SURREY COUNTY COUNCIL

CABINET

DATE: **26 NOVEMBER 2019**

REPORT OF: **MRS DENISE TURNER-STEWART, CABINET MEMBER FOR COMMUNITIES**

LEAD OFFICER: **STEVE OWEN-HUGHES, DIRECTOR OF COMMUNITY PROTECTION AND EMERGENCIES**

SUBJECT: **REGULATION OF INVESTIGATORY POWERS ACT 2000 – UPDATED CORPORATE POLICY AND PROTOCOL**

SUMMARY OF ISSUE:

The Cabinet is asked to agree an updated Policy and Protocol on the use of the Regulation of Investigatory Powers Act 2000 (RIPA) by Surrey County Council services.

The updates include changes on how services access communications data, because this has been changed under a new law (The Investigatory Powers Act 2016) which came into force in June 2019.

The updates include changes recommended during an inspection of Surrey County Council's use of RIPA earlier this year.

The update also includes a section (at paragraph 14.5) which allows for future changes to the policy to be made by the relevant Cabinet member using delegated powers.

RECOMMENDATIONS:

It is recommended that the Cabinet:

1. Endorse the proposed new Corporate Policy and Protocol on the application of the Regulation of Investigatory Powers Act 2000 to include:

    a. the updated section at paragraph 10 on the acquisition of Communications Data;

    b. the points at paragraph 6.3 updating the Office of Surveillance Commissioners to the Investigatory Powers Commissioner's Office, at paragraph 7.1 regarding the Directed Surveillance authorisation period, at paragraph 8.1 regarding cancellations and at paragraph 11.5 highlighting Covert Human Intelligent Source time limits, which encompass the recommendations made following the most recent RIPA Inspection; and

2. delegate authority to the Cabinet Member for Community Safety Fire and Resilience in consultation with the relevant Director to approve the Corporate Policy and Protocol on the use of the Regulation of Investigatory

Powers Act 2000 and any subsequent changes to this and that the Director of Law and Governance be authorised to make the necessary changes to the Council's Scheme of Delegation and the Constitution be updated accordingly.

REASON FOR RECOMMENDATIONS:

The inclusion of the above updates within the Corporate Policy and Protocol will provide an updated framework to ensure that the authority continues to comply fully with the requirements of RIPA. The updates ensure that Surrey County Council is operating in accordance with the latest legislation.

Following the RIPA Inspection carried out in February 2019, recommendations and observations were made to the Corporate Policy and Protocol on the use of RIPA which has led to the requirement to make some minor amendments to the Policy.

Allowing future changes to the policy to be authorised by the relevant Cabinet member using delegated powers will prevent this policy repeatedly being placed before full Cabinet for consideration.

DETAILS:

Background:

1. Local Authority Trading Standards Services conduct criminal investigations into a wide range of activities, bringing criminals to justice whilst protecting local communities and legitimate businesses.

2. During criminal investigations it is sometimes necessary to interfere with an individual's right to privacy, for example, by carrying out surveillance activity covertly or by tracing the subscriber of a telephone number used in connection with a crime. The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) allow such activities to continue and properly regulates such investigative activity.

3. The use of RIPA is included within existing Corporate Governance Policies and the Policy Custodian on behalf of SCC is Head of Trading Standards, Steve Ruddy. The Senior Responsible Officer (SRO) is Steve Owen-Hughes, Director of Community Protection and Emergencies.

What types of activities can be authorised?

4. Three different types of activity can be authorised known as:

   - **Communication Data Checks** – used to obtain entity data (such as subscriber and billing details) and some events data (such as where and when and how communications occurred. This **does not** include the ability to "bug" or otherwise monitor calls and their content or open emails.

   - **Directed Surveillance** - covert targeted monitoring of an individual. Used in situations such as age restricted test purchase exercises. This **does not**

include ‘intrusive surveillance’ i.e. an individual’s private residence or vehicle.

- **Covert Human Intelligence Sources (CHIS),** using or tasking individuals who establish or maintain a relationship with another person for a covert purpose e.g. using a profile on social media for the purpose of posing as a potential customer to investigate the sale of illicit goods over the internet.

5. In all cases, after less intrusive approaches have been considered, the activity authorised must be necessary and proportionate to the nature of the criminal offence under investigation. The offences under investigation must also either;

   - meet the ‘serious crime threshold’ being offences that attract a maximum custodial sentence of six months (or more) or,

   - be those that relate to underage sales of alcohol or tobacco for directed surveillance only.

6. All applications for Directed Surveillance and CHIS authorisations are initially scrutinised by the accredited RIPA Single Point of Contact (SPoC) or in-house Senior Legal Officers, before being passed to the Assistant Head or Head of Trading Standards to authorise. The authorised application is then presented in private to a Justice of the Peace by a Senior Legal Officer.

7. The Protection of Freedoms Act 2012 came into force on 31 October 2013. This requires RIPA authorisations to undergo judicial review with a magistrate approving a RIPA application only if satisfied that it:

   - Is necessary for the prevention and detection of crime or prevention of disorder.

   - Is proportionate in human rights terms to what it seeks to achieve.

   - Has been authorised by a person in the authority at the level designated in RIPA.

   - Meets any other restriction imposed by order (e.g. serious crime threshold).

   - In the case of a CHIS, sets out that the relevant procedures and supporting officers are in place to protect the welfare and safety of the CHIS.

8. In the case of applications for communications data, the Investigatory Powers Act 2016 has removed the previous requirement for judicial approval. Trading Standards applications for communications data must be submitted through a service provided by the National Anti-Fraud Network (NAFN) to the new Office for Communications Data Authorisations (OCDA). Trading Standards will not acquire communications data until a senior officer has confirmed they are aware of the application and the application is approved by the OCDA. NAFN act as a Single Point of Contact (SPoC) between Trading Standards and both OCDA and the Communication Service Providers.

9. All authorisations must be fully recorded and are subject to regular external oversight. In relation to Directed Surveillance and CHIS, they are recorded by

the Trading Standards Service, and in relation to Communications Data they are recorded by NAFN. There is an external inspecting body who reports to Parliament and also conducts audit visits and requires annual returns of use.

- **Investigatory Powers Commissioner's Office** – looks at how public authorities make use of authorisations in relation to Directed Surveillance, Covert Human Intelligence Sources and Communications Data

What are we trying to achieve:

10. The proposed policy and protocol (Annex 1) provides information on RIPA and how it must be applied across all relevant services. Adoption of the policy and protocol will:

    - Help ensure that all services are aware of and fully comply with RIPA and IPA requirements.
    - Comply with the requirements of the Protection of Freedoms Act 2012.
    - Ensure transparency through the reporting and scrutiny mechanisms, and help to keep public confidence in the use of RIPA and IPA by the local authority.
    - Ensure that everyone involved in making RIPA and IPA applications, and all those authorising or being made aware of applications, are appropriately trained and fully competent to do so.
    - Clearly specify those persons / posts that can authorise activity.

11. The amendments ensure that the policy is brought up to date with requirements in the Investigatory Powers Act in acquiring communications data.

12. The amendments ensure that the policy reflects the recommendations made by the Inspector following the RIPA inspection in February 2019.

13. Any Directed Surveillance and CHIS applications made through this policy will still need to be placed before the court and a Justice of the Peace will only grant the applications if they are satisfied that individual applications are legal, necessary and proportionate. Applications for communications data will be approved by the Office of Communications Data Authorisations.

External Oversight and Record Keeping

14. RIPA requires the local authority to keep a central record of all Directed Surveillance and CHIS authorisations. As the primary user of the legislation the central record is maintained and retained by the Trading Standards service. All authorisations are also subject to regular external inspection to ensure compliance with requirements of RIPA.

15. During 2018/19, three RIPA authorisations were granted for Communications Data (prior to IPA coming into force). For comparison purposes the figures for previous years are also given. As you can see, the usage of RIPA has been relatively low reflecting the Service's adherence to the requirements of RIPA and only using it where all other avenues for investigation had been exhausted.

16. It should be noted that IPA makes clear that the requirement for obtaining communications to be necessary does not mean that it should only be used as a last resort. We therefore anticipate that there will be an increased number of applications to access communications data, and to the end of September 5 applications had been made for communications data under the IPA.

	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20
Communications Data Authorisations	0	1	3	1	3	5 to end of Sept[1]
Directed Surveillance Authorisations	3	5	0	0	0	0
CHIS Authorisations	0	0	0	0	0	0

Are there choices?

17. There is no statutory requirement to maintain a corporate policy but feedback from previous inspections strongly recommends that a corporate policy is in place. However the authority should comply with the requirements of the Protection of Freedoms Act 2012.

What are the implications of not adopting a corporate policy and protocol?

18. The implications would be:

- Greater possibility of some services failing to be fully aware of their responsibilities under RIPA or IPA and consequently an increased risk of legal challenge.
- Increased likelihood that future external inspections would be very critical of the authority for failing to make improvements identified in earlier inspections, which could lead to an increased reputational risk.
- The benefits of the reporting and scrutiny activities in the policy and protocol would not be realised.

What has changed?

19. Within the existing corporate RIPA policy at paragraph 10, the section has been updated to reflect the current process for the acquisition of Communications Data under the Investigatory Powers Act 2016.

20. Within the existing corporate RIPA policy, several paragraphs have been amended slightly to reflect the recommendations made following the recent RIPA Inspection. This includes the points at paragraph 6.3 updating the Office of Surveillance Commissioners to the Investigatory Powers Commissioner's Office, at paragraph 7.1 regarding Directed Surveillance authorisation period,

---

[1] *Under the Investigatory Powers Act 2016, applications for communications data no longer require judicial approval and there is no longer a requirement to report this figure.*

at paragraph 8.1 regarding cancellations and at paragraph 11.5 highlighting Covert Human Intelligent Source time limits.

21. Within the existing corporate RIPA policy a paragraph has been inserted at paragraph 14.5 to allow the relevant Cabinet member to use delegated powers to authorise future changes and amendments.

CONSULTATION:

22. The RIPA Corporate Policy and Protocol last received approval from Cabinet on 25 September 2018. There has been no further consultation since then.

RISK MANAGEMENT AND IMPLICATIONS:

23. The adoption and application of this policy and protocol will help ensure that the local authority continues to act correctly when carrying out criminal investigations and reduce the risk of any actions in relation to allegations of breaches of the Human Rights Act. It will also minimise the potential reputational risk from any claims of misuse of investigatory powers.

Financial and Value for Money Implications

24. Application of this policy and protocol will minimise any risk of claims being made against the local authority alleging Human Rights breaches.

25. The revised policy will be administered by Trading Standards within existing resources and budgets. The presentation of each Directed Surveillance authorisation to the Justice of the Peace will be carried out by existing Trading Standards staff and no fee is payable.

Section 151 Officer Commentary

26. This is an update of an existing policy which clarifies the use of RIPA. The S151 Officer (Chief Finance Officer) confirms that all material, financial and business issues and risks have been considered / addressed.

Legal Implications – Monitoring Officer

27. The legal implications are as set out in the body of the report. The adoption of a RIPA policy by the Council is discretionary; albeit strongly recommended that the Council does so in order to aid its compliance with the statutory protections individuals are afforded against intrusive investigation. Cabinet will note that the final decision on the Council's ability to utilise Directed Surveillance and CHIS's under RIPA rests with a justice of the peace (magistrate) or, for Communications Data under IPA, the Office of Communications Data Authorisations.

Equalities and Diversity

28. Many rogue traders deliberately target elderly and vulnerable people. The investigative techniques covered by RIPA are often used in these crimes to help identify and locate such criminals. Therefore the Trading Standards

Service can continue to effectively protect the most vulnerable people in Surrey's communities.

29. Any decision to use techniques covered by RIPA/IPA are made against standard criteria and are not influenced by ethnicity, race or other factors. The process also requires that consideration be given to any local community influences or sensitivities.

WHAT HAPPENS NEXT:

The new policy and protocol will be introduced and all services made aware of the requirements.

Contact Officer:
Steve Ruddy – Trading Standards Head of Service

Contact details:

01372 371730
steve.ruddy@surreycc.gov.uk

Consulted:
There has been no consultation on this paper.

The RIPA Corporate Policy and Protocol last received approval from Cabinet on 25 September 2018.

Annexes:

Annex 1	Corporate Policy and Protocol on the use of the Regulation of Investigatory Powers Act 2000 (RIPA)

Sources/background papers:

- The Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016

This page is intentionally left blank