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

OXFORDSHIRE COUNTY COUNCIL

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert surveillance 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 This also includes the use of social media sites for gathering evidence to assist in enforcement activities, as set out below:

- officers must not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA.
- officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

1.3 Local Authorities do operate covert activities in a number of key areas. Activities can include covert surveillance in relation to Internal Audit and Human Resources 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.

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

- Chief Legal Officer
- Designated authorising officer – Head of Community Protection Services

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

1.5 Before seeking authorisation you should discuss the matter with your Line Manager.

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

2 Definitions

Surveillance – includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Covert Surveillance – This is carried out to ensure the person who is the subject of the surveillance is unaware that it is or may be taking place. The provisions of RIPA apply to the following forms of covert surveillance:

a) **Directed Surveillance** – is covert but not intrusive, is undertaken for the purposes of a specific investigation 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.

b) **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.[1]

c) **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.

Deputy Director/Head of Service – this also includes those authorised to act on behalf of the Deputy Director/Head of Service as set out in clause 7.4.

3 RIPA Requirements

3.1 Directed surveillance only falls within the scope of the RIPA if it meets one of the following tests – criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

Directed surveillance that does not meet one of these tests will fall outside the scope of the RIPA. In this instance specific authorisation must be sought from the Chief Legal Officer before the activity can take place.

3.2 Basically directed surveillance must be authorised prior to it taking place, be subject to regular review and must be shown to be **necessary and proportionate**. RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance.

[1] The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 [the 2010 Order] provides that directed surveillance carried out in certain premises (e.g. prisons, law firms, police stations) used for the purpose of legal consultations also amount to intrusive surveillance.

3.3 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.

3.4 Judicial approval is also required before any internal authorisations given under RIPA take effect. Once internal authorisation has been granted a specific application to the Magistrates Court will be required.

3.5 There is no direct sanction against Local Authorities within the RIPA 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 Investigatory Powers Tribunal is able to investigate complaints from anyone who feels aggrieved by a public authority's exercise of its powers under RIPA.

3.6 The consequences of not obtaining authorisation and Judicial approval 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 County Director or his/her delegated Authorising Officer.

7 Implementation Procedure

7.1 Deputy Directors/Heads of Service shall be 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/Covert Human Intelligence Services, which can be downloaded from the following link http://homeoffice.gov.uk/counter-terrorism/) in relation to covert surveillance and covert human intelligence source for their service.

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 following link: http://intranet.oxfordshire.gov.uk/cms/content/ripa-policy-surveillance)

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
RIPA Form 10 –	Application for a Judicial Order

7.3 All requests for authorisation must be forwarded to the Chief Legal Officer who will maintain a central record for inspection. The Chief Legal Officer will monitor the central register periodically and produce an annual report to CCMT and Audit & Governance Committee. Renewal of authorisations will be for 3 months and cancellation[2] [3] of authorisations should be requested as soon as possible i.e. as soon as the surveillance is no longer considered necessary. Judicial approval is required for the renewal of an authorisation but it is not required for any internal review or cancellation.

7.4 The Authorising Officers may authorise a person to act in their absence, the substitute will be a Senior Manager and who will have overall management responsibility for the operation/investigation. A list of all current named Authorising Officers and named substitutes will be included in the central

[2] All cancellations must be made in compliance with OSC guidance note 145

[3] Office of the Surveillance Commissioner – Procedures and Guidance

register and appended to this Policy (Appendix 1). The Chief Legal Officer will approve all proposed Authorising Officers for inclusion in a central register. The annual report to CCMT and Audit & Governance Committee will also include a review of the appropriate designated Authorising 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. Authorising Officers will keep up to date with developments in the law and best practice relating to RIPA.

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

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

7.8 RIPA Coordinator (Head of Community Protection Services)

The role of the RIPA coordinator is to have day-to-day oversight of all RIPA authorisations and maintain a central register of all authorisations, review dates, cancellations and renewals.

All forms should be passed through the coordinator to ensure that there is a complete record of all authorisations, contents of the forms will be monitored to ensure they are correctly filled in and the coordinator will supply quarterly statistics to the Senior Responsible Officer (Chief Legal Officer/Monitoring Officer).

The Coordinator will also monitor training requirements and organise training for new staff as appropriate, and ensure continued awareness of RIPA throughout the council via staff information on the Council's Intranet.

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 a telephone subscriber from communication service providers (CSP) 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 made by a Home Office designated

"Single Point of Contact (SPOC)". Arrangements are in place to enable the authority to access communications data via a third party "SPOC". Requests must be forwarded to the Head of Community Protection Services who will consult with the relevant Deputy Director/Head of Service. If the Head of Community Protection Services agrees the request is within the scope of RIPA he will make arrangements for the request to be processed via the SPOC.

8.3 The concept of the "SPOC" has been agreed between the Home Office and the CSP and introduces a verification process to ensure that only data entitled to be obtained is so obtained. Judicial approval of the application is required and the SPOC will not obtain any communications data without evidence of judicial approval.

8.4 Under guidance from the Interception of Communications Commissioner's Office, internal authorisation for an application to access communications data must be provided by an officer who is independent from the service conducting the investigation. Legal Services can provide appropriate independent authorisation of applications.

9 Briefings

The Chief Legal Officer will provide updates on the RIPA legislation and best practice but Deputy Directors/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 fully explored. Proper compliance with the procedure and properly recorded authorisations are the best defence should any of our investigations be challenged.

11 Review of Authorisations and Policy

The Council's "Audit and Governance Committee" will review:

- all authorised RIPA applications quarterly; and
- receive an annual report from the Chief Legal Officer on the operation of the Policy; and
- review the policy annually to ensure it remains compliant with current legislation, relevant codes of practice and continue to meet the responsibilities of the council.

Senior Responsible Officer:	Chief Legal Officer and Monitoring Officer
RIPA Coordinator:	Head of Community Protection Services
Date:	September 2016

Next Review Date: September 2017

Appendix 1 – Authorising Officers and Named Substitutes

Surveillance:

*Authorising Officer – Nick Graham, Chief Legal Officer and Monitoring Officer

*Named Substitute – Lorna Baxter, Chief Finance Officer

Authorising Officer – Richard Webb, Head of Community Protection Services

**Confidential Material Special Authorisation – Peter G Clark, County Director

**Named Substitute – Lorna Baxter, Chief Finance Officer

Communications data:

Authorising Officers:

Nick Graham, Chief Legal Officer and Monitoring Officer

Glenn Watson, Principal Governance Officer

Richard Webb, Head of Community Protection Services