Corporate Policy Regulation of Investigatory Powers Act 2000 (RIPA)

Version : October 2021

INDEX

Item Description Page

1. INTRODUCTION

1.1 This Corporate Policy is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ("RIPA"), the Home Office's Code of Practice for Covert Surveillance and property interference, and Covert Human Intelligence Sources ("CHIS") ("Codes"), and the Home Office guidance for local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance ("Guidance")

1.2 Selby District Council (the "Council") has also taken into account and incorporated the guidance given by the Investigatory Powers Commissioner on 15 February 2021 and is grateful to them for providing this.

1.3 The Audit & Governance Committee has responsibility for monitoring the Council's use of the Regulation of Investigatory Powers Act 2000 for the use and authorisation of surveillance. As recommended in the Codes an annual report will be taken to the Council's Audit & Governance Committee, which will contain such detail to enable Committee to determine that the Council's policy is fit for purpose. The Report will include statistics relating to the level of RIPA activity or inactivity.

1.4 Whilst this policy provides guidance it is not intended to be an authoritative source on the provisions of RIPA. All Officers must therefore refer to RIPA itself and to the Codes, and the Guidance for an authoritative position.

1.5 Should any Officer be uncertain in respect of any aspect of RIPA, the authorising procedures set out in this policy, or at all, they should contact the legal department of the Council immediately.

1.6 The Solicitor to the Council is the RIPA Senior Responsible Officer and as such is responsible for:

- The integrity of the process in place within the Council to authorise directed surveillance and CHIS;

- Compliance with Part II of the 2000 and with the Codes;

- Oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- Engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;

- Where necessary, overseeing the implementation of any post – inspection action plans recommended or approved by a Judicial Commissioner, and

- Ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner's Office (IPCO)

2. LEGISLATIVE BACKGROUND

2.1 The Human Rights Act 1998 (the "HRA") incorporated the European Convention on Human Rights (the "ECHR") into domestic law.

2.2 Article 8 of the ECHR provides that:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. 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 protections of the rights and freedoms of others." [Emphasis added]

2.3 There is therefore a qualified right for interference with individual's rights under Article 8 if it is:

2.3.1 done in accordance with the law;

2.3.2 necessary; and/or

2.3.3 proportionate.

2.4 Any individual undertaking surveillance and/or using CHIS on behalf of the Council will therefore be breaching a person's human rights unless that surveillance is authorised in accordance with the law, is necessary for one of the reasons set out above, and is proportionate.

2.5 This could have serious implications for the Council, not only in terms of its reputation, but could also potentially render any evidence gathered during the surveillance inadmissible in criminal proceedings, leave the Council open to civil proceedings for a breach of an individual's human rights, and/or lead to a complaint being made to the Ombudsman. To avoid such a situation arising therefore, Officers must not carry out either Surveillance and/or CHIS unless the provisions of paragraph 2.3 are complied with.

In accordance with the law – RIPA

2.6 RIPA came into force on 25 September 2000, with the Codes subsequently coming into force pursuant to Section 71 of RIPA. The aim of RIPA was to strike a balance between protecting individuals' rights under Article 8 ECHR and the HRA and the need for investigatory powers to protect the interests of society as a whole. It therefore allows interference with individuals' rights in certain circumstances.

Necessity

2.7 It should be noted that pursuant to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence

Sources) Statutory Instrument No. 2010/521 **("RIPA Order 2010")** a local authority, (and hence the Council) **can only rely on Section 28 (3) (b) of RIPA as a ground for its interference being necessary**. Therefore, under RIPA any interference can **only** be necessary if it is "**for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least six months imprisonment.**"

2.8 Regulation 7A of the 2010 RIPA Order (as amended by the 2012 RIPA Order SI 2012/1500) introduced this further limitation so that Authorising Officers may only authorise surveillance in respect of a criminal offence which is punishable by a maximum term of at least 6 months imprisonment or which constitutes an offence under section 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

2.9 However, not all applications for the purpose set out above will be necessary. The Authorising Officer must be satisfied that it is necessary in all the circumstances. A judgment will have to be made on a case-by-case basis. Generally, any such interference will be not be necessary if there is an alternative overt method which could be used to obtain the information. Authorising Officers should therefore satisfy themselves that all other methods have either been exhausted or are not practicable. Authorising Officers should also take care to record in the authorisation their reasoning as to why the action is necessary.

Proportionate

2.10 Once it has been established that such interference is necessary it must then be considered whether it is proportionate to what is to be achieved. The Authorising Officer should consider the following elements of proportionality (as set out in paragraph 4.7 of the Code):

2.10.1 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

2.10.2 Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

2.10.3 Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought; and

2.10.4 Evidencing as far as reasonably practicable what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully

2.11 Authorising Officers should also take care to record within the authorisation form the reasons why they consider the action proportionate and must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

Judicial Approval

2.12 Following authorisation by an Authorising Officer judicial approval must be obtained prior to any surveillance being undertaken. Section 32A (2) of RIPA states that "*The authorisation is not to take effect until such time (if any) as the relevant judicial authority has made an order approving the grant of the authorisation*."

2.13 Section 32A (3) of RIPA further provides that:

"(3) The relevant judicial authority may give approval under this section to the granting of an authorisation under section 28 if, and only if, the relevant judicial authority is satisfied that

at the time of the grant there were reasonable grounds for believing that the requirements of section 28(2) were satisfied in relation to the authorisation, and

the relevant conditions were satisfied in relation to the authorisation, and

at the time when the relevant judicial authority is considering the matter, there remain reasonable grounds for believing that the requirements of section 28(2) are satisfied in relation to the authorisation.

(4) For the purposes of subsection (3) the relevant conditions are –

(a) in relation to a grant by an individual holding an office, rank or position in a local authority in England or Wales, that

the individual was a designated person for the purposes of section 28,

the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 30(3), and

any other conditions that may be provided for by an order made by the Secretary of State were satisfied…".

2.14 The procedure for making an application for judicial approval is contained in The Magistrates' Court (Regulation of Investigatory Powers) Rules 2012 (SI 2012/2563, and is explained further in the Guidance.

3. SURVEILLANCE

What is surveillance?

3.1 Surveillance includes:

3.1.1 Monitoring, observing, or listening to persons, watching or following their movements, their conversations or their activities or communications;

3.1.2 Recording anything mentioned above in the course of authorised surveillance; and/or

3.1.3 Surveillance, by or with, the assistance of a surveillance device.

3.2 Surveillance can be either overt or covert.

Overt Surveillance

3.3 The vast majority of surveillance, which the Council carries out, will be overt and will involve Officers and employees noting events in the course of their normal daily duties. This will not fall within the scope of RIPA and will not require an authorisation. For example, a dog warden who notes an offence being committed as he/she carries out their daily routine will not require RIPA authorisation as this is an immediate response to events.

Covert Surveillance

3.4 Covert surveillance is defined in section 26(9)(a) of RIPA. It provides that "*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*".

Surveillance not relating to specified grounds or core functions

3.5 An authorisation for directed surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation is necessary on the grounds specified in RIPA (Section 28(3)). Covert surveillance for any other general purposes should be conducted under other legislation, if relevant and an authorisation under Part II of RIPA should not be sought.

3.6 These core functions referred to are the 'specific public functions undertaken by the Council in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc). These ordinary functions are covered by the Data Protection Act 2018 and the Information Commissioners Employment Practices Code.

RIPA Part II

3.7 RIPA Part II applies to the following conduct:

3.5.1 Directed Surveillance

3.5.2 Intrusive surveillance

3.5.3 Covert Human Intelligence Sources

Directed Surveillance (Section 26(2) RIPA)

3.8 **Section 26(2)** defines directed surveillance as surveillance, which is:

3.8.1 Covert but not intrusive;

3.8.2 Undertaken for the purpose of a specific operation;

3.8.3 Undertaken 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); or

3.8.5 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 this Part to be sought for the carrying out of surveillance.

3.9 **Section 26(10)** defines "private information" in relation to a person as "*including any information relating to his 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. Family should be treated as extending beyond the formal relationships created by marriage or civil partnerships.

3.10 Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

3.11 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether

or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute covert surveillance, a directed surveillance authorisation may be considered.

3.12 Private Information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Online Covert Activity

3.13 The growth of the internet and the extent of the information which is now available online have presented new opportunities for the Council to view or gather information which may assist it in preventing or detecting crime.

3.14 Much of the information can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. However, it should be noted that 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.

3.15 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, if reasonable steps have been taken 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 required.

3.16 Depending on 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.

3.17 Where information about an individual is placed on a publicly accessible database, such as Companies House, which is commonly known to be available to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by 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.

3.18 Whether a public authority interferes with a person's private life includes 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 not likely to require a directed surveillance authorisation. However, where a public authority is systematically collating and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of whether the information was shared online. Paragraph 15 of the Code provides useful examples which will assist officers in their consideration of these issues.

3.19 Paragraph 3.16 of the Code sets out useful guidance on the factors to consider when determining whether authorisation should be sought for accessing information on a website as part of a covert investigation or operation. These 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.

Aerial Covert Surveillance

3.20 Where surveillance using airborne crafts or devices, i.e. drones, is planned, the same considerations outlined in chapters 3 and 5 of this code should be made to determine whether a surveillance authorisation is appropriate. When considering whether such

surveillance is covert, consideration should be given to the reduced visibility of a craft or device at altitude.

Intrusive Surveillance (Section 26(3)-(6))

3.21 **Section 26(3)** defines surveillance as intrusive if and only if it is covert surveillance that:

3.21.1 Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

3.21.1 involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.22 Pursuant to **Section 26 (5)** surveillance which:

3.22.1 Is carried out by means of a surveillance device in relation to anything taking place on a residential premise or in any private vehicle, but

3.22.2 Is carried out without that device being present on the premises or in the vehicle

is not intrusive **unless** the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3.23 Please note that there is **NO** provision for a local authority to authorise intrusive surveillance.

4. COVERT INTELLIGENCE SOURCES ("CHIS")

Who is a CHIS?

4.1 **Section 26(8)** of RIPA defines a CHIS as a person who:

(a) Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within (b) & (c) below;

(b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

4.2 This is defined further within **Section 26(9) (b) &(c)** so that:

4.2.1 A **purpose** will only be covert if, and only if, it is carried out in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4.2.2 A **relationship** is used **covertly**, and information obtained is **disclosed covertly**, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

4.3 Hence, there is no use of CHIS if a member of the public offers information to the Council that may be material to an investigation of an offence, but there would be if the Council then asked that person to obtain further information.

Authorising a CHIS

4.4 An authorisation must be obtained for CHIS in the same way as for directed surveillance. A detailed explanation of the authorisation

process is contained in **Section 5** below. However, in addition, to the process for considering whether an authorisation is justified, a CHIS should not be authorised if it does not comply with the requirements of **Section 29(5**) of RIPA.

4.5 **Section 29(5)** requires that:

4.5.1 There will at all times be a person holding an office, rank, or position with the relevant investigating authority who will have **day to day responsibility for dealing with the source** on behalf of that authority, and **for the source's security and welfare ("Handler")**;

4.5.2 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have **general oversight** of the use made of the source ("**Controller**");

4.5.3 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;

4.5.4 The records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State **(see below**); and

4.5.5 The records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

4.6 With regard to paragraph 4.5.4 above the regulations are set out in the Regulation of Investigatory Powers (Source Records) Regulations 2000.

These regulations can be found at

www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments

and must be referred to by Officers.

Security and Welfare

Before authorising the use of conduct of a CHIS the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of CHIS become known.

The ongoing security and welfare of the CHIS, after cancellation of the authorisation should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or at court.

The Handler will be responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS in so far as they might affect:

- The validity of the risk assessment;
- The conduct of the CHIS; and
- The safety and welfare of the CHIS. Where appropriate concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

Vulnerable Individuals

4.7 A vulnerable individual is a person who is or may need community care services by reason of mental or other disability, age, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Vulnerable individuals should only be authorised to act as a source in the most exceptional circumstances, and the Chief Executive may only give such an authorisation.

Juvenile sources

4.8 There are also special safeguards with regard to the use or conduct of juvenile sources (under 18 years).

4.9 A source under 16 years of age must not be authorised to give information against his parents or any person who has parental responsibility for him.

4.10 There are also further requirements within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793), and in other cases authorisations should not be granted unless these provisions are complied with.

A copy of this can be also be found at

www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments

and **must** be referred to by all Officers

4.11 The duration of such an authorisation is one month instead of 12 months.

4.12 Notwithstanding the above, the Council has not to date utilised these powers and considers that it is rare that they would be used in the future. As such only the **Chief Executive** may authorise any application for the use of CHIS and Officers should contact the legal department before making any application.

5. AUTHORISATION PROCESS

5.1 Directed surveillance and/or the use of CHIS shall be lawful for all purposes, if the conduct is properly and legitimately authorised and an Officer's conduct is in accordance with the authorisation.

5.2 Therefore all officers must obtain an authorisation from an Authorising Officer[1] and Judicial approval before undertaking either directed surveillance and/or the use of CHIS, to ensure that it is lawful. A flowchart setting out the steps to be taken is contained at page 17 of the Guidance which can be found at Appendix 3.

5.3 Authorisations will only be given where:

5.3.1 The directed surveillance and/or the use of CHIS is necessary in the interests of preventing or detecting crime or disorder where the offence is punishable by a maximum term of at least six months imprisonment; and

5.3.2 It is proportionate to the objective which it is intended to achieve.

5.4 The Authorising Officer must satisfy himself of this before granting the authorisation.

5.5 In particular the Authorising Officer must consider whether the activity could be carried out in an overt or less intrusive manner. If it could then this should be the preferred method.

Collateral Intrusion

5.6 Before granting an authorisation an Authorising Officer must take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

5.7 Wherever practicable measures should also be taken, to avoid or minimise unnecessary intrusion into the lives of those people. 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

[1] Head of Operational Services, Head of Planning, Director of Corporate and Commissioning, Director of Economic Regeneration & Place and the Chief Executive.

same proportionality tests should be applied to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

5.8 All applications must include an assessment of the risk of collateral intrusion in the application form. To ensure that the Authorising Officer is properly able to consider this the application should include:

- The scope of the anticipated surveillance;
- The likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject of the application.

Confidential Information

5.9 RIPA does not provide any special protection for "confidential information".

5.10 Notwithstanding this, special care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information may be involved.

5.11 Confidential information includes, matters subject to legal privilege, confidential personal information or confidential journalistic material.

5.12 For example special care should be taken with surveillance where it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

5.13 In cases where through the use of surveillance and/or CHIS, confidential information may be obtained, only the **Chief Executive**, or in his absence, a Director, may give authorisation.

Application Forms

5.14 All applications and authorisations must be made/granted on the relevant Home Office forms. Electronic copies of these forms are available on the Home Office website at https://www.gov.uk/government/collections/ripa-forms--2

If an officer has difficulty obtaining the correct form they should contact the Legal Department.

Content of Application

5.15 The applicant must ensure that each application contains a unique reference number ("URN"). This must be inserted into the box at the top right-hand corner of the relevant form. This should include a reference to their department, the year, and the number of the application during that year. Authorising Officers should not authorise any application, which does not contain this.

5.16 Applicants must also ensure that they complete all boxes within the forms. If done properly this will ensure compliance with RIPA's requirements. However, to ensure that there is full compliance the details of RIPA's requirements are set out below.

Application for Directed Surveillance

5.17 A written application for directed surveillance should include:

5.17.1 the reason(s) why the authorisation is necessary in the particular case and the ground(s) on which it is considered necessary pursuant to Section 28(3) of the Act. As set above the only ground on which the Council can now rely is "for the purpose of preventing or detecting crime or disorder".

5.17.2 the reasons why the surveillance is considered proportionate to what it seeks to achieve;

5.17.3 the nature of the surveillance;

5.17.4 the identities, where known of those to be the subject of the surveillance;

5.17.5 an explanation of the information, which it is desired to obtain as a result of the surveillance;

5.17.6 the details of any collateral intrusion and why the intrusion is justified;

5.17.7 the details of any confidential information that is likely to be obtained as a consequence of the surveillance;

5.17.8 the level of authority required (or recommended where that is different) for the surveillance; and

5.17.9 a subsequent record of whether authorisation was given or refused, by whom, and the date and time.

Application for the use of CHIS

5.18 An application for the use or conduct of a source should include:

5.18.1 the reasons why the authorisation is necessary, and the grounds listed in section 29(3). Again, the only ground upon which the Council can rely is "for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least six months imprisonment";

5.18.2 the reasons why the authorisation is considered proportionate to what it seeks to achieve;

5.18.3 the purpose for which the source will be tasked or deployed;

5.18.4 where a specific investigation or operation is involved, the nature of that investigation or operation;

5.18.5 the nature of what the source will be tasked to do;

5.18.6 the level of authority required (or recommended where different);

5.18.7 the details of any potential collateral intrusion and why the intrusion is justified;

5.18.8 the details of any confidential information that is likely to be obtained as a consequence of the authorisation; and

5.18.9 a subsequent record of whether authority was given or refused, by whom and the time and date.

Duration of Authorisations Directed Surveillance

5.19 A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

CHIS

5.20 A written authorisation will unless renewed cease to have effect at the end of a period of twelve months beginning with the day on which it took effect.

Reviews

5.21 Regular reviews should be carried out to assess the need for the authorisation to continue. Reviews should take place frequently if the source of surveillance provides confidential information or involves collateral intrusion.

5.22 The Authorising Officer must decide how frequently and when the reviews should take place. This should be as frequently as is considered necessary and practicable.

5.23 The Authorising Officer must use the appropriate form to complete the review, and the results of the review should be recorded in the central record of authorisations and retained for at least 3 years. Authorisations may be renewed more than once, if necessary and proportionate, and provided they continue to meet the criteria for authorisation.

Renewals

5.24 If at any time before an authorisation ceases to have effect an Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given he may renew it for:

5.28.1 3 months (Directed Surveillance)

5.28.2 12 months CHIS

5.25 The renewal will take effect at the time at which, or the day on which the authorisation would have ceased to have effect but for the renewal.

5.26 An application for renewal of an authorisation should not be made until shortly before the authorisation is due to cease to have effect.

5.27 Any person who would be entitled to grant a new authorisation is able to renew an authorisation.

5.28 An authorisation can be renewed more than once as long as it continues to meet the criteria for authorisation.

5.29 The application for renewal must include:

Directed Surveillance

- Whether this is the first renewal of an authorisation on which the authorisation has been renewed previously;
- Any significant changes to the information included in the initial application;
- The reasons why the authorisation for directed surveillance should continue;
- The content and value to the investigation or operation of the information so far obtained by the surveillance; and
- The results of regular reviews of the investigation or operation.

CHIS

- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously
- Any significant changes to the information in the original application;
- The reasons why it is necessary to continue to use the source;
- The use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
- The tasks given to the source during that period and the information obtained from the conduct or use of the source; an
- The results of regular reviews of the use of the source.

5.30 **As with new applications judicial approval must also be sought after the Authorising Officer gives authorisation.**

Cancellations

5.31 The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that it no longer meets the criteria under which it was first granted.

5.32 The Authorising Officer must complete the relevant form to do so and pass the information to the legal department to be included on the central register.

5.33 In addition, when the decision is taken to stop surveillance, an immediate instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central register and on the cancellation form.

5.34 There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation but effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6. AUTHORISING OFFICERS

6.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010 No. 521 provides that the Director, Head of Service, Service Managers, or equivalent officer may give authorisations for directed surveillance and CHIS under RIPA.

6.2 In light of the infrequent use made of RIPA and CHIS, Selby District Council has designated only five Authorising Officers - the Chief Executive, the two Directors, the Head of Operational Services and the Head of Planning. These Officers will receive regular training to enable them to deal properly with all authorisations.

6.3 Moreover, applicants must submit their application to an Authorising Officer, from outside of their department.

7. RECORDS AND CENTRAL REGISTER

7.1 The Council's Legal Department will maintain a central record of all authorisations. This will be updated whenever an authorisation is granted, renewed, or cancelled.

7.2 The record will be retained for a period of at least three years from the end of the authorisation and will contain the following information:

7.2.1 the type of authorisation;

7.2.2 the date the authorisation was given;

7.2.3 Name and rank/grade of the authorising officer

7.2.4 the unique reference number (URN) of the investigation or operation;

7.2.5 the title of the investigation or operation, including a brief description and names of subjects, if known;

7.2.6 details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;

7.2.7 the dates of any reviews;

7.2.8 if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;

7.2.9 whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;

7.2.10 whether the authorisation was granted by an individual directly involved in the investigation; and

7.2.11 the date the authorisation was cancelled.

7.3 In respect of each step in the procedure Authorising Officers must retain all original documentation and must give to the legal department a copy of the following information:

7.3.1 the application, and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;

7.3.2 a record of the period over which the surveillance has taken place;

7.3.3 the frequency of reviews prescribed by the authorising officer;

7.3.4 a record of the result of each review of the authorisation;

7.3.5 the renewal of an authorisation, given together with the supporting documentation submitted when the renewal was requested;

7.3.6 the date and time when any instruction to cease surveillance was given;

7.3.7 the date and time when any other instruction was given by the authorising officer; and

7.3.8 a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).

7.4 For the avoidance of doubt the information set out above must be passed to the legal department contemporaneously to ensure that the Council's central record can be maintained and that the Council can therefore ensure that all authorisations are reviewed and cancelled in accordance with RIPA.

8 ERRORS

8.1 The Council's Senior Responsible Officer will undertake a regular review of errors and a written record will be made of this review. In the event that relevant errors occur, the Council's Senior Responsible Officer will notify the Investigatory Powers Commissioner's Office as soon as practicable and no later than 10 working days after it has been established that the error occurred and will have regard to Section 8 of the Code in doing so.

9. INFORMATION

9.1 The Council will have regard to the guidance provided in the Code with regard to the relevant legislation, guidance and the Code when handling, storing, or disseminating information.

10. COMPLAINTS

10.1 Complaints about the Council's use of investigatory powers can be made to:

The Investigatory Powers Tribunal PO Box 33220 London SW1H 9ZQ

10. APPENDICES

1. Code of Practice on Covert Surveillance
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

2. Code of Practice on Covert Human Intelligence Sources
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

3. Home Office Guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance –

www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf