

Annual review of the Regulation of Investigatory Powers Act 2000 (RIPA)

Portfolio Holder: Peter Seib, Finance and Legal Services
Director: Martin Woods, Director - Service Delivery
Lead Officer: Paula Goddard, Senior Legal Executive
Contact Details: Paula.goddard@southsomerset.gov.uk or 01935 462186

Reason for the Report

1. The Council must have arrangements in place to ensure compliance with the Regulation of Investigatory Powers Act 2000 (RIPA) and those arrangements are subject to inspection by the Office of Surveillance Commissioners (OSC). This is achieved through the adoption of a set of Policy and Procedures that ensure compliance with the requirements of the legislation. The Council has had arrangements and procedures in place for authorising and conducting necessary surveillance since 2002. Members should review the use of RIPA and set the policy at least once per year. They should also consider internal reports on use of RIPA periodically to ensure it is being used consistently with the policy and that the policy remains fit for purpose.

Recommendations

2. That District Executive:
 - a. notes the Council's use of RIPA powers;
 - b. approves and adopts the revised Regulation of Investigatory Powers Act 2000 Policy and Procedures attached at Appendix A along with the new Using Social Media and Networking Sites in Investigations Policy (Appendix 5);
 - c. appoints the Director of Service Delivery as Senior Responsible Officer and amendments to authorising officers are noted.

Background

3. RIPA provides a statutory mechanism to make sure that the way investigatory powers are used by organisations like councils and government departments complies with human rights law, in particular the European Convention on Human Rights.
4. As mentioned above the Council must have arrangements in place to ensure compliance and is subject to inspection by the (OSC).
5. RIPA was introduced in order to provide the correct balance between an individual's right to privacy under the Human Rights Act 1998 and the proper use of data and surveillance by public authorities, such as the police and local councils, who are entrusted by law to carry out certain enforcement duties. The Act identifies certain areas where carrying out these enforcement duties will inevitably conflict with individuals' rights to privacy. The main areas which are of concern to the Council are:
 - The use of directed surveillance ; and
 - The use of covert human intelligence sources (CHIS).

6. Some of the Council's activities necessarily require surveillance as part of their enforcement functions such as benefit fraud investigations, environmental, planning and licensing enforcement and other fraud investigations. However, the use of RIPA powers by the Council has been very limited (Appendix 1). This summary shows there have only been two authorisations sought since 2008 which reflects the fact that the powers are used very much as a "last resort" and other means of obtaining the necessary evidence are relied upon first.
7. The Council has had arrangements and procedures in place for authorising and conducting necessary surveillance since 2002; training for practitioners from relevant services and authorising officers has been provided and the current policy and procedures were adopted in October 2015 following changes in the legislation and a previous inspection.
8. In October 2014 the Office of Surveillance Commissioners carried out another routine inspection of the Council's arrangements for managing the use of RIPA authorisations. The Inspector commended the Council for having a comprehensive RIPA policy and procedure and training strategy and also found that responsible senior managers had a good grasp of the key issues. The main recommendation made was to include guidance on the use of social networking sites and internet within the Policy and Procedures now that these are now more commonly being used as an investigative tool.
9. The revised policy and procedures (Appendix A) therefore includes a new section on social networking / internet and is based upon current legislation, Home Office Codes of Practice and OSC procedures and guidance. A new social networking guidance note and policy has also been incorporated as this area is now being widely used in investigations.
10. The Policy and Procedures also include details of the Authorising Officers, most of whom have had recent relevant training for their authorising role, further training is currently being reviewed.

How this report links to Corporate Priorities

11. Maintaining up-to date policy and procedures and reporting on their use will ensure that the Council complies with its legislative duties under RIPA.

Equality and Diversity Implications

12. Equality and Diversity/Equality Impact Assessment - This report has been prepared in accordance with the Council's Diversity and Equality Policies.

Financial Implications

13. There are no financial considerations associated with this report.

Legal Implications

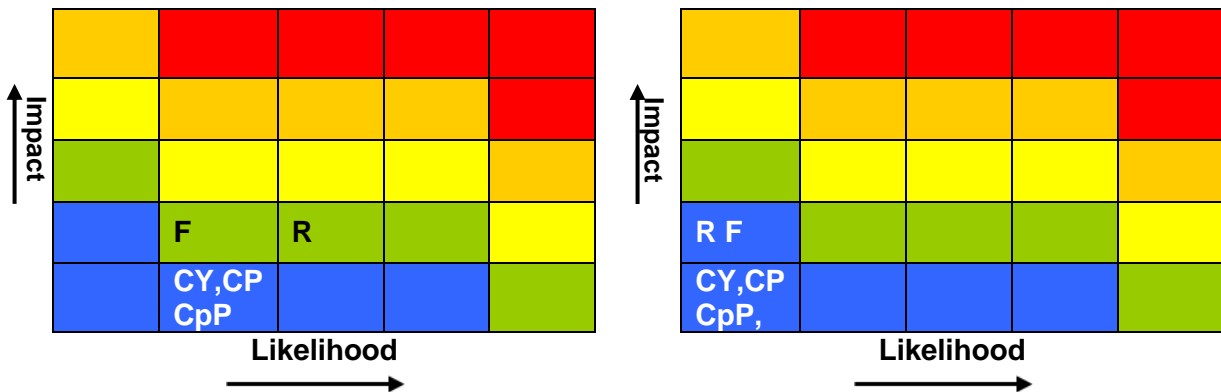
14. Surveillance investigations which are not authorised could leave the Council open to legal challenge by individuals who consider that there has been an intrusion of their privacy.

Risk Assessment

15. An up to date policy, properly trained officers and regular monitoring of the use of RIPA reduces the risks that would accompany any improper use.

Risk Profile before officer recommendations

Risk Profile after officer recommendations



Key

Categories		Colours (for further detail please refer to Risk management strategy)	
R	= Reputation	Red	= High impact and high probability
CpP	= Corporate Plan	Orange	= Major impact and major probability
Priorities		Yellow	= Moderate impact and moderate probability
CP	= Community Priorities	Green	= Minor impact and minor probability
CY	= Capacity	Blue	= Insignificant impact and insignificant probability
F	= Financial		

Background Papers

Regulation of Investigatory Powers Act 2000 Policy and Procedures (Appendix A)
 Using Social Media and Networking Sites in Investigations Policy (Appendix 5)