Body:	**Cabinet**
Date:	**19 March 2014**
Subject:	**Eastbourne Borough Council's use of its powers under the Regulation of Investigatory Powers Act 2000 ('RIPA') as amended by the Protection of Freedoms Act 2012 ('POFA') and associated legislation**
Report of:	**Julian Osgathorpe, Deputy Chief Executive**
Ward(s)	All
Purpose	(1) To report on the authority's recourse to the its powers available under RIPA and associated legislation during the 2013 calendar year (2) To ask Cabinet to approve the adoption of a policy on the acquisition and use of communications data which brings the authority's approach into line with that on covert surveillance.
Recommendation:	(1) That Members note the results of the yearly RIPA review, and of the authority's recourse to RIPA regulated surveillance during the 2013 calendar year. (2) That Members adopt a policy on communications data which brings this authority's approach to those powers in line with the 'last resort' approach to all types of covert surveillance (3) That Members give authority to the Lawyer to the Council to a) incorporate such amendments to the policies of this authority on both surveillance and communications data which are necessary to ensure that it is up to date and accords with the law and b) to continue to review the authority's procedures, policies and training on RIPA related matters on an annual basis in consultation with the SRO for RIPA and the Cabinet portfolio holder.
Contact:	Victoria Simpson, Lawyer to the Council, Telephone 01323 415018 or internally on extension 5018. E-mail address: victoria.simpson@eastbourne.gov.uk

1.0 Background

1.1 Members are aware that RIPA supplies a statutory framework within which certain types of covert investigative tools may be lawfully used by public authorities for the purposes of enforcement as long as rigourous criteria are met and a set process followed. The latter includes amongst other things obtaining both internal approval at a senior level and also judicial approval before the measures are used.

1.2 The types of covert investigative tools covered by the RIPA regime include directed surveillance (essentially covert surveillance in places other than residential premises or private vehicles) as well as the use of a covert human intelligence source, or informant.

1.3 In addition, however, RIPA also regulates the interception of some types of communications data (the 'who', 'when' and 'where' of a communication, as opposed to the 'what' i.e. the content of what was said or written). While the interception of communications data is also covered by RIPA, it is subject to a separate overview and inspection regime by an entirely separate office: that of the Interception of Communications Commissioner.

1.4 Notably, local authorities may only authorise the acquisition of the two less intrusive types of communications data: service use (the type of the communication, time sent and its duration) and subscriber information (including billing information). Under no circumstances are local authorities empowered to obtain traffic data under RIPA, ie information about where the communications were made or received. Similarly, local authorities may not intercept the content of any person's communications and it is an offence to do so without lawful authority.

1.5 The last report to this Cabinet, in March 2013, noted the safeguarding measures incorporated into the Protection of Freedoms Act 2013 which aimed to constrain local authorities' recourse to RIPA-regulated surveillance. Some of those measures apply equally to communications data powers.

2.0 The Protection of Freedoms Act: safeguards applied to Communications Data powers

2.1 Since the Protection of Freedoms Act came into force, local authorities' powers relating to communications data must – like those relating to covert surveillance - be subjected both to an internal application process and also to the justices at the Magistrates' Court. The requirements for judicial approval are that the judicial authority is satisfied that at the time of the grant or renewal there were reasonable grounds for believing that the actions proposed were reasonable and proportionate and that these grounds still remain. Further conditions must be satisfied in relation to the authorisation or notice in that amongst other things the application is be made by the correct person using the process laid out by the statutory framework.

2.2 Although the requirement of judicial approval of a local authority authorisation or notice applies to applications to obtain communications data, there is no requirement that the "serious crime test" is met. This requirement that the offence being investigated is either punishable by a custodial sentence of six months or more or be concerned with the sale of alcohol or tobacco to a minor is to be applied only to directed surveillance and the use of a CHIS.

2.3 Members may have noted the introduction of a Communications Data Bill to Parliament in 2013. While this has yet to be enacted, it largely relates to the arrangements which communications providers may (or may not, depending on the outcome of the Bill) be required to put in place to enable enforcement authorities to access communications data more readily. It is not therefore dealt with in any detail here.

3.0 Eastbourne Borough Council's recourse to RIPA: the annual returns

3.1 In accordance with the relevant Codes of Practice, the Lawyer to the Council retains a central record of all RIPA applications and authorisations made by either this authority or by its investigative partners. Those records are held securely (although the redacted data thereon is freely available to people making FOI requests) and is reported quarterly to the Audit and Governance Committee in line with best practice.

3.2 The annual returns compiled for the period 1/1/2013 to 31/12/2013 include the following data:

RIPA applications for the use or conduct of a CHIS:
Nil applications made by EBC
Nil applications by partner organisations with which the authority is working on relevant matters

RIPA applications for authorised surveillance:
Nil applications made by EBC
Nil applications made by partner organisations with which the authority is working on relevant matters.

RIPA applications for the acquisition of communications data:
Nil applications made by EBC
Nil applications by partner organisations with which the authority is working on relevant matters

3.3 The 2013 returns show that Eastbourne Borough Council's historically low usage of RIPA continues across the full range of enforcement activities governed by this legislation.

3.3 This authority's arrangements in respect of covert surveillance remains subject to inspection by the Office of the Surveillance Commissioner, who inspected this authority and gave it a favourable report in June 2013. Notably, the Interception of Communications Commissioner (the ICCO') is an entirely separate inspectorate with responsibility for communications data. While the ICCO has not inspected this authority's arrangements at time of writing, it has responsibility for doing so across the range of enforcing authorities in much the same way as the OSC.

3.4 Both Commissioners report annually to Parliament and take a critical stance where they find inadequate policies and/or arrangements. In his most recent annual report, the ICCO noted various in those enforcement agencies which had recourse to their communications data powers. Where issues were noted

those appeared statistically more likely to come from authorities which did not rely on expertise from a third party to assist them in making communications data applications – hence the recommendation below.

4.0 This authority's arrangements in relation to communications data: a new policy alongside recourse to the National Anti-Fraud Network, or 'NAFN'

4.1 This authority's requirement of an annual audit of its RIPA policies, procedures and training was discharged by the Lawyer to the Council at the end of 2013 at the direction of the Senior Responsible Officer. In the context of a recent favourable write-up by the OSC of the authority's arrangements in relation to covert surveillance and the use of CHIS, and given the ongoing nil returns with regard recourse to surveillance powers, no substantive changes were considered necessary other than an updating of the resources available to enforcement officers and to information on the website.

4.2 It was however noted that – although this authority had not had recent recourse to its communications data powers – a formal policy on the acquisition and use of communications data would clarify matters. It was considered that a policy of 'last resort', which made provision for use of said powers only exceptionally and where stringent criteria were met, would be consistent with this authority's approach to the other powers available to it under RIPA. That policy is appended hereto and in the interest of clarity makes basic provision for relevant roles and accountabilities should this sort of activity be deemed necessary on exceptional grounds.

4.3 Four individual roles are required where local authorities seek to acquire communications data: the Applicant or investigator, who submits the application for communications data; the Designated Person, who objectively and independently considers the application; the Single Point of Contact, who is an accredited individual responsible for acquiring the data from the Communication Service provider and ensuring that the local authority acts in an informed and lawful manner, and the Senior Responsible Officer, who is responsible for the overall integrity of the process.

4.4 It was considered that the Deputy Chief Executive was best placed to act as the SRA, while the Monitoring Officer and Deputy Monitoring Officer would be best placed to act in the role of Designated Person: a role which has a parallel with that of Authorising Officer. That left the role of the Single Point of Contact, or SPoC, and as a result it is proposed that this authority use the services of the National Anti Fraud Network, or 'NAFN' if or when needed.

4.5 Like the majority of local authorities, this authority subscribes to NAFN: a not for profit organisation which provides advice and support across a range of enforcement areas. NAFN are in a position to provide assistance with applications to acquire communications data by acting as designated 'Single Point of Contact' for authorities at a nominal cost, thereby ensuring that consistency is achieved by those authorities who do not apply to the justices on a regular basis.

4.6 Reportedly 87% of local authorities used NAFN to perform the SPoC function in relation to communications data and as a result appear to have more

consistently achieved good practice. Recourse to NAFN has therefore been built into the 'last resort' policy - NAFN charge on a case by case basis and the likelihood is that there will be little recourse to this investigative tool.

5.0 Consultation

5.1 Consultation has taken place with the Senior Responsible Officer for RIPA and with the Cabinet portfolio officer.

6.0 Resource Implications

None

6.1 **Financial**

None

6.2 **Staffing**

None

7.0 Other Implications: Environmental, Human Rights, Community Safety, Youth, Anti-poverty.

7.1 None.

8.0 Conclusion

8.1 Since RIPA was first introduced in 2000, local authorities have had to put in place robust arrangements which ensure that they are seen to deploy the protection it offers only proportionally and in situations where doing so is adjudged to be strictly necessary according to rigorous criteria.

8.2 This authority's covert surveillance policy includes rigorous safeguards to ensure that this authority engages in RIPA-regulated activity only as a measure of last resort. Those arrangements were noted with approval by the Surveillance Commissioner when his inspector attended in June 2013. It is proposed to roll out that same approach to this authority's use of its communication data powers, and to ensure that – notwithstanding this authority's consistently low recourse to its powers under RIPA – the authority's arrangements continue to be reviewed and updated regularly. way.

JULIAN OSGATHORPE
DEPUTY CHIEF EXECUTIVE

Background Papers:

The Background Papers used in compiling this report were as follows:

- The Regulatory and Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- Reports to Cabinet on RIPA from 2008 to 2013
- Guidance issued by the Home Office and the Office of the Surveillance Commissioner, as well as the Interception of Communications Commissioner
- Annual Reports of the Office of the Surveillance Commissioner and the Interception of Communications Commissioner
- Other resources and guidance protected by copyright

To inspect or obtain copies of background papers please refer to the contact officer listed above.