South Kesteven District Council

Regulation of Investigatory Powers Act Policy

1. Introduction

1.1 South Kesteven District Council recognises that a need for secret or covert surveillance and the gathering of communications data will arise from time to time during the course of investigations carried out by its Officers in the discharge of the Authority's statutory functions. The Council agrees, however, that it should be used as sparingly as possible and only when all legal safeguards have been met.

1.2 All such activities will be carried out in compliance with the Human Rights Act 1998. Where appropriate, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) will be used to ensure this. Statutory Codes of Practice published by the Home Office will be complied with.

1.3 Responsibility is placed upon the Council's Head of Paid Service (Chief Executive) to ensure the Authority's overall compliance with the Act and act as the "Senior Responsible Officer". The Council's Monitoring Officer will act as the Authority's "RIPA Coordinating Officer" to assist in this.

2. Purpose of RIPA

2.1 The primary purpose of RIPA is to ensure that surveillance and other techniques employed by public bodies are justified when they would otherwise infringe an individual's rights under Article 8 of the European Convention on Human Rights and be unlawful under Section 6 of the Human Rights Act 1998.

2.2 The rights in Article 8 to respect a citizen's private and family life and his or her home correspondence are not absolute. In certain circumstances a public authority may interfere with them provided the interference is:

- In accordance with the law
- Necessary for a number of prescribed purposes
- Proportionate in the circumstances.

2.3 RIPA and IPA create a statutory framework for the authorisation of such interference. The surveillance and other monitoring covered by RIPA are not necessarily "cloak and dagger" activities but can include many forms of observation and information gathering which have in the past been a routine part of Council Officers' work.

2.4 All Local Authority RIPA authorisations for Directed Surveillance and Covert Human Intelligent Sources are subject to judicial approval by a Magistrate before they have effect. Applications for Communications Data under IPA are authorised by the Office for Communications Data Authorisations (OCDA) and therefore judicial approval is not required.

3. Surveillance and Covert Human Intelligence Sources (CHIS)

3.1 The Act defines three particular types of activity:

Directed Surveillance: covert surveillance undertaken in relation to a specific planned investigation or operation which is likely to lead to private information about a person being obtained. Surveillance is covert where it is conducted in a manner calculated to make sure that the subject is not aware that it is happening.

Intrusive Surveillance: covert surveillance which takes place in residential premises or a private vehicle either by the presence of a person within the premises or vehicle or the installation of a device. It cannot be conducted by a Local Authority.

Use of a Covert Human Intelligence Source (CHIS): a CHIS is a person who maintains a personal or other relationship with a person for the covert purpose of obtaining or gaining access to information. It does not mean circumstances where members of the public volunteer information or to contact numbers set up to receive information but it will cover cases where officers or other agencies with which the Council works are asked to obtain information from someone by establishing or maintaining a personal or business relationship with that person.

3.2 Authorisations for the use and conduct of a CHIS should define the use, nature and conduct of the CHIS' task, in broad terms. Such authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked however, if there is a significant change in nature of the task, then a new authorisation should be sought.

3.3 Only the Head of Paid Service (Chief Executive), or in their absence the person acting as the Head of Paid Service, can authorise the use of a person under 18 or a vulnerable individual as a CHIS. A vulnerable individual is someone who by reason of mental or other disability may be in need of community care services or unable to protect him or herself against harm or exploitation.

Covert and overt

3.4 The word "covert" is common to all three of the definitions in the preceding paragraph. It means simply that the surveillance will be carried out in a manner intended to make sure that the person under observation is unaware that it is taking place. Much of the surveillance carried out by the council is of course overt either because there is nothing hidden about it and staff go about their business openly or because the subject has been told (preferably in writing) that surveillance will take place. However, it is important to note that the mere visibility of the officer carrying out the surveillance does not in itself make the surveillance overt.

4. Closed circuit television (CCTV)

4.1 As the CCTV cameras operated by the District Council are both publicly signed and not normally directed at particular individuals, RIPA does not ordinarily apply to their use. However, from time to time, CCTV control will receive requests from enforcement agencies to use the system to monitor persons or premises for a period. The Control Room Supervisor must then obtain evidence that a RIPA authorisation has been obtained. The Biometrics and Surveillance Camera Commissioner provides information on this area.

5. Social Media Platforms

5.1 Council staff need to be aware that activity on, or intelligence gathering from, social media platforms may raise privacy and RIPA issues. A preliminary examination of an online presence, to see if the site or contents are of interest, or 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 is recorded, a RIPA authorisation should be considered. If reasonable steps are taken to inform the public or individuals that online surveillance may be taking place, the activity can be regarded as overt.

5.2 Where a "minimal" level of interaction is required before access is permitted (e.g "friend") this may not constitute a relationship. However, if further interaction may follow, a CHIS authorisation should be considered.

6. Authorisation of Directed Surveillance and use of a CHIS

6.1 Directed surveillance and CHIS authorisations will only be made by officers listed in Appendix 1 when they are satisfied that:

- the authorisation is necessary for the prevention and detection or crime or preventing disorder and
- in the case of Directed Surveillance only, that the offences in question meet the "crime threshold" (maximum sentence of at least six months imprisonment OR certain specified offences relating to the sale or supply of age restricted products) and
- the proposed activity is proportionate to its objective and
- in the case of a CHIS:
  - That a suitable risk assessment is carried out to determine the risk to the CHIS of the deployment, and any consequences should the role of the CHIS become known.
  - That there are arrangements in place to update the assessment to reflect developments in course of the deployment.
  - That consideration has been given to the management of any requirement to disclose information that could risk revealing the identity of the CHIS.
  - That specific arrangements exist to ensure that the CHIS is independently managed and supervised, that records are kept of the use made of the CHIS, and that any concerns about the validity of risk assessments, conduct of the CHIS and safety and welfare of the CHIS

are appropriately addressed, in accordance with the current CHIS records regulations.
- Where appropriate, concerns about such matters must be considered by the Authorising Officer and decisions taken on the continuance of the authorisation.

6.2 The standard application forms for Directed Surveillance and use of a CHIS and other processing and review documents are held by the Monitoring Officer.

7. Relevant Considerations

"Necessary" and "Proportionate"

7.1 These are key definitions to the application of RIPA in both Parts 1 and 2. Not only must information be sought for a prescribed purpose (set out in the previous paragraph) but the use of the covert technique to obtain it must meet both these criteria. Applications for authorisation must have regard to this requirement and set out coherently how the information or evidence obtained is intended to assist the investigation.

7.2 The action must be necessary in relation to a prescribed reason (the only reasons prescribed for Local Authorities are the prevention or detection of crime or preventing disorder, and a "crime threshold" test as to seriousness exists for Directed Surveillance) and it must be proportionate in that even if it is necessary to obtain the information the interference with a person's right of privacy is not excessive in all the circumstances. A judgement on whether a covert technique is appropriate will involve the consideration of other options and if these exist the least intrusive method of procuring information is likely to be the most proportionate.

Collateral Intrusion

7.3 Whenever appropriate and practical a proposed surveillance should include a plan to minimise the possibility of intrusion being caused to people who are not the primary subject of the surveillance and to deal with any irrelevant material thereby obtained.

Health and safety

7.4 Authorising Officers must pay special attention to any health and safety issues which may be raised by any proposed surveillance or CHIS authorisation Unless these have been carefully considered and risks kept to an acceptable level the proposal should not be authorised.

8. Authorisation Procedures

(For detailed requirements see the Home Office Codes of Practice)

Applications

8.1 These must be in writing. The standard application forms and processing documents are held by the Monitoring Officer and will follow the format of those published by the Home Office.

Authorisation

8.2 An authorisation will be endorsed or rejected using the appropriate form. Authorisations can last for up to 3 months in the case of surveillance and 12 months in the case of CHIS. After this period a new application may be made. Authorisations are not open ended and Authorising Officers will indicate a date for review in all authorisations. Where the relevant considerations for authorisation are no longer met, the authorisation will be cancelled.

Records

8.3 The Monitoring Officer maintains a central retrievable register of all authorisations granted, renewed or cancelled. Although under the relevant Codes of Practice, records are only required to be retained for at least three years (five years from authorisation end for CHIS), it is desirable to retain them for five years. After this time they will be subject to data retention, review and deletion under the Data Protection Act 2018. To ensure this register is kept up to date a copy of the relevant paperwork must be provided to the record keeper within **one week** of application/authorisation/renewal/cancellation etc. The record keeper is the Council's Head of Public Protection.

Audit

8.4 The District Council is accountable to the Investigatory Powers Commissioner both for the sound administration of its systems and for record keeping.

9. Communications

9.1 Under the IPA Local Authorities are entitled to obtain certain information from Communications Service Providers. Relevant definitions of available material are:

Communications Data – information from telecommunications companies, internet service providers and mail services. It includes "Entity" data and "Events" data but not the content of communications.

Entity Data – this is data about entities or the links between them but does not include information about individual events. Entities can be individuals, groups or objects. Examples are:

- Subscriber information.
- Top-up history of a mobile phone.
- Social media logon information.
- Website registrant details.
- Royal Mail redirection and payment information.

Entity Data is available for the purposes of preventing and detecting crime.

Events Data – this is data which identifies or describes events which consists of one or more entities engaging in an activity at a specific time or times. It will include information which identifies, or appears to identify any person, apparatus, or location to or from which a communication is transmitted.

Examples of Events Data:

- Incoming and outgoing call data (numbers called and received), including the date, time and duration.
- Cell site start and end location for mobile phone calls (shows the area a phone call was made/received from the closest mobile phone mast).
- IP address information (date and time of connection).

Events Data is available for the purposes of preventing and detecting "**Serious Crime**". This means the offences it relates to must be:

- capable of attracting a prison sentence of 12 months or more or
- committed by a person who is not an individual (e.g. a corporate body)
- an offence involving violence
- involve the sending of a communication or breach of a person's privacy.

9.2 Successful applications must satisfy tests for necessity and proportionality, as with Part 2 Surveillance and CHIS applications. The purpose of any IPA application for Communications Data must relate to a matter that is the statutory or administrative function of the Local Authority.

9.3 Only people who have successfully completed Home Office accreditation may deal with Communications Service Providers on these issues and will act as a Single Point of Contact (SPOC). The only permitted SPOC for Local Authorities is the National Anti-Fraud Network (NAFN) housed by Tameside Council. The SPOC will act as a gatekeeper in relation to necessity and proportionality and make initial enquiries as to feasibility and will then submit any applications considered to meet the tests to the Office for Communications Authorisations (OCDA) for consideration for approval.

9.4 This means that internal authorisation and judicial approval are not required. However, the Senior Responsible Officer or a Designated Senior Officer will be made aware of any application.

10. Records

10.1 The Monitoring Officer maintains a central, retrievable register of all Notices or Authorisations granted within the preceding three years. This is maintained by the Legal Services Team.

11. Oversight by Members

11.1 Elected members will review the Authority's use of RIPA and the RIPA Policy at least once a year.

A format for summary of use is at Appendix 2.

Appendices

Appendix 1: Authorising Officers/Designated Senior Officers

- Head of Paid Service/Chief Executive (Senior Responsible Officer) – Karen Bradford
- Deputy Chief Executive (Authorising Officer/Designated Senior Officer) – Richard Wyles
- Monitoring Officer (Authorising Officer/Designated Senior Officer) – Graham Watts
- Head of Public Protection (Authorising Officer/Designated Senior Officer) – Ayeisha Kirkham

Appendix 2: Format for Summary of RIPA Use

Services making use of RIPA: Housing, Planning, Public Protection and Revenues and Benefits.

Statement of General Purposes: South Kesteven District Council uses powers made available to it under RIPA in order to investigate and prevent crimes in areas such as flytipping, unlicensed activities, rogue landlords or breach of environmental health legislation. These powers are used only when necessary. They have successfully assisted in bringing flytippers and other criminals to court resulting in successful prosecutions.

RIPA is aimed at safeguarding Human Rights and provides a framework to ensure that the authority's actions are necessary and proportionate. It allows our decisions to be externally audited and it is only to prevent and detect crime that a local authority is allowed to conduct non-intrusive surveillance.