Regulation of Investigatory Powers Act 2000 (RIPA)

Policy Document

September 2018

Contents

Appendices

RIPA authorisations

1a Application for Authority to Conduct Directed Surveillance

1b Application for Renewal of Authority to Conduct Directed Surveillance

1c Application for Cancellation of Authority to Conduct Directed Surveillance

Covert Human Intelligence Source (CHIS)

1m Application for Authority to Use a Covert Human Intelligence Source (CHIS)

1n Application for Renewal of Authority to Use a Covert Human Intelligence Source (CHIS)

1o Application for Cancellation of Authority to Use a Covert Human Intelligence Source (CHIS)

Part 1

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime.

1. INTRODUCTION

1.1 Covert surveillance is surveillance that is carried out in a manner calculated to ensure that the person(s) subject to the surveillance are unaware that it is or may be taking place. Deployment of overt surveillance is increasingly common in places to which the public have access and this Council has employed it in the form of CCTV monitoring of its offices, car parks and the town centre areas of Dover, Deal and Sandwich for several years. From its inception in 1994, the Council's town centre CCTV scheme has been subject to a Code of Practice, which has been reviewed periodically to ensure compliance with relevant legislation and best practice. The Code applies to CCTV systems operated overtly in public places for the purposes of crime reduction, prevention and detection. The Code, together with the operating procedures, systems management and documentation based on it, take into account the requirements of the General Data Protection Regulation and the Data Protection Act 2018, together called Data Protection Law and the Human Rights Act 1998 (HRA) that must be observed in carrying out overt surveillance activities.

1.2 Advances in technology and social media use make it increasingly possible for covert surveillance to be carried out. Interception of communications via the Internet and telephone is now technologically possible and covert surveillance also includes observation with the naked eye.

1.3 Covert surveillance is the subject of legislative controls. The requirements of the Data Protection Law and the HRA that have to be borne in mind in overt surveillance need to be considered also in the area of covert surveillance. The Regulation of Investigatory Powers Act 2000 (RIPA) that came into force in October 2000 is of relevance whenever covert surveillance of an identifiable or named person is carried out by a public authority carrying out an investigatory function. RIPA includes a local authority within the description of public authority. Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

1.4 Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

1.5 Covert surveillance includes not only the use of CCTV but also the interception of communications via e-mail, the Internet, telephone or post. The Council is unlikely to make use of a covert human intelligence sources (CHIS) and anyone considering to do so must consult the Legal Services department. The use of (CHIS) is also regulated by RIPA. Under the 2000 Act, a person is a CHIS if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
(b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or
(c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

1.6 Covert surveillance can be either

(a) intrusive, that is carried out in relation to anything taking place in any premises used for residential purposes, or in any private vehicle, (including car, boat, aeroplane,) and involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device: or,

(b) directed, namely, undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather private information about them.

Local Authorities are not authorised by RIPA to conduct intrusive surveillance.

1.7 Council officers will at times need to conduct directed surveillance in the course of carrying out the Council's investigatory functions. Officers will on occasions need to conduct that surveillance covertly whether the subject of the surveillance is a member of the public or a Council employee. There will also be situations where the use of a CHIS, who can be a Council officer, is required. Examples include the use of a professional witness to obtain information and evidence and in potential entrapment cases. If use of a CHIS is to be considered, you must discuss this in advance with the Council's Legal Services Department.

1.8 Subject to para. 1.9, covert surveillance must be carried out within the provisions of the relevant legislation and only commence when authorisation has been granted in accordance with the provisions of this policy.

1.9 In genuinely exceptional circumstances, use of surveillance outside of RIPA and this policy may be approved. Approval must be by both the Head of Paid Service and the Monitoring Officer. The circumstances and reasons in such a case must be genuinely exceptional, fully documented and the case must be kept under constant review.

1.10 This policy document clarifies the circumstances in which Council officers will be permitted to embark on a covert surveillance operation and the requirements that will need to be observed in order that the Council will neither contravene the relevant legislation nor the national Codes of Practice issued by the Home Office, the Investigatory Powers Commissioner's Office and the Office of the Information Commissioner. Obtaining appropriate authorisation for any form of surveillance will be of importance to ensure that any evidence obtained is not to be judged inadmissible in any subsequent legal proceedings as well as to provide the Council with some protection if the surveillance activities of its officers are ever challenged under the HRA, Data Protection Law, as part of a Judicial Review of a Council decision or in any reference to the Ombudsman.

2. RELEVANT LEGISLATION

2.1 The General Data Protection Regulation 2016 (GDPR)

2.1.1 GDPR provides six principles to be observed to ensure that the requirements of the Act are complied with. They provide that personal data, which includes personal data obtained from covert surveillance techniques, must be:

(1) Processed, lawfully, fairly and in a transparent manner;
(2) Collected for specified, explicit and legitimate purposes;
(3) Adequate, relevant and limited to what is necessary;
(4) Accurate;
(5) Kept for no longer than is necessary;
(6) Processed in a manner than ensures appropriate security;

In collecting data under the RIPA umbrella, the Council must be able to demonstrate compliance with the above principles.

2.2 The Human Rights Act 1998

2.2.1 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights. Article 8 of the Convention is relevant in the context of covert surveillance in that everyone has the right to respect for his/her private and family life, home and correspondence. It is now clear from decided cases that this right extends to activities of a professional or business nature and so includes employees. Article 6 of the Convention is relevant in the context of covert surveillance in that everyone has the right to a fair trial, including internal procedures or hearings, and fairness extends to the way in which evidence is obtained.

2.2.2 Consequently, there is to be no interference with the exercise of these rights by any public authority, including a local authority, except where such interference 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 the protection of the rights and freedoms of others.

2.3 The Regulation of Investigatory Powers Act 2000

2.3.1 This Act and its associated regulations also follow the philosophy of recent legislation in trying to strike a balance between community responsibilities, including effective law enforcement, and individual rights and freedoms.

2.3.2 The Council has the right to request certain data via the National Anti-Fraud Network (NAFN), from any communication service provider where the information is necessary in order to prevent or detect crime, or prevent disorder. NAFN provides the Single Point of Contact (SPOC) in relation to the Investigatory Powers Act 2016. Communication service providers (CSPs) cover three main areas, being the telephone, internet service providers and postal services. In all cases there is a formal request and authorisation procedure which must be followed. The Councils' process follows the Code of Practice on Acquisition and Disclosure of Communications Data (revised 2015).

2.3.3 Directed covert surveillance, including a situation where a CHIS is used, that is likely to result in obtaining private information about a person is permitted by RIPA and its associated regulations if such surveillance has been authorised in the manner provided by the Act, the Home Office Code of Practice and the prescribed standard forms. Authorisation for directed surveillance can be granted by the Authorising Officer of a local authority, together with judicial approval, only if it is for the purpose of preventing or detecting crime or of preventing disorder. The Authorising Officer is the Monitoring Officer or his nominated deputy. The Senior Responsible Officer (SRO) is the Head of Paid Service.

2.3.4 The various application forms to complete for authorisation to carry out, extend or cancel covert surveillance in any of these circumstances are attached to this policy document.

2.3.5 Approval of Local Authority Authorisations under RIPA by a Justice of the Peace: Local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving that authorisation or notice has been granted by a Justice of the Peace (JP).

2.3.6 Directed surveillance crime threshold: a local authority can only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

3. IMPLEMENTATION

3.1 This Policy was originally developed in consultation with representatives from all departments in September 2001.

3.2 This Policy applies to all Council staff and contractors employed by the Council. All relevant Council contracts will include a term that this Policy and the Council's associated procedures are to be observed by any contractor operating on behalf of the Council.

3.3 Any enquiries about the policy should be referred to the Monitoring Officer or the Corporate Services team.

3.4 The Home Office Covert Surveillance and Property Interference Code of Practice require that Members approve the Councils RIPA Policy at least annually and they should receive on a regular basis reports on the use of powers under RIPA. In view of the low usage of powers under RIPA by the Council, this will be reported as the annual policy review.

3.5 This policy will be subject to annual review to ensure that it remains compliant with all relevant legislation, regulation and Home Office guidance.

Part 2

4. POLICY

4.1 General - All forms of covert surveillance

4.1.1 The Council will conduct its covert surveillance operations, including the interception of telecommunications, within the General Data Protection regulation's six principles and restrict those operations to situations falling within the permitted exceptions of the HRA and RIPA.

4.1.2 The Council's powers in relation to RIPA authorised covert surveillance are restricted to those for the purpose of preventing or detecting crime or of preventing disorder.

4.1.3 In respect of telecommunications systems, the Home Office has agreed with the CSPs that every Authority shall channel all requests for information from them through a Single Point of Contact (SPOC), the National Anti-Fraud Network. All applications must be made electronically through the NAFN secure online portal http://www,nafn.gov.uk. The NAFN act as the Council's SPOC to ensure a centralised and managed approach in making applications for communications data.

4.1.4 Surveillance equipment will be installed, a CHIS used, or communications information sought for legitimate purposes only, when sufficient evidence exists and has been documented to warrant the exercise and surveillance is shown to be both the least harmful means of meeting that purpose and proportionate to what it seeks to achieve. It is extremely important that all reasonable alternative methods to resolve a situation, such as naked-eye observation, interview or changing methods of working or levels of security, must be attempted first and recorded in writing and the reason for surveillance being requested fully documented. Where the subject of covert surveillance is an employee, the Head of Paid Service and Monitoring Officer must be informed to ensure compliance with the Council's other relevant policies.

4.1.5 All requests to conduct, extend or discontinue a covert surveillance exercise must be made in writing on the relevant form provided as per the Appendices. All such requests must be submitted for initial consideration to the Corporate Services Officers, this includes requests for telecoms information from the SPOC, who have responsibility in consultation with the Monitoring Officer for co-ordinating covert surveillance within the Council. All requests that are approved at this initial stage must then be considered by the Monitoring Officer as the Council's Authorising Officer, or their nominated deputy, to approve or refuse the request (but please see 4.1.6).

4.1.6 Where confidential material is likely to be obtained or where there is to be the deployment of a juvenile or vulnerable adult as a CHIS the Head of Paid Service shall act as the Authorising Officer rather than the Monitoring Officer.

4.1.7 The Council must then obtain an Order from a Justice of the peace approving the request before the authorisation can take effect and the activity carried out. All requests must be authorised in writing.

4.1.8 Authorisation will only be granted where covert surveillance or use of a CHIS is believed by the Authorising Officer, or their deputy, to be necessary and proportionate to what is being sought to be achieved by carrying out the surveillance. This would then be subject to judicial approval. The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

4.1.9 Before authorising applications for directed surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions.

4.1.10 Once the Authorising Officer has authorised the directed surveillance or CHIS a hearing will be arranged at the appropriate Magistrates' Court. The Legal Services Department will present the application for approval at the hearing. It is not sufficient to provide oral evidence where it is not reflected or supported within the completed application. The Justice of the Peace will consider whether he/she is satisfied that the authorisation was necessary and proportionate. They will also consider whether the authorisation was given by the appropriate designated person within the Council and, in the case of directed surveillance, the crime threshold has been met.

4.1.11 Written authorisations for a covert surveillance operation will be valid for a maximum of three months from the date of approval by the Justice of the Peace, but will be subject to review within that period to establish whether the authorisation should continue for the entire three month period

4.1.12 The power to discontinue authorisations will be limited to the Authorising Officer only in order to ensure greater independence and consistency.

4.1.13 An existing authorisation can be renewed on the same terms as the original at any time before the original ceases to have effect. The renewal must then be approved by a Justice of the Peace in the same way the original authorisation was approved. The time in which to get judicial approval should be factored in when seeking to get an extension of authorisation.

4.1.14 Surveillance that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to get authorisation falls outside the definition of directed surveillance and therefore authorisation is not required. If later, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced. Embarking upon covert surveillance or the use of a CHIS without authorisation or judicial approval, or conducting covert surveillance outside the scope of the authorisation will not only mean that the 'protective umbrella' of RIPA is unavailable but may result in disciplinary action being taken against the officer/officers involved.

4.1.15 In circumstances where the Council's town centre CCTV overt surveillance system is to be used in a targeted operation at the request of the Police or Customs and Excise, the Head of Paid Service or, in their absence, the Monitoring Officer, and a Police Superintendent or Customs and Excise Officer of equivalent rank will authorise such activities using an abridged version of the forms contained in the Appendix to this document.

4.1.16 Surveillance equipment will only be installed with the authorisation of the Council's Authorising Officers. It will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council and such matter can only be investigated with the aid of covert surveillance techniques. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant. Intrusive surveillance (see paragraph 1.4) cannot be authorised by RIPA, and will not be carried out.

4.1.17 Any request by a Council officer to a resident to keep a video diary as part of an evidence-gathering exercise will be regarded as a covert surveillance exercise conducted on behalf of the Council and must be authorised as such. In respect of noise nuisance, where notice is given to the alleged offender that recordings will be made, monitoring the falls out of the scope of RIPA, as the evidence will then be collected overtly.

4.1.18 The Corporate Services Team/ SPOC will retain the originals of all authorisation documents and maintain a register of all requests and authorisations for covert surveillance together with the reasons for any request being denied in accordance with Home Office Guidance.

4.1.19 No covert operation will be embarked upon by a Council officer without detailed consideration of the insurance and health and safety implications involved and the necessary precautions and insurance being put in place.

4.1.20 During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed daily and access to it will be restricted to the Corporate Services Team, the Authorising Officer and the authorised officer concerned. The Monitoring Officer, acting in that role, will decide whether to allow requests for access by third parties including Council officers. Access will generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings). The current separate arrangements in place in respect of the Council's town centre CCTV operations for the security and review of information and access to it will continue to apply.

4.1.21 A register will be maintained by the officer concerned of all reviews of material recorded and collected covertly. The current separate arrangements in place in respect of the Council's town centre CCTV operations will continue to apply.

4.1.22 Where digital recordings are made, they are only retained on our recorders for a period of 30 days and then automatically wiped. Any digital download is only kept for 30 days and then destroyed. Downloads carried out are on to discs supplied by Kent Police and are immediately sealed, then stored in a secure cabinet to await collection. If they are not collected within a 30 day period they are destroyed. All collected downloads are signed for prior to release.

4.1.23 Once a covert operation results in an individual being under suspicion of having committed a criminal or disciplinary offence, he/she must be informed of this as promptly as is reasonably practicable in order to ensure his/her right to a fair trial or hearing within a reasonable time in accordance with the HRA. In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be under caution and conducted by a suitably trained officer or, if appropriate, the police must be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed. The register of recordings will include a note of any recorded material handed over to the police.

4.1.24 Any failure to comply with the procedures in place for the implementation of the covert surveillance policy will be a disciplinary offence.

4.1.25 The Monitoring Officer has responsibility for ensuring Home Office Guidance and the recommendations of any inspectorate are complied with in respect of the administration & implementation of RIPA.

4.2 General Applications

4.2.1 All applications should be made using the appropriate application form, submitted to the Corporate Services team. Details on the form should be sufficient to demonstrate that all other avenues of investigation have been tried / considered, and to show that the proposed surveillance is proportionate. Where possible the extent / impact of the crime should be noted.

4.2.2 Applications should be supported by the addition of plans / maps to show the positioning of any surveillance equipment.

4.2.3 The proposed application will be discussed with the Community Safety and CCTV Manager, to ensure that, to the best of their knowledge, the surveillance will not interfere with or jeopardise any other operation being undertaken within the District by the Council or by any of our partners. Where there is a potential conflict with an existing operation the proposed application may need to be delayed and the effect of this will be discussed with the officer putting forward the application.

4.2.4 The surveillance should cease and the application should be cancelled as soon as sufficient evidence is available to either clear the target or to prove their involvement in crime.

4.2.5 Where the surveillance needs to continue past the initially approved timescale, the application should be renewed on a timely basis, taking account of any new information gathered to ensure that the continuing surveillance remains proportional.

4.2.6 Where collaborative surveillance is being undertaken, there is no need for both/all parties to seek authorisation for the operation. Home Office Guidance states that the tasking authority should usually provide the authorisation. Officers should therefore be clear when undertaking joint work, who is the tasking authority. It should however be borne in mind that other authorities, e.g. police, have greater powers, and that the Councils' powers in relation to surveillance are restricted to directed surveillance for the purpose of preventing or detecting crime or of preventing disorder.

4.2.7 Where possible, public authorities should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where two agencies are conducting directed surveillance as part of a joint operation, only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

4.3 Surveillance of non-Council Telecommunications

4.3.1 Information available from Communication Service Providers (CSPs).

4.3.1.1 The Council access is restricted to two classifications of data –
(a) Information about the use of the service, Section 21(4)(b) and / or
(b) Information about the service user (subscriber), Section 21(4)(c).

A separate application form is required for each classification of data.

4.3.1.2 Service Use Information includes the following-

- Itemised list of telephone numbers called
- Itemised connection records to internet services
- Itemised timing and duration of service usage
- Information about the connection, disconnection and reconnection of services
- Information about the provision and use of forwarding / redirection services (both postal and telecoms services)
- Information about call waiting, call messaging, conference calling and similar telecoms services
- Records of postal items, such as registered, recorded or special delivery postal items, parcel consignment, delivery and collection.

4.3.1.3 Subscriber Information includes the following-

- Subscriber information (e.g. who is the subscriber to a particular telephone number / e-mail account / web address)
- Subscribers account information, including payment method
- Address for both the installation and for billing purposes.
- Any abstract data held by the CSP (demographic details etc, but not, for example, passwords).

4.3.2 All applications must be made electronically through the NAFN secure online portal http://www.nafn.gov. NAFN act as the Council's single point of contact (SPOC). This is to ensure a centralised and managed approach is undertaken when making applications to obtain communications data.

4.3.3 NAFN is authorised to request Category B and Category C communications data from CSPs on behalf of the local authority.

4.3.4 NAFN will be notified of the Council's Designated Persons. Applicants and Designated Persons can submit, approve and track applications through the NAFN secure online portal

4.3.5 The NAFN's SPOC will review all applications for legal compliance prior to approval by the Designated Person. All Applicants must be authorised by the Designated Person before NAFN will assign them with a website username and password. Each application will be allocated a universal reference number by NAFN. Applications will only be approved by the Designated Person where they consider the application to be both necessary and proportionate to the investigation.

4.3.6 Following approval by the DP, NAFN will prepare the court documentation for the Applicant to obtain judicial approval. The Applicant must upload the Magistrate's Order to the NAFN portal. NAFN will request the communications data from the CSP and provide the results to the Applicant via the portal.

4.3.7 Authorisations are only valid for a maximum of one month from the date of the Notice or Authorisation, although they can be renewed subject to judicial approval. If no longer necessary or proportionate they must be cancelled. NAFN will undertake the cancellation process and notify the Designated Person and CSP.

4.3.8 Information obtained under these regulations is to be handled in strictest confidence. The application form should indicate who will be privy to the information, including, where other

partners / agencies may be involved in the investigation and if they are likely to need to know the data. Disclosures should be necessary and proportional to the investigation.

4.4 Social Networking and Internet Sites

4.4.1. 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.

4.4.2 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).

4.4.3 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.

4.4.4 As set out in paragraph 4.4.5 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 still apply. This is because the intention when making such information available was not for it to be used for a covert purpose 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.

4.4.5 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 likely to hold a reasonable expectation of privacy in relation to that information.

4.4.6 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. These considerations apply regardless of when the information was shared online, for example:

A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

4.4.7 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

4.4.8 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

4.4.9 Where directed surveillance authorisation has been granted for accessing information on a website/social media site a record shall be kept of the date and time of each visit and details of the website/social media site viewed. The record shall state whether any information viewed was downloaded, stored or recorded in any way.

4.4.10 In the normal course of business of the Council approval would not normally be given for the use of covert profiles. The use of this technique may be approved in genuinely exceptional circumstances. Approval must be by both the Head of Paid Service and the Monitoring Officer. The circumstances and reasons in such a case must be fully documented and the case must be kept under constant review

5. AUTHORISATION TESTS

5.1 Authorisation will be required for a proposed activity if the answer is 'Yes' to all of the following questions.

5.2 If the answer is 'No' to any of the following questions, the proposed activity will not be entitled to protection under RIPA and authorisation will not be granted so should not be the subject of an application request.

(a) Is the proposed activity 'surveillance'? The officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.

(b) Is it 'covert'? The officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.

(c) Is it 'directed'? The officer must decide whether the proposed activity is for the purposes of a specific investigation / operation.

(d) Is it likely to result in obtaining private information about a person? The officer must decide whether any information about the target's / targets' private or family life is likely to be obtained. This test is different from: 'Is there the faintest chance that I will obtain private information?'

(e) Is it a 'foreseen/planned response'? The officer must decide whether the proposed activity is something other than an immediate response in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the immediate reaction to events happening in the course of the officer's work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been 'Yes'.

Any enquiries about the policy should be referred to the Corporate Services team.

DOVER DISTRICT COUNCIL PROCEDURE:

APPLICATION TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

DDC investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

Yes / No

Does the offence being investigated attract a custodial sentence of 6 months or more ?

No / Yes

Is the offence being investigated either: Section 146/147/147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1993

No / Yes

Investigator may **not** use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met **if** further offences come to light as the case progresses.

Complete RIPA authorisation/notice form and seek approval of authorising officer/designated person as per current arrangements. Complete judicial application form

Within Office Hours
The Legal team will contact the Courts to arrange a hearing

An officer from the Legal team will attend court with the signed RIPA authorisation and judicial application.

Outside usual office hours:
A JP may consider an authorisation out of hours in **exceptional** circumstances. If urgency is agreed, arrangements will be made for a suitable JP to consider the application.

You will still need to provide a completed authorisation form to accompany the judicial application form.

Outcome

Refuse to approve the grant or renewal and quash the authorisation or notice.

This may be appropriate if the JP considers that an application is fundamentally flawed. The court will give at least 2 business days in which to make representations before the authorisation is quashed.

Refuse to approve the grant or re-newal of an authorisation or notice.

The grant or renewal of the RIPA authorisation or notice will not take effect and the use of covert surveillance can not be undertaken. The investigating officer may wish to address, for example, a technical error and reapply.

Approve the grant or re-newal of an authorisation or notice.

Covert surveillance may be used in this case.

The signed order and original RIPA authorisation/notice will be retained by the Corporate Services team.