North Tyneside Council
Report to Cabinet
Date: 12 November 2012

ITEM 7(h)

Title: Annual Review of Council Policy on Covert Surveillance

Portfolio(s):	**Regulatory Services**	**Cabinet Member(s):**	**Councillor G Westwater**

Report from Directorate: **Chief Executive's Office**

Report Author: **Vivienne M Geary, Head of Legal, Governance and Commercial Services** **(Tel: 0191 643 5339)**

Stephen Ballantyne, Lawyer Specialist: Governance and Employment **(Tel: 0191 643 5329)**

Wards affected: **All**

PART 1

1.1 Purpose:

This report seeks Cabinet's approval of an updated Covert Surveillance Policy. In accordance with the Codes of Practice applying to the Regulation of Investigatory Powers Act 2000 (RIPA) the Council Policy should be reviewed annually. A copy of the revised draft Policy is attached at Appendix 1.

1.2 Recommendation(s):

It is recommended that Cabinet:

1. Approve the Authority's draft Policy on Covert Surveillance (attached at Appendix 1);
2. Review and note the use of surveillance by the Authority in the preceding year; and
3. Note the further regulation of the use of surveillance by local authorities from 1 November 2012.

1.3 Forward plan:

This item is listed on the Forward Plan published on 10 October 2012.

1.4 Council plan and policy framework

There is no reference in the Council Plan to this item of business.

1.5 Information:

1.5.1 Introduction

A Surveillance Policy was approved by Cabinet in June 2011 and is subject to annual review. The Policy has been revised to reflect the changes to the RIPA regime brought about as a result of the Protection of Freedoms Act 2012 and also the requirement for any surveillance to be linked to serious crime. The draft policy is attached at Appendix 1.

The aims of the Authority's Policy are to:

- Set out the Authority's arrangements for complying with RIPA; the relevant Codes of Practice and guidance issued by the Home Office; and guidance from the Office of the Surveillance Commissioner (OSC) and the Interception of Communications Commissioner's Office (IOCCO);

- Give effect to the rights of citizens to respect for their private and family lives (pursuant to the Human Rights Act 1998); and

- Protect the Authority from legal challenge when undertaking surveillance.

1.5.2 The RIPA Shield

The Regulation of Investigatory Powers Act 2000 (RIPA) puts covert surveillance on a statutory basis. RIPA enables certain public authorities to carry out surveillance operations with statutory protection from legal challenge. It is often referred to as the "RIPA shield".

Three covert investigatory techniques are available to local authorities under RIPA:

i. the acquisition and disclosure of communications data such as telephone billing information or subscriber details e.g. to tackle target rogue traders;
ii. directed surveillance - covert surveillance of individuals in public places e.g. to tackle criminal activity arising from anti social behaviour; and
iii. covert human intelligence sources (CHIS) such as the deployment of undercover officers.

Local authorities may only use RIPA provisions to authorise surveillance activities in order to detect and prevent serious crime.

Local authorities may undertake surveillance for other purposes but such surveillance will not benefit from the RIPA shield and will leave a local authority more vulnerable to challenge. For this reason all surveillance activity undertaken by the Authority must be appropriately authorised and subject to central monitoring.

1.5.3 Central Register

The Authority has a Central Register of all RIPA and non-RIPA surveillance activity. It is important that staff across all Directorates of the Authority are aware of the need to obtain authorisation prior to undertaking surveillance and for relevant information to be fed into the Central Register.

1.5.4 Inspection

Organisations using RIPA are subject to regular inspection by:

1. The Office of Surveillance Commissioners (OSC); and
2. The Interception of Communications Commissioner's Office (IOCCO).

The Authority received an inspection visit from the OSC in April 2010. The purpose of the OSC inspection was to examine policies, procedures, operations and administration in relation to directed surveillance and covert human intelligence sources. All of the issues identified through the inspection process were incorporated into the Policy that was approved by Cabinet in June 2010.

The Authority received an inspection visit by the IOCCO on 23 May 2011. The outcome of this inspection was not available when the Cabinet considered the policy in June 2011. The outcome of the inspection was received later that year and no issues identified through the inspection process have been required to be incorporated into the draft policy attached to this report.

1.5.5 Summary of Use of Surveillance, Acquisition of Communications Data and CHIS

Between 1st April 2011 and 31 March 2012, the Authority used the RIPA directed surveillance provisions on 8 occasions. All the authorisations related to investigations of instances of anti social behaviour, through the use of covert cameras. The purpose of the authorisations was to gather evidence (including the identification of perpetrators) for use in criminal and anti-social behaviour proceedings. On these occasions no criminal or anti-social behaviour proceedings were brought from the evidence gathered. All these authorisations have come to an end.

Between 1 April 2011 and 31 March 2012 the Authority has acquired communications data on 3 occasions. The acquisitions related to telephone subscriber information connected to investigations undertaken by the Trading Standards team. Information obtained has subsequently supported court proceedings and sharing of intelligence with other local authorities.

The Authority has not used the covert human intelligence source (CHIS) provisions. The Policy requires that if the use of a CHIS is being contemplated, the officers concerned should seek appropriate advice from Legal Services and from other organisations that more commonly use CHIS, such as the Police. Approval for the use of a CHIS can only be given by the Head of Paid Service.

The Senior Responsible Officer will keep the Central Register under review and will advise Authorising Officers/Designated Persons of changes in approach or procedure.

1.5.6 Corporate Responsibilities

The Codes of Practice advise that a Senior Responsible Officer (SRO) should be nominated to ensure the Authority has appropriate policies and processes that accord with RIPA and the related Codes of Practice.

The Officer Delegation Scheme places the Senior Responsible Officer role with the Head of Legal, Governance and Commercial Services.

Each Strategic Director and Head of Service is responsible for ensuring effective and legally compliant systems and procedures are in place for surveillance work within their Directorates and Service Areas.

All employees connected with surveillance and handling of evidence are responsible for ensuring that they act only in accordance with their level of responsibility and training and in accordance with this Policy and associated documents. To assist in this an Authority 'Employee Handbook: Use of Covert Surveillance, Covert Human Intelligence Sources and Communications Data', has been prepared. The Handbook provides key information for officers and directs them towards key sources of detailed guidance. It will be kept under review and revised as necessary to ensure it reflects current procedures and best practice.

If Officers wish to undertake surveillance that falls outside of the RIPA regime they must take legal advice and seek appropriate authorisation. Information regarding surveillance (whether under RIPA or not) must be held centrally by the Senior Responsible Officer to enable the Authority to have an overview of all surveillance activities being undertaken by the Authority. Between 1 April 2011 and 31 March 2012, no authorisations have been sought or approved for surveillance that falls outside of the RIPA regime.

1.5.7 Compliance and Oversight

The Codes of Practice indicate that elected members of a local authority should review its use of RIPA and set the general surveillance policy at least annually. A local authority should also consider internal reports on the use of RIPA at least quarterly to ensure that it is being used consistently in compliance with the Authority's Policy and that the Policy remains fit for purpose.

To meet these requirements the Policy Statement provides that:

- Cabinet receives an annual report covering the Authority's use of RIPA powers, and review of the Policy for the following year;
- Quarterly reports are presented to the Regulation and Review Committee on the Authority's use of RIPA powers. The Committee's role is to look at compliance, oversight and use of RIPA. The Committee will also consider whether the Policy remains fit for purpose and recommend changes to the Policy as appropriate for Cabinet's consideration; and
- The Cabinet Member with responsibility for RIPA related activities will receive regular updates from the Senior Responsible Officer regarding the use of the Authority's powers.

In addition to the above, the Authority's Internal Audit Service is currently undertaking an audit of "Investigatory Powers, CCTV Surveillance and Security Arrangements". This audit is being undertaken in accordance with the agreed 2012/13 Internal Audit Plan. The outcome of the internal audit is awaited.

1.5.8 Closed Circuit Television (CCTV) Systems

North Tyneside Council's CCTV control room operates cameras throughout the Borough. Overt surveillance as conducted through the use of CCTV is covered by the Data Protection Act 1998 and not by RIPA. Signage is in place informing the public when they enter zones covered by CCTV equipment. The Authority's CCTV control room is registered with the Information Commissioner under the Data Protection Act 1988.

If the CCTV cameras are used for covert surveillance (whether by the Authority or the Police), a RIPA authorisation is required. The Police may make formal written requests for surveillance of a target for which they have a RIPA authorisation. The CCTV Control Room Co-ordinator will seek written confirmation of this authorisation.

1.5.9 Protection of Freedoms Act and Additional Controls on Surveillance

Prior to the 2010 general election the coalition parties indicated an intention to revise local authority surveillance powers. Concerns were raised abut the proliferation of CCTV cameras without assessment or consultation and that surveillance was being used in a disproportionate manner to investigate minor offences.

In accordance with the provisions contained in the Protection of Freedoms Act 2012 the Authority's policy and procedures have been revised.

The Protection of Freedoms Act 2012 makes provision for the following:

1. Further regulation of CCTV, Automatic Number Plate Recognition (ANPR) and other surveillance camera technology operated by the police and local authorities.

   CCTV is already subject to controls under both the Data Protection Act and if used covertly, RIPA. CCTV is already subject to a Code of Practice under the Data Protection Act which is enforced by the Information Commissioner.

   Under the new provisions the Secretary of State will be required to publish a Code of Practice for the use of surveillance camera systems and to appoint a Surveillance Camera Commissioner to monitor the operation of the code. The Code of Practice must contain guidance on the development or use of surveillance camera systems and the use or processing of images or information obtained through such systems.

2. A requirement for local authorities to obtain judicial approval for the use of any one of the three covert investigatory techniques available to them under the Regulation of Investigatory Powers Act 2000 (RIPA).

   In addition to obtaining authorisation from an Authorising Officer within the Authority further approval must be sought from a Justice of the Peace prior to undertaking the activity. This is similar to the current process for applying for search warrants.

1.5.10 Serious Offence Test

Before 1 November 2012 local authorities had the following ground to authorise directed surveillance; where it was necessary "for the purpose of preventing or detecting crime or preventing disorder."

From 1 November 2012, local authorities may only use the RIPA provisions to authorise surveillance activities in order to detect and prevent crime as defined by the Regulations and not to prevent disorder.

In particular the crime which is sought to be prevented or detected by the surveillance activity must be punishable, whether on summary conviction or on indictment, by a maximum term of **at least 6 months of imprisonment**, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.

The removal of the prevention of disorder as part of the ground to authorise directed surveillance is likely to mean a reduction in the number of authorisations that the Authority seeks to make in the future.

1.6 Decision options:

Option 1

Cabinet may:

1. Approve the Authority's Policy on Covert Surveillance (attached as Appendix 1);

2. Review and note the use of surveillance by the Authority in the preceding year; and

3. Note the changes to the use of surveillance by local authorities.

Option 1 is the recommended option.

Option 2

Cabinet may ask Officers to revise the draft Policy and/or provide additional information regarding any matters contained in the report.

1.7 Reasons for recommended option:

Approving the Authority's Policy on Covert Surveillance will secure adherence to the recommended best practice contained within the Codes of Practice. In particular, paragraph 3.30 of the Code of Practice – Covert Surveillance and Property Interference indicates that elected members should review the Authority's use of Part II of the Regulation of Investigatory Powers Act 2000 and set the policy at least once a year.

1.8 Appendices:

Appendix 1: Authority Policy on Covert Surveillance (draft)

1.9 Contact officers:

Stephen Ballantyne, Lawyer Specialist – Governance and Employment (0191 643 5329)
Alison Campbell, Finance Business Manager (0191 643 7038)

1.10 Background information:

The following background papers/information have been used in the compilation of this report and are available at the office of the author:

- Regulation of Investigatory Powers Act 2000 and relevant Orders
- Code of Practice - Covert Surveillance and Property Interference
- Code of Practice - Covert Human Intelligence Sources
- Code of Practice - Acquisition and Disclosure of Communications Data
- Protection of Freedoms Act 2012

PART 2 – COMPLIANCE WITH PRINCIPLES OF DECISION MAKING

2.1 Finance and other resources

The provisions of the Policy can be implemented within the Service's existing resources.

2.2 Legal

The Policy has been prepared with reference to the relevant law and Codes of Practice. A number of Statutory Instruments and Codes of Practice published by the Home Office that govern the operation of RIPA.

The Authority may only authorise directed surveillance where it is both necessary and proportionate to the investigation or operation being undertaken and to what is being sought to achieve in terms of evidence gathering. Senior Officers are appointed as Authorising Officers and have a key role in carefully scrutinising all applications for the use of RIPA powers under a specific authorisation.

Authorising Officers must ensure that authorisations are granted only in appropriate cases and that the extent of all authorisations are clearly set out.

The Authority cannot authorise intrusive surveillance under RIPA. Intrusive surveillance would involve placing an investigator on residential premises or in a private vehicle or allowing the use of an external surveillance device outside of the premises or vehicle that gives the same quality of information as if it was on the premises or in the vehicle.

The Policy, together with the Employee Handbook covers the procedures to be followed in seeking authorisations, maintaining appropriate oversight of the Policy and the central record of decisions.

2.3 Consultation/community engagement

The Policy is aimed at ensuring adherence to the best practice contained within the Codes of Practice and feedback from the Office of Surveillance Commissioners and the Interception of Communications Commissioner's Office as well as the law.

Internal consultation has taken place with officers with responsibility for the management and supervision of surveillance activity as well as the Cabinet Member for Community and Regulatory Services and the Regulation and Review Committee.

2.4 Human rights

Human rights implications are addressed within the report and the Policy. RIPA provides a framework under which surveillance activity can be authorised and conducted in a way that is compatible with the rights of individuals.

The Authority must also ensure that activity that falls outside of the RIPA regime is subject to careful scrutiny and authorisation to ensure that human rights are respected and the activity is lawfully undertaken.

2.5 Equalities and diversity

There are no equalities and diversity implications directly arising from the report.

2.6 Risk management

The Authority's Policy and the procedures contained in the Employee Handbook are designed to ensure the Authority complies with the law and Codes of Practice and thereby reduce the risks associated with surveillance activity.

2.7 Crime and disorder

RIPA may only be utilised by the Authority for the purposes of detecting and preventing crime.

2.8 Environment and sustainability

There are no environment and sustainability implications directly arising from this report.

PART 3 - SIGN OFF

• Chief Executive	X
• Mayor/Cabinet Member(s)	X
• Chief Finance Officer	X
• Monitoring Officer	X
• Strategic Manager for Policy and Partnerships	X