Use of Authorised Covert Surveillance

Regulation of Investigatory Powers Act 2000 (RIPA)

Dorset Council

Contents

Purpose of the Use of Authorised Covert Surveillance Policy

This policy explains how Dorset Council will manage covert surveillance activity, including how the Council will comply with the Regulation of Investigatory Powers Act 2000 (RIPA) when authorising directed surveillance under Section 28(1) of RIPA, covert human intelligence sources under Section 29(1) of RIPA and obtaining communications data under Section 22(3) and 22(4) of RIPA. It also sets out the procedures to be adopted in compliance with the Investigatory Powers Act (IPA) 2016.

This Policy is supplementary to the relevant provisions of any code of practice issued under RIPA (see RIPA codes - GOV.UK (www.gov.uk) and IPA (see Investigatory Powers Act 2016 – codes of practice - GOV.UK (www.gov.uk). The policy also applies to authorised surveillance not subject to RIPA legislation, but where good practice should be applied to the authorisation process (referred to as "RIPA light").

This policy is appropriate for all officers involved in any form of surveillance as part of their duties, or for the authorisation of such surveillance. It supersedes the Regulation of Investigatory Powers Act 2000 policy that was approved by Shaping Dorset Council Shadow Executive on 11 March 2019.

1. What is Surveillance?

1.1 Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications (including within social media). It also includes recording any of the aforementioned activities. It can be 'overt' or 'covert'.

1.2 For clarification, covert surveillance is surveillance carried out without the knowledge of the individual subject to the surveillance. Overt surveillance is where the devices used are both visible and obvious.

1.3 There are two types of 'covert' surveillance. **Directed surveillance** and **intrusive surveillance.**

1.4 Directed surveillance is defined as being "covert, but not intrusive, carried out for the purposes of a specific investigation or operation related to preventing or detecting a crime and likely to result in the obtaining of private information about a person or persons".

1.5 Intrusive surveillance meanwhile is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device). Surveillance equipment mounted outside the premises will not be intrusive unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle. Intrusive surveillance **cannot** be carried out or approved by the Council. Only the police or other law enforcement agencies

are permitted to use such powers. Likewise, the council has no statutory powers to interfere with private property.

1.6 Most of the surveillance carried out by the Council is done overtly – there is nothing secretive or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues). Surveillance is "covert" if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

2. What Legislation Applies to Surveillance?

2.1 Regulation of Investigatory Powers Act (RIPA) 2000
The Regulation of Investigatory Powers Act (RIPA) was introduced in 2000 to give public authorities a legal framework to follow if they are carrying out covert surveillance. Local authorities have always been able to carry out surveillance - RIPA now regulates that use and provides the council with protection against any breach of Article 8 of the Human Rights Act.

2.2 Local authorities are only allowed to carry out surveillance under RIPA for preventing or detecting a criminal offence which would be punishable by a prison sentence of at least twelve months. Currently under RIPA we can only carry out directed covert surveillance.

2.3 Before using RIPA we need to show a valid reason for its use and consideration will be given to the use of less intrusive methods first. We also have to obtain magistrate's approval before any surveillance is carried out. As such, the use of activities under RIPA will be as a last resort and the Council will not look to undertake such activities unless absolutely necessary. Authorisations will be undertaken by Authorising Officers as set out in 4.2. The RIPA authorisation forms can be found on the Gov.uk website RIPA forms - GOV.UK (www.gov.uk).

2.4 If the Authorising Officer is satisfied that the surveillance is necessary and proportionate, they will instruct Legal Services to seek approval from a Justice of the Peace sitting at the Magistrates' Court. Legal Services will request a hearing date from the Court. The time taken to obtain a hearing date from the Court will need to be taken into account when scheduling any proposed surveillance.

2.5 At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer, together with any supporting documents relevant to the matter showing the necessity and proportionality of the authorisation and which contain all the information relied upon. Also included will be a summary of the circumstances of the case. The hearing will be in private heard by a single Justice of the Peace (Magistrate / District Judge) who will read and consider the application.

2.6 Whilst RIPA activities are a last resort, there will be occasions where covert surveillance will be required but where the statutory criteria for a formal RIPA authorisation are not met (for instance, certain trading standards activity; internal audit investigations). In such cases the

Council will adopt an internal authorisation procedure which mirrors the good practice set out in RIPA and the associated codes of practice (defined in this policy as "RIPA light"). This will be subject to a similar authorisation process, but will not require approval of a magistrate. Authorisations will be undertaken by Authorising Officers as set out in 4.2. The "RIPA Light" authorisation form is set out in Appendix A.

2.7 A central record will be maintained of all authorisation forms. As per the Council's Records Retention policy these will be retained for a period of three years from the cancellation of the authorisation.

2.8 Investigatory Powers Act 2016
Whilst RIPA provides a statutory framework for the authorisation of certain types of covert intelligence, the Investigatory Powers Act 2016 (IPA) sets out the extent to which certain investigatory powers may be used to interfere with privacy. In particular about the interception of communications, equipment interference and the acquisition and retention of communications data.

2.9 The term "communications data" includes the "who", "when", "where", and "how" of a communication rather the content of what was said or written. It includes the way in which, and by what method, a person communicates with another person. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication. It can however include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

2.10 The acquisition of communications data is permitted under Part 3 of the IPA and will be a justifiable interference with an individual's human rights under the European Convention on Human Rights only if the conduct being authorised or required to take place is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with law. In such instances, you should make contact with the Senior Responsible Officer (the Director for Legal and Democratic Services).

3. Safeguards

3.1 The Council will apply a presumption in favour of overt investigation methods. So, the Council will always look to investigate matters using a variety of overt investigatory tools, before considering whether the use of these powers is required. Directed surveillance, using covert human intelligence sources or obtaining communications data (collectively described in this policy as "covert surveillance") will be used only when other reasonable options have been considered, and ruled out.

3.2 The Council will use covert surveillance proportionately. So, the Council will not use covert surveillance to address minor matters, but instead will focus on those issues which are of greatest concern to the community, so, the Council will:

(a) balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence, or disorder;

(b) explain how and why the methods to be adopted will cause the least possible intrusion on the target and others; and

(c) evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.3 Without prejudice to paragraph 3.2 no authorisation for the carrying out of directed surveillance will be granted unless the authorisation is “necessary” for the purposes of preventing or detecting crime and in the case of directed surveillance a crime punishable by a maximum term of at least 12 months imprisonment or for the purpose of preventing or detecting certain other specified offences.

3.4 The Council will only use covert surveillance either to obtain evidence that can be presented at court, or where another positive outcome relating to the prevention or detection of crime has been identified, for example through the positive identification of perpetrators.

3.5 In addition, the interception of Council telecommunications will only be carried out in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and following procedures agreed by the Director for Legal and Democratic Services in the following circumstances:

- to establish the existence of facts or to ascertain compliance with regulatory or self-regulatory practices (e.g. to keep records of communications where the specific facts are important);
- to check the standards are being achieved or ought to be achieved;
- to prevent or detect crime (e.g. to check that employees or others are not involved in defrauding the Council);
- to investigate or detect unauthorised use of the telecommunications system; or
- to ensure the security of the system and its effective operation.

3.6 Non-compliance with RIPA and IPA may result in a complaint to the Investigatory Powers Commissioners Office and/or the Local Government and Social Care Ombudsman, a compensation claim and ultimately evidence obtained being disallowed by the courts.

4. Responsibilities

4.1 Senior Responsible Officer

The Director for Legal and Democratic (Monitoring Officer) is the senior responsible officer, who is responsible for:

- Maintaining the integrity of RIPA processes within the Council;
- ensuring compliance with the relevant provisions of RIPA and the codes of practice; and
- engaging with the Investigatory Powers Commissioner's Office and overseeing the implementation of post-inspection action plans.
- Reporting annually to the Audit and Governance Committee on the Council's use of RIPA, as part of the Annual Information Governance report.

4.2 Authorising Officers

The Council will ensure that authorising officers are at Service Manager level as a minimum. The following posts have been designated as authorising officers:

- Service Manager for Assurance
- Service Manager for Business Intelligence and Performance
- Service Manager for Democratic and Electoral Services
- Service Manager for Trading Standards

4.3 Where there is the likelihood of confidential information (see 4.4) being obtained, or in the event of absence of the authorising officers set out in 4.2, authorising officers will instead be at Corporate Director level as a minimum. This will avoid any perception that authorising officers are directly involved with the investigations they authorise. Authorising officers will therefore be able to apply more independently reasoned judgment of the issues. In the event that an authorisation under RIPA legislation is required, surveillance cannot be carried out until an order has been made by a Magistrates Court approving that authorisation.

4.4 Confidential Information for these purposes means: i) information that has been provide in confidence, identifies an individual (whether living or dead) and relates to that person's physical or mental health or spiritual counselling; ii) information about confidential discussions between members of Parliament and their constituents; iii) confidential journalistic material; and iv) information to which legal professional privilege attaches.

4.5 The Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorising Officers may not sub-delegate their powers to other officers.

4.6 The Authorising Officer should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

4.7 The Executive Directors are responsible for:

- Ensuring all applicants within their service areas are aware of this policy and the requirements of RIPA;

- ensuring all authorising officers within their service areas are trained in RIPA and meet the standards required by the Investigatory Powers Commissioner's Office.

4.8 RIPA Co-ordinating Officer

The **Data Protection Officer** will be the RIPA co-ordinating officer and is responsible for:

- maintaining a central record of authorisations and collate the original applications/authorisations, reviews, renewals and cancellations;
- monitoring the quality of notices and authorisations; and
- ensure an appropriate and proportionate training regime exists.

4.9 Information Asset Owner

The **Service Manager for Assurance** will be the Information Asset Owner for completed authorisations and will ensure that they are retained in accordance with the Council's records retention policy.

4.10 Officers engaged in covert surveillance

All officers engaged in covert surveillance will:

- be familiar with RIPA, the relevant codes of practice and the Investigatory Powers Commissioner's Office procedures and guidance;
- provide the authorising officer with all the information necessary for an informed decision to be made as to whether an authorisation should be granted or cancelled;
- advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance; and
- cease the use of covert surveillance when it no longer meets the authorisation criteria.

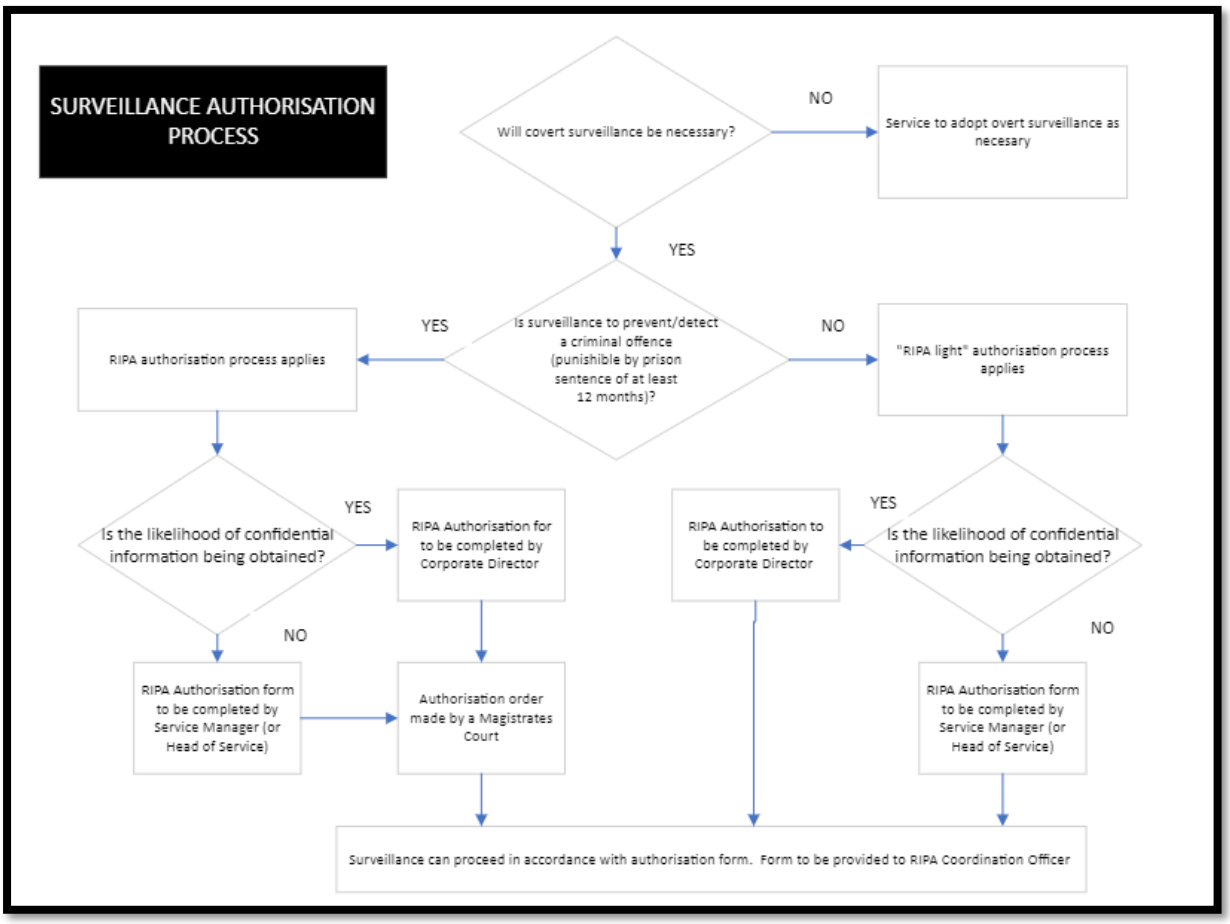
4.11 Audit and Governance Committee

Will review and approve the RIPA policy every three years, and more regularly where dictated by changes to process or legislation. The Committee will also receive an annual update on RIPA activity, as part of the Annual Information Governance report. This will include:

- The number of RIPA authorisations requested and granted, including joint operations where RIPA authorisation has been sought and granted by another authority;
- The number of RIPA light authorisations requested and granted;

- The number of times social networking sites have been viewed in an investigatory capacity

4.12 The authorisation process is summarised in the chart below:



5. Social Media

5.1 Officers and members may use social media on a regular basis, both for work and personally. When joining a social media group in an official capacity you should only do so by using a Dorset Council account, not a personal account, and membership of that group should be declared so that members of that group are aware.

5.2 The use of internet and social networking sites may be deemed to be covert surveillance if used to gather evidence or monitor an individual's status by viewing more than once. In such cases, it will only be permitted once an authorisation is in place (whether RIPA or "RIPA light"). Where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, you should consider if RIPA authorisation applies.

5.3 When conducting an investigation which involves the use of the internet factors to consider are:

- officers must not create a false identity in order to “befriend” individuals on social networks without an authorisation under RIPA;
- officers viewing an individual’s public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual’s status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and
- officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

5.4 The social media policy clearly sets out what is appropriate and inappropriate use of social media, whether you use it for work or on a personal basis in your own time.

6. Training

6.1 Appropriate corporate training will be arranged by the RIPA Monitoring Officer for all officers likely to make applications or authorise them. It is the responsibility of Authorising Officers to ensure that they have carried out the training prior to undertaking any authorisation. Training should be refreshed every three years.

7. Further Information

7.1 If you require any clarification on the policy and its supporting processes, please contact the Data Protection Officer, as the identified RIPA Co-ordinating Officer.

8. Review

8.1 This policy will be subject to review by the Audit and Governance Committee every three years, or earlier if dictated by change of legislation. The Committee will consider a report on the Council’s use of RIPA powers annually, as part of the Annual Information Governance report.

Policy Owner: Marc Eyre, Service Manager for Assurance

Date Approved: Audit & Governance Committee (To be presented 15 January 2024)

Review Date: January 2027