Authorised Officers must ensure full compliance with the RIPA Authorisation Procedure set out in the appropriate forms in 7.2 above.

7.7 Authorised Officers and Heads of Service will co-operate fully with any inspection arranged by the Office of Surveillance Commissioners.

8 Communications Data

8.1 Part I of RIPA sets out these requirements. The Council can access certain communications data only “for the purpose of preventing or detecting crime or of preventing disorder”. The exception to this is for the Fire Control Officer in an emergency for the purposes of preventing death or injury.

Despite what some commentators claim the Council does not have an automatic legal right to intercept (i.e. “bug”) phones or listen into other people’s telephone conversations. The primary power the Council has is to obtain certain details (e.g. name and address) of e.g. a telephone subscriber from communications service providers such as: BT, Vodafone, Orange etc.

Monitoring of calls may be necessary for legitimate employment purposes but will be subject to the same authorisation requirements as set out in this policy.

8.2 The applications to obtain communications data, other than for the prevention of death or injury as in 8.1 above, must be forwarded to the “Single Point of Contact (SPOC)” in consultation with the relevant Head of Service. If the SPOC agrees the request is within the scope of RIPA he will

then forward it to the appropriate designated officer within the relevant Service/Directorate.

8.3 The concept of the "SPOC" has been agreed between the Home Office and the communication service providers (CSPs) and introduces a verification process to ensure that only data entitled to be obtained is so obtained.

8.4 The "SPOC" for Oxfordshire County Council is the Assistant Head of Trading Standards. The designated officer, after signing the authorisation, must then forward it to the SPOC for him to endorse and forward to the relevant CSP.

9 Training and Briefings

The County Solicitor will provide updates on the RIPA law and best practice but Heads of Service and other Managers must be able to recognise potential RIPA situations.

10 Conclusion

The benefit of having a clear and regulated system of authorising all covert activities is self-evident. Surveillance by its very nature is intrusive and therefore should be subject to appropriate scrutiny at the highest level and the authorisation procedure requires that the reasons for the decision are specifically and clearly set out and the basis for the decision is readily accessible and understood. Completion of appropriate authorisations also means that in reaching a decision alternative options will also have been explored. Proper compliance with the procedure and properly recorded authorisations are the best defence should any of our investigations be challenged.

11 Review of this Policy

The County Solicitor will review this Policy annually.

Responsible Officer: Peter G Clark
County Solicitor

Date: October 2009

Next Review Date: October 2010

Appendix 1

Examples of Use of Surveillance in the Council's Services

(both Directorates: Children, Young People & Families and Social and Community Services)

1. Any use of process servers or private investigators where enquiries may need to be made as to parents'/children's whereabouts etc.
2. Surveillance of properties to establish whether prohibited persons are visiting. Surveillance of premises for any other reason including possible drug dealing, domestic violence, paedophile activity etc.
3. Using clients (including vulnerable adults to record times and duration of home care visits).
4. Use of concealed cameras to record possible theft within home environment (may be intrusive and, therefore, requires police authorisation).

Note: In joint Police and Social Services child protection investigations it should be the Police that would normally take responsibility for appropriate authorisation.

Education

1. Possible use of surveillance to check fraudulent grant claims i.e. checks on addresses and financial details including use of credit enquiry agent.
2. Covert surveillance within schools to ascertain possible criminal activities including threats, assaults, bullying, criminal damage etc.

Environmental Services

1. Covert surveillance to establish damage to "street furniture" e.g. traffic signs, bridges etc.
2. Covert surveillance of roads adjacent to farms to ascertain wilful or negligent discharge of farm material on roads.
3. Covert surveillance of unauthorised gypsy sites for evidence of tipping, trespass, harassment etc.
4. Waste enforcement - covert surveillance in relation to planning control e.g. mineral extractions or in-fill in excess of planning conditions (Town and County Planning Act 1990).
5. Covert surveillance on removal of obstructions to highways (Section 130 Highways Act 1980).

Fire Service

Covert surveillance for potential arson/fire raising incidents.

Debt Collection

Use of private investigators to establish identity, whereabouts, personal relevant background information of debtors.

Human Resources and Internal Audit

The following areas could apply to any particular service department and would involve HR and/or Internal Audit.

Surveillance and C.H.I.S. in relation to investigation of possible false claims or fraudulent practices including the following:

- travel claim forms and other claims and making appropriate enquiries
- investigation to establish that staff are properly timing and claiming for visits made
- investigation of email, internet use and telephone calls where professional misconduct or unlawful activity is suspected
- covert surveillance of workplace
- installation of covert CCTV
- using overt CCTV for a covert operation
- covert investigation of staff alleging sickness/disability.

Contract Monitoring

Covert investigation to establish compliance (both surveillance and C.H.I.S.) e.g. pretending to be a customer /client to check level of service.

Trading Standards

Covert investigation to fulfil enforcement duties to secure prosecution for consumer protection offences e.g. test purchases/telephone contact where officers will be pretending to be consumers.

Appendix 2 – Authorised Officers and Named Substitutes

Authorised Officer – Peter G Clark County Solicitor

Named Substitute – Stephen P Capaldi Assistant Chief Executive

Authorised Officer – Richard Webb, Deputy Head of Trading Standards

Confidential Material Special Authorisation – Joanna Simons Chief Executive

Named Substitute – Stephen P Capaldi Assistant Chief Executive