CHESHIRE EAST COUNCIL

AUDIT AND GOVERNANCE COMMITTEE

Date of Meeting:	27th March 2014
Report of:	Compliance and Customer Relations Manager
Subject/Title:	Compliance with Regulation of Investigatory Powers Act (2000) (RIPA) and Protection of Freedoms Act (2012)
Portfolio Holder:	Councillor David Brown

1.0 Report Summary

1.1 This report provides an update on how the Council has complied with RIPA legislation during 2013/14 and the number of RIPA applications which have been authorised.

2.0 Decision Requested

2.1 That the Committee notes the contents of the report in respect of the numbers of applications and the current arrangements in place to ensure the Council complies with the legislation.

3.0 Reasons for Recommendations

3.1 In order to form an opinion on the Council's compliance with this legislation, the Audit and Governance Committee needs to gain assurance that there are effective arrangements in place to record, coordinate and authorise requests for directed surveillance and that the Council complies fully with the requirements of RIPA legislation in so doing.

4.0 Wards Affected

4.1 All wards.

5.0 Local Ward Members

5.1 Not applicable.

6.0 Policy Implications including - Carbon reduction - Health

6.1 Using RIPA powers can conflict with an individual's human rights and so it is imperative that, when investigating alleged wrongdoing, certain conditions are met in each case, in order that successful prosecutions can be made.

6.2 By following the authorisation procedures set out in RIPA legislation and outlined in the Council's Policy and Procedures (Surveillance under the Regulation of Investigatory Powers Act 2000 – Policy and Procedures –

1st November 2012), officers are demonstrating that the surveillance is necessary for a purpose permitted by the Human Rights Act 1998 and that it is a proportionate measure to take, given all the circumstances.

7.0 Financial Implications

7.1 Failure to comply with the legislation can lead to the Office of the Surveillance Commissioner withdrawing the Council's ability to conduct directed surveillance for a period of time, which would then result in a follow up inspection. This would have a detrimental impact on the Council's ability to carry out investigations. There could also be fines imposed if the Council was found to be illegally breaching someone's Human Rights.

8.0 Legal Implications

8.1 The Regulation of Investigatory Powers Act 2000 was enacted to consolidate and update a range of law enforcement investigative powers, to ensure that these powers were fit for purpose, as well as compliant with the UK's obligations under the European Convention on Human Rights. A number of codes of practice have also been issued under this Act.

8.2 The Protection of Freedoms Act 2012, introduced additional safeguards in respect of certain surveillance undertaken under RIPA 2000 by local authorities. These safeguards include a requirement for local authorities to obtain Magistrate approval of the use of RIPA 2000 powers in certain instances.

8.3 Given the possible infringement of peoples Human Rights when using these powers, it is important that the Council complies fully with the law and it's own policy and that it reflects on it's use of these powers to ensure it is proportionate at all times.

9.0 Risk Management

9.1 The impact on the Council of not complying with the legislation would be significant, as identified above in 7.1.

10.0 Background and Options

The Regulation of Investigatory Powers Act (RIPA) provides a regulatory framework to enable public authorities to obtain information through the use of certain covert investigatory techniques. The Protection of Freedoms Act, which came into force on 1st November, 2012, requires public authorities to acquire judicial approval to use covert surveillance techniques. It also restricts the use of surveillance to the investigation of offences which attract a custodial sentence of six months or more.

10.1 Compliance with RIPA Legislation

The Council will, on occasion, need to use directed surveillance in order to carry out its enforcement functions effectively, e.g. benefit fraud, planning enforcement, licensing enforcement, trading standards, environmental health

and community safety investigations. Directed surveillance is essentially covert surveillance in places open to the public. Using RIPA powers can conflict with an individual's human rights, and so it is imperative that, when investigating alleged wrongdoing, certain conditions are met in each case, in order that successful prosecutions can be made. In particular, RIPA requires that covert techniques are only used when it is necessary and proportionate to do so. All covert surveillance must be properly authorised and recorded, the tests of necessity and proportionality must be satisfied, and the potential for collateral intrusion must be considered and minimised.

All applications must be authorised by an Authorising Officer. The Authorising Officers for the Council are:

Chief Executive
Chief Operating Officer
Executive Director of Strategic Commissioning
Director of Public Health
Director of Children's Services
Director of Adult Social Care and Independent Living
Head of Service – Early Help and Protection
Head of Organisational Development

Once authorised, all applications need the approval of a Justice of the Peace/Magistrate. The investigating officer makes arrangements to meet the magistrate in person at the court. Surveillance cannot take place until the application has been granted.

The Monitoring Officer assumes responsibility for the integrity of the process and procedures to ensure that the Council complies with the requirements of the legislation.

10.2 Access to Communications Data – use of National Anti Fraud Network

The Regulation of Investigatory Powers (Communications Data) Order 2010 currently sets out which organisations can access communications data and for what purposes. The Council is limited to accessing only service user and subscriber data i.e. the 'who', 'when' and 'where' of a communication but not the actual content. The Council is required to nominate a Single Point of Contact (SPOC), who needs to be an accredited person, to ensure that data is obtained lawfully and to facilitate access to the data with the communications service providers. The SPOC may be an employee of the Council or an externally appointed person. The Council has been using the SPOC service provided by the National Anti-Fraud Network (NAFN) since 25 October 2012 and this process has run smoothly.

10.3 Numbers of applications authorised

	Directed Surveillance	Communications Data
2009-2010	1	0
2010-2011	8	1
2011-2012	7	2
2012-2013	15	3
2013-2014 to date	7	3

The apparent rise in applications in 2012-2013 includes five renewals of existing investigations that have been entered in the central register as new applications.

10.4 Inspections

The Office of the Surveillance Commissioners is responsible for inspecting the Council's use of and compliance with RIPA Legislation and the Council was last inspected on 2nd May 2013.

The Inspector's Report was very positive about the Council's use of RIPA, but also included some recommendations about how the standards might be improved further (see Appendix 1). These recommendations have been implemented and the RIPA Policy is currently being revised to reflect these changes.

The Interception of Communications Commissioner's Office is responsible for inspecting applications to access communications data, and this took place on 3rd-5th June, 2013. However, the inspection was carried out on NAFN, rather than on the Council.

11.0 Access to Information

11.1 The background papers relating to this report can be inspected by contacting the report writer:

Sandra Smith
Compliance and Customer Relations Manager
01270 685865
sandra.smith@cheshireeast.gov.uk

APPENDIX 1

RIPA INSPECTION – 2.5.13

Comments

1. Excellent training regime

2. All staff involved in inspection were receptive to constructive comment and approached the inspection in a most positive, courteous and cooperative manner.

3. Policy and procedures, training documentation and CCTV Policies and Protocols provide an extremely helpful and comprehensive policy and guidance regime for practitioners.

4. Privacy Risk Assessments are an example of good practice.

5. Review Panel process – whereby applications and authorisations are quality assured – is to be commended, as is the process by which the Senior Responsible Officer (Monitoring Officer) oversees the Central Record, and can be involved in rectifying mistakes/failings by applicants and Authorising Officers.

Recommendations

1. Policy and guidance documents to include guidance on the use of social networking sites and the internet.

2. CCTV Code of Practice and Protocol for use of CCTV in Covert Policing – both documents should explain the process by which the relevant details of an authorisation are made available to staff in the CCTV Control Room.

3. Central Record of Authorisations – more details to be included regarding the names of the Magistrate and the Officers at the hearing, the outcome of the hearing and any amendments to the authorisation.

4. Application Forms – some general recommendations made regarding improvements to the completion of forms by applicants and Authorising Officers.