Leeds CITY COUNCIL

Originator: M. J. Turnbull

Tel: 2474408

Report of the Director of Environment and Neighbourhoods

Corporate Governance & Audit Committee

Date: 24 January 2011

Subject: RIPA Policy and Quarterly Reports

Electoral Wards Affected:	**Specific Implications For:**
	Equality and Diversity ☐
	Community Cohesion ☐
☐ Ward Members consulted (referred to in report)	Narrowing the Gap ☐

Executive Summary

The Regulation of Investigatory Powers Act 2000 (RIPA) is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with when the law permits and there is a clear public interest justification.

This report provides Members with information about the recent use of authorisations for covert (directed) surveillance. This report also advises Members of the conclusions and recommendations in the latest Office of Surveillance Commissioners Inspection Report, arising from an inspection of the Council's arrangements for authorising surveillance of this nature. This report also advises Members of the outcome of an inspection by the Interception of Communications Commissioner's Office in relation to the acquisition of communications data, and the action plan which is needed. This report also contains proposals for changes to the Council's RIPA policy which was approved by Executive Board in August 2010, so that the policy covers the acquisition of communications data, as well as covert surveillance.

1.0 Purpose of the Report

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with when the law permits and where there is a clear public interest justification.

1.2 The Covert Surveillance and Property Interference Revised Code of Practice provides that elected Members "should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on the use of the 2000 Act on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose". At the August 2010 Executive Board, the Board agreed a RIPA policy, which provides that the policy will be reviewed on an annual basis, and that reports on use will be provided on an annual basis, in each case by Corporate Governance and Audit Committee. This report advises Members about the recent use of directed surveillance.

1.3 This report also advises Members about the outcome of the latest Office of Surveillance Commissioners (OSC) Inspection Report, in relation to the use of directed surveillance, and also the outcome of an inspection by the Interception of Communications Commissioner's Office in relation to the acquisition of communications data.

1.4 There are also proposals for consequential changes to the Council's RIPA policy, and subject to the views of the Committee, the revised policy will then be submitted to Executive Board, for approval. As the RIPA policy is not part of the Policy Framework as specified in the Council's Constitution, it falls to be approved by Executive Board.

2.0 Background

2.1 RIPA provides an authorisation process for certain types of surveillance and information gathering, and that process can be used as a defence against human rights claims. At present, the Council is entitled to authorise its own directed surveillance under RIPA, and the Council's RIPA policy contains a number of safeguards against the over-use of authorisations.

2.2 The RIPA policy provides that the policy will be reviewed on an annual basis, and that reports on the use of authorisations will be considered on a quarterly basis, in each case by Corporate Governance and Audit Committee.

2.3 The RIPA policy was approved by Executive Board in August 2010, and there have been no applications for directed surveillance authorisations since then. Indeed, there has been only one such application since the new arrangements were introduced in April 2010, and whilst the operation in question was authorised, it did not in fact take place. The application concerned the use of an Environmental Analyser to trace, record and analyse sound levels in a noise nuisance investigation, where the case history demonstrated this was the last available option which remained open to the Council. However, all relevant services have been notified formally about the current arrangements, and corporate guidance which includes the RIPA policy is available on both the intranet and the on the Council's website. The drastic reduction in the number of applications since last April has been raised formally with the Director of Environment & Neighbourhoods, given that the Anti-Social Behaviour Unit, and Health and Environmental Action Service were previously

the main users of covert surveillance. He has confirmed that he is satisfied the reduction simply reflects the new RIPA policy, and the clear presumption in favour of overt practices.

2.4 The Council is inspected periodically by the OSC, the regulator for directed surveillance, and the latest inspection was on 14 October 2010. The report concluded that there was now "a thoroughly competent system" governing the Council's use of covert surveillance, and commended officers for "excellent work" in relation to the corporate guidance and procedure document, and in relation to training materials. The report also commended the Assistant Chief Executive (Corporate Governance) for her "well-informed and forceful leadership" on RIPA issues. The report made only 3 minor recommendations in relation to the corporate guidance, the directed surveillance application form, and future training respectively, all of which are acceptable and have now been implemented.

2.5 The Council has also received its first inspection by Interception of Communications Commissioner's Office (IOCCO). RIPA permits local authorities to acquire certain subscriber information about phone number and e-mail account holders, in particular the name and billing address of a subscriber (but not the content of any communication). In order to acquire such information, there must be a formal application to the provider of the service, and again there are a number of statutory safeguards. In particular, the Council can only use these powers for the purpose of preventing or detecting crime or of preventing disorder, and the person who authorises their use (the designated person) can only do so if they believe this is necessary and proportionate to what is sought to be achieved by acquiring the data. In addition, the relevant Code of Practice provides that in order to use these powers, a public authority must have an accredited single point of contact (SPoC). To become accredited, an individual must complete a specified course of training and have been issued with a SPoC personal identification number. Details of all accredited individuals are made available to communications service providers for authentication purposes.

2.6 To date, the only service which has made use of these powers is the Health and Environmental Action Service. The Service makes occasional use of these powers as part of their investigations into environmental enforcement, in particular when the only lead available is an advertised phone number or web site address. The Service uses these powers infrequently, and has issued only seventeen notices to communications service providers since June 2007. The Service has confirmed these powers are only used for the purpose of investigating serious incidents, and that overt surveillance is the "default position", with covert methods only being used if the required information cannot be obtained by overt means.

2.6 As the Service uses the powers to acquire communications data only infrequently, it was considered more cost-effective for the Service to outsource the role of single point of contact (SPoC), and to pay for applications to be considered on an ad hoc basis. A supplier was identified to advise on whether data requests appeared to comply with the requirements of RIPA, and the supplier gave contractual assurances to the Service that it carried out its activities in line with good industry practice. This outsourcing of the SPoC role avoided the cost of training and accrediting officers to SPoC standards for these purposes. Unfortunately, the IOCCO inspector concluded that the applications were generally completed to a poor standard, and did not sufficiently justify the principles of necessity and proportionality. The inspector was not satisfied that the company to whom the Service had outsourced the SPoC role, was fulfilling its roles and responsibilities in the Code of Practice, or that it was

advising applicants or the designated person appropriately, or ensuring that the Council acted in an informed and lawful manner.

2.7 The IOCCO inspector made a number of recommendations in his report, in particular in relation to considering the use of the SPoC facility provided by the National Anti-Fraud Network (NAFN), maintaining a proper audit trail of applications and a central record, guarding against the supply of excess data, reviewing who should act as designated person and as Senior Responsible Officer, evidencing properly that necessity and proportionality have been considered, and the proper recording of errors.

2.8 The Service has urgently reviewed its use of these powers, and applications for communications data were suspended when the report was issued. An action plan to implement the recommendations in the IOCCO report has been agreed by the Chief Officer (Health & Environmental Action Services), and by the Assistant Chief Executive (Corporate Governance). This action plan has been submitted to IOCCO, and they have confirmed that they regard this as a "comprehensive response" from the Council. The Council has given a commitment to IOCCO to implement all items in the action plan by February/March.

2.9 The purpose of the action plan is to create a robust system which will govern the use of these powers. To a great extent, this system will mirror the system governing the use of covert surveillance. The new system will therefore provide this Committee with the assurances it needs that appropriate controls are in place, and that the Council is using these powers where this is necessary and proportionate.

2.10 In particular, the action plan provides for full training to be provided to specified applicants, the designated person, and senior responsible officer, the discontinuation of services from the previous company, the receipt of proposals from NAFN, the setting up of a comprehensive central record, changes to the role of designated person and senior responsible officer, and the proper recording of recordable errors. In addition, the role of designated officer will be raised to Head of Service level as a minimum, or in their absence the Chief Officer, and the Senior Responsible Officer who will have responsibility for the integrity of system will be Nicole Jackson, Assistant Chief Executive (Corporate Governance).

3.0 Main Issues

3.1 It is proposed that the Council's RIPA policy should be amended to reflect current practice within Environment & Neighbourhoods in relation to the acquisition of communications data, and also to reflect the commitments given by the Council in its response to the IOCCO report.

3.2 A proposed revised policy is set out in Appendix 1. The proposed changes to the current policy are shown underlined in italics.

3.3 The policy should ensure that all of these powers under RIPA, whether in relation to directed surveillance or the acquisition of communications data, are only used in a balanced and proportionate way in serious and/or persistent cases, where overt methods are not appropriate, or where overt methods have been used and have failed.

4.0 Implications for Council Policy and Governance

4.1 The Codes of Practice mentioned above must be taken into account by the courts, and by the OSC/IOCCO respectively when carrying out inspections. The Council can be required to justify, with regard to the Codes, the use or granting of authorisations and notices generally. The current system governing the use of directed surveillance, and the system to be established for governing acquisition of communications data will provide this Committee with the necessary assurances that the Council has appropriate controls over the use of RIPA powers, and that the use of these powers is compliant with the legislation and relevant Codes of Practice.

4.2 The terms of reference of Corporate Governance and Audit Committee include the review of the "adequacy of policies and practices to ensure compliance with statutory and other guidance". It is therefore proposed that periodic reports on the use of RIPA should also include the use of the powers to acquire communications data.

4.3 Officers will check the Officer Delegation Scheme (Executive Functions) to see if any consequential changes need to be made to the Scheme, arising from the revised policy.

4.4 For the reasons mentioned above, the proposed policy will need to be approved by Executive Board.

5.0 Legal and Resource Implications

5.1 The legal implications of the proposals in this report, are as set out above.

5.2 The resource implication is that notices and authorisations in relation to communications data are proposed to be dealt with at a more senior level, and an overview of the arrangements for acquiring communications data is proposed by the Assistant Chief Executive (Corporate Governance). It is understood that the Council is already a subscriber to NAFN, and enquiries are being made with NAFN to establish whether the provision of SPoC services by NAFN will require any additional payment.

6.0 Conclusions

6.1 The Council needs to adopt a clear policy about the use of RIPA authorisations, whether in relation to covert surveillance or the acquisition of communications data, to the effect that they will only be granted in serious cases, after overt methods have been considered, and that there will be a demonstrable balance between the impact of the surveillance proposed, and the gravity and extent of the perceived crime or disorder.

7.0 Recommendation

7.1 Members are requested to comment on the revised draft policy prior to consideration by Executive Board.

7.2 Members are asked to note the outcomes of the OSC inspection report, and the IOCCO inspection report, and in relation to the latter to note that an appropriate action plan has been agreed.

Background Documents

- OSC Inspection Report
- IOCCO Inspection report
- RIPA 2000

Appendix 1

Draft Revised Regulation of Investigatory Powers Act 2000 (RIPA) Policy

1.0 Extent

This policy applies to the authorisation of directed surveillance under Section 28(1) of RIPA. *This policy also applies to authorisations and notices for the purposes of obtaining communications data, under Section 22(3) and 22(4) of RIPA.* This policy does not cover the authorisation of covert human intelligence sources under Section 29 of RIPA, nor does this policy cover intrusive surveillance (which the Council is not entitled to authorise under RIPA).

2.0 Safeguards

2.1 The Council will apply a presumption in favour of overt investigation methods. The Council will always consider using a variety of overt investigatory tools, *before considering whether the use of these powers is required*. Covert surveillance or investigation will be used only when other reasonable options have been considered, and ruled out.

3.0 Covert Surveillance

3.1 In order to comply with the duties in Section 28(2) of RIPA, that a person shall not grant an authorisation for the carrying out of directed surveillance unless they believe that the authorisation is "necessary" on the ground of preventing or detecting crime or preventing disorder, and in accordance with the Covert Surveillance and Property Interference Revised Code of Practice, the Council will

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence, or disorder;
- explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.2 The Council will only use covert surveillance when the problem is serious and/or persistent, and where overt surveillance would not provide evidence and/or might displace the problem elsewhere.

3.3 *The Council will use covert surveillance proportionately*, and will not use covert surveillance to address minor matters, but instead will focus on those issues which are of greatest concern to the community, namely environmental damage such as flytipping and graffiti, and anti-social behaviour where individuals or families are targeted or threatened.

3.4 The Council will only use covert surveillance either to obtain evidence that can be presented at court, or where another positive outcome relating to the prevention or

detection of crime or the prevention of disorder has been identified, for example through the positive identification of perpetrators.

3.5 The Council will give responsibilities to a single member of its Corporate Leadership Team, Nicole Jackson, Assistant Chief Executive (Corporate Governance) to ensure that designated authorising officers meet the standards required by the Office of Surveillance Commissioners.

3.6 The Council will ensure that the quality of authorisations is monitored by Legal, Licensing and Registration Services.

3.7 The Council will ensure applicants and authorising officers receive an appropriate level of training.

3.8 The Council will ensure that in accordance with The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, authorisations will only be granted by Directors. This will avoid any perception that authorising officers are directly involved with the investigations they authorise. Authorising officers will therefore be able to apply more independently reasoned judgment of the issues.

4.0 Acquisition of Communications Data

4.1 *In order to comply with the duties in Section 22(1) and 22(5) of RIPA that a designated person will not grant an authorisation or give a notice for the acquisition of communications data unless they believe this is "necessary" for the purpose of preventing or detecting crime or for preventing disorder, and "proportionate" to what is sought to be achieved, the Council will balance the extent of the intrusiveness of the interference with an individual's right to respect for their private life against a specific benefit to the investigation or operation being undertaken by the Council in the public interest.*

4.2 *The Council will only use powers to acquire communications data when investigating serious incidents, (such as vehicles causing nuisance within communities, and illegal advertising) and where overt investigation methods would not provide the necessary evidence.*

4.3 *In accordance with the Acquisition and Disclosure of Communications Data Code of Practice, the Council will appoint a senior responsible officer, who will be responsible for the integrity of the process within the Council to acquire communications data, compliance with the relevant provisions of RIPA and the Code, oversight of the reporting of errors to IOCCO and the identification of both the cause of errors and the implementation of processes to minimise the repetition of errors, engagement with IOCCO inspectors, and overseeing the implementation of post inspection action plans. The senior responsible officer will be Nicole Jackson, Assistant Chief Executive (Corporate Governance).*

4.4 *The Council will ensure that the quality of notices and authorisations is monitored by Legal, Licensing and Registration Services.*

4.5 *The Council will ensure applicants, the designated person, and the senior responsible officer receive an appropriate level of training.*

4.6 *The Council will ensure that in accordance with The Regulation of Investigatory Powers (Communications Data) Order 2010, the designated person will be a*

“Director, Head of Service, Service Manager or equivalent”, or someone in a more senior position. The Council will ensure the designated person is at Head of Service level as a minimum.

5.0 Review

5.1 This policy will be reviewed on an annual basis, and *reports on the use of these RIPA powers* will be considered on a quarterly basis, in each case by Corporate Governance and Audit Committee.