Appendix A

Rother District Council

REGULATION OF INVESTIGATORY POWERS ACT 2000

Policy

Introduction

1. The Regulation of Investigatory Powers Act 2000 (RIPA) (as amended by the Protection of Freedoms Act 2012) regulates surveillance carried out by the Council in the conduct of its business. It relates to directed surveillance and the use of Covert Human Intelligence Sources (CHIS).

2. It provides a legal framework for authorising investigations in a manner consistent with obligations under the Human Rights Act 2000 (HRA) where the investigation is for the purposes of preventing or detecting crime or for preventing disorder.

3. RIPA is wide ranging in its application and will impact all officers with an enforcement or investigatory capacity, including internal investigations. Failure to comply with RIPA may result in a claim for a breach of the HRA. This may result in evidence being deemed inadmissible in a prosecution or even a claim for compensation for an infringement of that person's human rights. By obtaining approval from a Court for surveillance the Council and Officers are protected from complaints about the inappropriate obtainment and use of information and data.

4. The Council is committed to implementing RIPA in a manner that is consistent with the spirit and letter of RIPA and the HRA. The Council is committed to conducting all relevant actions in a manner which strikes a balance between the rights of the individual and the legitimate interests of the public.

5. Any authorisation by the Council under RIPA for the use of covert techniques can only be given effect once an order approving the authorisation has been granted by a Magistrates' Court. Courts can only approve surveillance if intended to prevent or detect criminal offences that are punishable by a maximum term of at least 6 months' imprisonment or offences related to the underage sale of alcohol and tobacco.

Codes of Practice

6. Statutory Codes of Practice supplement RIPA. RIPA codes - GOV.UK (www.gov.uk)

7. The Council will have due regard to and follow the guidance in the relevant Codes of Practice in the conduct of its activities relating to RIPA.

Surveillance

8. Almost all the surveillance carried out by the Council is done overtly (it is not covert or directed surveillance). Overt surveillance is not subject to the authorisation requirements under RIPA. In many cases, officers will be behaving in the same way as a member of the public or will be going about

normal council business, openly. Surveillance is overt if the subject has been told that it will happen.

9. Covert surveillance is defined in section 26(9)(a) of RIPA as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It may be either direct or intrusive surveillance.

10. **Directed surveillance** is defined in section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

- for the purposes of a specific investigation or specific operation;
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance.

The Code of Practice for Covert Surveillance and Property Interference provides detailed guidance on whether covert surveillance activity is directed surveillance or intrusive, or whether an authorisation for either activity would not be deemed necessary.

11. **Intrusive surveillance** is defined in section 26(3) of RIPA as covert surveillance that:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Local Authorities are not authorised to conduct intrusive surveillance.

12. A **CHIS** is defined in section 26(8) of RIPA as a person who:
establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling with paragraph (b) or (c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Communications Data (CD)

13. The Council may also access certain Communications Data (CD), provided it is for the purpose of preventing or detecting crime or of preventing disorder. All applications for CD must be made via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All Councils must use the National Anti-Fraud Network (NAFN) as their SPoC.

Authorising Officer (see Appendix 1)

14. Before application to the Magistrates' Court, all requests must first be authorised by an Authorising Officer.

RIPA Co-Ordinator

15. The RIPA Co-ordinator will check all applications before being submitted to an Authorising Officer.

Social Media (see Appendix 2)

16. The use of social media in an investigation could, depending on how it is used and the type of information likely to be obtained, constitute covert activity that requires authorisation under RIPA.

CCTV (see Appendix 3)

17. The Council owns and operates CCTV on its premises. CCTV cameras in towns are controlled by Sussex Police.

Non-RIPA approved surveillance

18. Surveillance may be carried out for crimes that do not meet the threshold of 6 months imprisonment or are related to the underage sale of alcohol and tobacco. If an officer carries such surveillance that does not require a RIPA approval by a Magistrate or District Judge, it will still require authorisation.

Training

19. All officers with an enforcement or investigatory function will receive training on the provisions of RIPA.

Central Record of all authorisations

20. The Senior Responsible Officer (SRO) will be responsible for maintaining a record of all authorisations, renewals, reviews and cancellations issued by the Council.

Data retention

21. Any records obtained during the course of a criminal investigation must be retained in compliance with the Criminal Procedure and Investigations Act (CPIA) Codes of Practice and all material stored in line with the General Data Protection Regulations (GDPR) data retention policy.

22. Line managers must be aware of the evidence obtained in connection with a RIPA application and will monitor this evidence, ensuring it is manged in line with the safeguarding requirements in the codes. This includes retention, storage and review. At the conclusion of a case the manager should ensure the evidence is destroyed when no longer necessary under CPIA or other legislation. If retained beyond this period, that it is reviewed on a three-monthly basis. When destroyed, how and when will be recorded.

Review of Policy

23. The Senior Management Team will review this policy annually. The Senior Responsible Officer will provide an annual report to the Licensing and General Purposes Committee.

Appendix 1

List of Authorising Officers/Designated Persons

Chief Executive - Lorna Ford
Deputy Chief Executive - Vacant
Director - Ben Hook

Senior Responsible Officer

Head of Service-Environmental Services, Licensing and Community Safety
Richard Parker-Harding

RIPA Co-Ordinator

Legal Services Manager
Rother & Wealden District Councils Shared Legal Service

INTERNET AND SOCIAL MEDIA

1. Introduction

1.1 Online open-source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

1.2 The use of online open-source internet and Social Media research is a method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues. However, the use of the internet and Social Media is constantly evolving and with it the risks, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

1.3 Rother District Council is a Public Authority in law under the Human Rights Act 1998, and as such, the staff of the authority must always work within this legislation. This applies to research on the internet.

1.4 Researching, recording, storing, and using open-source information regarding a person or group of people must be both necessary and proportionate and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a Magistrate under the Regulation of Investigatory Powers Act (RIPA) 2000. To ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, the material must be retained and processed in accordance with the principles of the General Data Protection Regulations (GDPR).

2. Scope of Policy

2.1 This policy and associated procedure ensures that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff, when engaged in their official capacity of the implications and legislative framework associated with online internet and Social Media research. It will also ensure that the activity undertaken, and any evidence obtained will stand up to scrutiny.

2.2 This policy takes account of the Human Rights Act 1998, Regulation of Investigatory Powers Act (RIPA) 2000, Criminal Procedures Investigations Act (CPIA) 1996, General Data Protection Regulations (GDPR), NPCC Guidance on Open-Source Investigation/Research.

2.3 This policy and associated procedure will be followed at all times and should be read, where required with the RIPA Codes of Practice.

2.4 This policy is not exempt from disclosure under the Freedom of Information Act 2000.

3. Risk

3.1 Staff must be aware that any activity carried out over the internet leaves a trace or footprint which can identify the device used, and, in some circumstances, the individual carrying out the activity. This may pose a legal and reputational risk

to the Council from being challenged by the subject of the research for breaching Article 8.1 of the HRA which states “Everyone has the right to respect for his private and family life, his home and his correspondence”. 8.2 states “There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others”.

3.2 There is also a risk of compromise to other investigations, therefore, the activity should be conducted in a manner that does not compromise any current or future investigation or tactics.

4. Necessity / Justification

4.1 To justify the research, there must be a clear lawful reason, and it must be necessary. Therefore, the reason for the research, such as, the criminal conduct that it is aimed to prevent or detect must be identified and clearly described. This should be documented with clear objectives. Should the research fall within RIPA activity, the RIPA authorisation deals with this criteria for it to be lawful.

5. Proportionality

5.1 Proportionality involves balancing the intrusiveness of the research on the subject and other innocent third parties who might be affected by it (collateral intrusion) against the need for the activity in operational terms. What is the benefit to carrying out the activity? How will the benefit outweigh the intrusion?

5.2 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6. Private information

6.1 Private information is defined at Section 26(10) of RIPA 2000 as including any information relating to a person’s private or family life. Private information should be taken generally to include any aspect of a person’s private or personal relationship with others, including family and professional or business relationships.

6.2 Prior to, and during any research, staff must take into account the privacy issues regarding any person associated with the research.

7. Reviewing the Activity

7.1 During the course of conducting the internet open-source research, the nature of the online activity may evolve. It is important staff continually assess and review their activity to ensure it remains lawful and compliant. Where it evolves into RIPA activity, the RIPA procedure should be followed. If in doubt, seek advice.

8. Use of Material

8.1 The material obtained from conducting open-source internet and Social Media research may be used as intelligence or evidence.

8.2 Any material gathered from the internet during a criminal investigation must be retained in compliance with the Criminal Procedure and Investigations Act (CPIA) Codes of Practice and all material stored in line with the General Data Protection Regulations (GDPR) data retention policy.

CCTV

Why do we have CCTV?

1. The purpose of CCTV is to help:

    - monitor security of our premises;
    - provide greater personal protection for staff and members of the public;
    - reduce costs resulting from criminal damage or loss;
    - reduce insurance costs;
    - prevent, investigate and detect crime; and
    - apprehend and prosecute offenders.

2. If we inform the public CCTV or Body Cams are operating, then it is overt monitoring.

Responsibility

3. The day-to-day management of CCTV systems and control of the recordings is the responsibility of the Head of Service in control of the premises or land. The Head of Service will designate Officers who can view the recorded images for specific purposes.

4. Images should not be held on the system for longer than 31 days (the standard overwrite time) unless there is a legitimate reason for keeping them e.g. a criminal investigation. In such cases, the reasons must be recorded.

Third party requests for disclosure

5. Where you receive a request for personal information from an outside organisation or individual, you must be satisfied that the information requested falls within one of the exemptions from non-disclosure.

6. Those disclosing information must be satisfied that the disclosure is necessary, and that if we did not disclose the information the non-disclosure would be likely to prejudice the exemption aims. Requests should always be made in writing, and the person requesting disclosure should provide the information listed below:

    - name and contact details of person or organisation making the request;
    - date of request;
    - details of the person to whom the disclosure relates; and
    - the reason the information is required.

7. A written record of the above, together with any steps taken to verify the identity of the requester, and a record of the information disclosed. This information is in order to protect staff and officers from accusations of unlawful disclosure and to enable the Council to assess any disclosure decision.

Requests from members of the public about themselves

8. If a member of the public wants to see a recording of him/herself they must fill out a Subject Request Form (which is available via the website – see Data Protection Subject Access Request Form) and return it with a search fee and two forms of identification to the Data Protection Officer. They should indicate if viewing will be sufficient or if a copy is required.

9. They will get a response within 40 days of us receiving the form, the fee and valid identification. They may also be asked to provide a photograph of themselves so that the correct images can be retrieved. If a request is granted, any other person appearing in the images will be edited out.

Body cams: https://www.rother.gov.uk/wp-content/uploads/2020/05/Rother-Privacy-Policy-body-cams.pdf

Privacy Policy: https://www.rother.gov.uk/data-protection-and-foi/privacy-policy/

Further Information: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice