COMMUNITY PDG
20 AUGUST 2019

REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY AND PROCEDURES 2019

Cabinet Member(s): Cllr Nikki Woollatt, Cabinet Member for the Working Environment and Support Services

Responsible Officer: Director of Corporate Affairs and Business Transformation

Reason for Report: **to undertake the annual review of the Council's existing RIPA policy; to inform Members of the use of RIPA powers by the Council; to consider whether officers should draft a policy on covert surveillance for non-RIPA cases; and to inform Members of the intention to roll out training to officers on the monitoring of information online such as social media posts**

RECOMMENDATIONS:

(1) that it is recommended to Cabinet to approve the revised RIPA Policy, including the new Annex 1 on social media/internet research;
(2) that officers draft a policy on covert surveillance for non-RIPA cases to be submitted for approval; and
(3) to note that the contents of the Report, including the fact that the Council has not used its powers under RIPA since March 2014 and that training will be given to officers on monitoring of information posted online, such as social media posts.

Financial Implications: None directly arising, other than officer time

Legal Implications: As set out in the policy and this report

Risk Assessment: Adopting and complying with a RIPA Policy will minimise any risk to the Council of acting unlawfully

Equality Impact Assessment: No equality issues directly arising from this report

Relationship to Corporate Plan: Statutory guidance requires elected members to review the Council's use of RIPA and approve the RIPA policy at least once a year- therefore these requirements need to be complied with to show the Council is a well-managed Council

Impact on Climate Change: None directly arising

1 Background

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was put in place to ensure that the use of certain investigatory powers by certain organisations complies with the UK's obligations under the European Convention on Human

Rights (ECHR) including Article 8 (the right to privacy). The proper authorisation of certain covert surveillance powers under RIPA ensures that the Council is acting in accordance with such human rights.

1.2 Following criticism of local authorities' use of covert surveillance powers additional safeguards were put in place including:-

- The need to obtain magistrate approval
- Only be used to investigate offences which attract sentences of six months or more or relate to the underage sale of alcohol or tobacco.

2 The need for a covert surveillance policy for non-RIPA cases

2.1 The effect of these safeguards and restrictions mean that it will be a very rare occurrence for RIPA authorisation and judicial approval to be obtained – indeed the Council has not made use of such powers since 2014. The type of offences which the Council typically investigates does not attract sentences of six months or more. However, there may be occasions when the Council wants to conduct covert surveillance which could not be approved under RIPA because it is not an investigation into an offence which attracts a sentence of six months or more.

2.2 It should also be noted that covert investigation carried out without RIPA authorisation is not automatically unlawful because of the lack of authorisation. For instance if the Council conducts covert surveillance without RIPA authorisation it will not be in breach of Article 8 privacy rights if the Council can show that the interference was necessary and proportionate and there was process of authorisation that was fair.

2.3 The Office of Surveillance Commissioners in its Annual Report for 2012 to 2013 at paragraph 5.5 said the following:

> *It is not my role to encourage more or less use of covert surveillance but there are occasions when it is considered necessary and proportionate but the protection of RIPA cannot be sought. For example, covert surveillance within the residential premises of a vulnerable person may be a necessary and proportionate response but may not meet the serious crime criteria to enable authorisation for intrusive surveillance. My published guidance is supported by the Investigatory Powers Tribunal in the case of BA and others v Cleveland Police (IPT/11/129/CH). Though less frequent there may be occasions when a local authority deem it necessary and proportionate to conduct covert surveillance which does not meet the six month criteria set out in the relevant Act. In all of these circumstances since I do not decide whether the decision is correct or the authorisation valid, I consider it wise to have a verifiable audit similar to the process and documentation for RIPA available for later scrutiny*

2.4 Officers seek Members' agreement to develop a policy for covert surveillance where RIPA does not apply. This policy should set out the authorisation procedure which would mirror the RIPA policy, but there would not be a judicial review mechanism. This policy would set out stringent tests for authorisation similar to RIPA authorisation and it would have to take into

account the Data Protection issues and well as Human Rights considerations. Once the policy has been formulated it would be brought back before Members for approval.

3 Approval for amendments to the Council's RIPA policy

3.1 The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of investigatory powers. It carries out periodic inspections every 3 years. The IPCO wrote to the Council on the 18th October 2018 (Appendix 1) after it carried out a "desktop based documentary inspection" by one of the inspectors. IPCO was grateful that the Council had facilitated the process enabling the inspection to be conducted by way of a "desk top" approach. The IPCO was also pleased that the level of compliance shown by the Council with RIPA was such that a physical inspection was not necessary at the present time.

3.2 The IPCO reviewed the Council's RIPA policy and suggested amendments along the following lines:-

1. The policy should indicate that the renewal of directed surveillance or covert human intelligence source (CHIS) authorisation must be approved by a magistrates' court in the same manner as the initial authorisation

2. Authorisation for vulnerable persons/juveniles as CHIS or for directed surveillance where there is a risk of obtaining confidential information may only be granted by the person who has been formally nominated as the acting Chief Executive in the absence of the Chief Executive

3. There is a need for guidance on the monitoring of information online such as social media posts, during investigations.

3.3 Officers have drafted amendments to the Council's RIPA policy to take into account the IPCO's comments. Suggested amendments for nos. 1 and 2 above are technical changes which do not require much in the way of comment. Suggested amendment for no. 3 above is contained in the draft Annex 1 to the RIPA policy. The revised policy with tracked changes is shown at Appendix 2 to this Report.

3.4 For clarity, much of the publicly accessible internet content can be accessed by officers without the need for RIPA authorisation, but in some cases RIPA authorisation is required. Unfortunately the point at which access strays into surveillance is not always clear-cut. The Government has issued a code of practice for Covert surveillance and covert human intelligence sources in order to assist compliance with RIPA. The following paragraphs at 3.10 to 3.15 of the code of practice for directed surveillance put into context the use of the internet and RIPA:

> *3.10. The growth of the internet and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in*

preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation: use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications stilly apply. This is because the intention when making such information available was not for it to be used for covert purposes such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information.

Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less to hold a reasonable expectation of privacy in relation to that information

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. There considerations apply regardless of when the information was shared online. See also paragraph 3.6

3.5 The need to consider how the Council uses social media as an investigatory tool was further emphasised in expert training to key senior council officers in November 2018. Officers have therefore drafted an annex to the RIPA policy to provide guidance on the monitoring of information online such as social media posts. It is considered that training will need to be given to officers on the monitoring of information online, such as social media posts.

4 Other RIPA related activity in 2018-19

4.1 In addition to the review carried out by the IPCO (see paragraph 3.1 above) and the training provided in November 2018, the Co-ordinating Officer has also provided the annual statistical return to the IPCO. Thankfully, this was straightforward, given the non-use of RIPA in the previous year.

Contact for more Information: Philip Langdon (Solicitor and RIPA Co-ordinating Officer) 01884 234204 plangdon@middevon.gov.uk; Kathryn Tebbey (Group Manager for Legal Services and Monitoring Officer as Senior Responsible Officer) 01884 234210 ktebbey@middevon.gov.uk

Circulation of the Report: Cabinet Member seen and approved yes Cllr Woollatt, Leadership Team seen and approved [yes/no]

List of Background Papers: Appendix 1 – IPCO Letter dated 18 October 2018
Appendix 2 – RIPA policy – with draft revisions and additions