| Internal Ref: | NELC/Legal |
| --- | --- |
| Review date | July 2027 |
| Version No. | V01.8 |



**Employees’ Guide to the**

**Regulation of Investigatory**

**Powers Act 2000**

**&**

**Investigatory Powers Act 2016**

**On**

**The Acquisition of Communications Data,**

**Directed Surveillance and Use of Covert Human Intelligence Sources**

**CONTENTS**

[1. Introduction 3](#_Toc21080317)

[2. Responsibilities 4](#_Toc21080318)

[3. When RIPA applies 4](#_Toc21080319)

[4. When IPA applies 7](#_Toc21080320)

[5. Definitions 7](#_Toc21080321)

[6. RIPA application process (directed surveillance & CHIS only) 14](#_Toc21080322)

[7. Reviews 18](#_Toc21080323)

[8. Cancellations 19](#_Toc21080324)

[9. Renewals 19](#_Toc21080325)

[10. Use of Covert Human Intelligence Sources (CHIS) 20](#_Toc21080326)

[11. Registers of Authorisations and Notices 21](#_Toc21080327)

[12. Benefits of Obtaining Authorisation under RIPA 22](#_Toc21080328)

[13. IPA application process (all communications data) 22](#_Toc21080329)

[14. Joint Working 24](#_Toc21080330)

[15. Handling and disclosure of the products of surveillance 24](#_Toc21080331)

[16. Training 25](#_Toc21080332)

[17. Scrutiny and Tribunal 25](#_Toc21080333)

# Introduction

* 1. The Human Rights Act 1998 incorporates into UK law the European Convention on Human Rights, the effect of which is to protect an individual’s rights from unnecessary interference by the ‘State’.
  2. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates covert investigations undertaken by ‘public bodies’ and provides a framework within which the ‘State’ (the specified public bodies) can work to ensure that law enforcement and other important functions can effectively protect society as a whole.
  3. The Public Bodies defined in RIPA include Local Authorities and, therefore, North East Lincolnshire Council’s activities are subject to the RIPA framework.
  4. The Protection of Freedoms Act 2016, introduced a judicial approval process for RIPA applications made by Local Authorities and introduced a serious crime threshold for directed surveillance.
  5. The Investigatory Powers Act 2016 (IPA) replaced part 1 of RIPA and brings together in one place all the powers available to law enforcement agencies in respect of obtaining communications data and data about communications.
  6. **The Local Authority must not use any other legislation to obtain communications data (including exemptions to non-disclosure contained in schedule 2 of the Data Protection Act 2018)**.
  7. The purpose of this guidance is to:
     + explain the scope of RIPA and IPA and the circumstances where they apply;
     + provide guidance on the authorisation procedures to be followed.
  8. The Council has had regard to the [Codes of Practice](https://www.gov.uk/government/collections/ripa-codes) produced by the Home Office in preparing this guidance. The Home Office codes of practice expand on the information in this guide.
  9. The codes do not have the force of statute but are admissible in evidence in any criminal and civil proceedings.

# Responsibilities

* 1. The Head of Paid Service and Monitoring Officer are responsible for authorising applications for the use of a Covert Human Intelligence Sources (CHIS) in respect of the regulatory services for which they are responsible. The Monitoring Officer may delegate the power to authorise applications under RIPA to officers of an appropriate level (Strategic Director, Head of Service, Service Manager or equivalent).
  2. The Council has a Senior Responsible Officer (SRO) as recommended by the RIPA Code of Practice. The SRO is responsible for monitoring the Council’s compliance with its RIPA obligations and this policy statement. This will include:-
     + maintaining the integrity of the process in place for the management of CHIS and directed surveillance under RIPA;
     + maintenance of a central register of authorisations;
     + ensuring authorising officers are of the required standard;
     + maintaining a corporate working group;
     + engagement with the Investigatory Powers Commissioner’s Officer (IPCO);
     + ensuring that actions plans recommended by a Commissioner are implemented;
     + reporting to members via scrutiny, as appropriate, and annual reporting to Cabinet.

* 1. The Council includes RIPA as a standing item at the Enforcement Working Group, which meets twice per year and is Chaired by the Deputy Monitoring Officer, whom reports directly to the SRO. The Group is responsible for ensuring that awareness of RIPA is maintained throughout the Council in addition to developing any policies and procedures to assist the Council in delivering its statutory obligations. Each Directorate is represented on the Group as is deemed necessary by the relevant Strategic Director. The remit of this group has been extended to include relevant matters relating to the IPA.

# When RIPA applies

* 1. Local Authorities may apply for authorisation under RIPA to undertake the following investigative activities for the purpose of preventing or detecting crime only:
* Directed Surveillance;

* Use of a Covert Human Intelligence Source (CHIS). Local Authorities are not prescribed to use RIPA in any other circumstances.

From 1st November 2012, The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 placed further restrictions as to when a RIPA authorisation can be granted. This order requires that:

* The criminal offence which is sought to be prevented or detected must be punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment; or
* It would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.
  1. The order also removed a local authority's ability to grant authorisations under RIPA for the purpose of preventing disorder. This means that directed surveillance for the purposes of tackling antisocial behaviour can longer be able to be authorised, unless the behaviour constitutes a criminal offence carrying a maximum prison term of six months or more.
  2. Furthermore, The Protection of Freedoms Act 2012 requires that any Local Authority authorisation under RIPA must now have judicial approval.
  3. Local Authorities cannot apply for authorisation under RIPA in any circumstances to:
* Obtain communications data;
* Conduct intrusive surveillance;
* Interfere with property or wireless telegraphy.
  1. Authorisation under RIPA gives lawful authority to carry out directed surveillance and to use a CHIS. This is known as the “RIPA shield”. Before approving applications, the Authorising Officer must have regard to the necessity and proportionality of the application. But, once obtained, the authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8 of the European Convention on Human Rights (the right to private and family life). See [RIPA application form – detailed guidance](https://www.nelincs.gov.uk/your-council/fraud-and-corruption/) (under Investigatory Powers) for more information on completion and authorisation of applications.
  2. Some surveillance may be carried out in the Council which does not appear to fall within RIPA because the surveillance is not being undertaken “for the purpose of preventing or detecting crime”, for example, in child protection or employee surveillance in relation to misconduct issues. **In these circumstances the RIPA process should still be used.**
  3. This is because although RIPA will not itself provide lawful authority (and so the RIPA shield does not apply) it is considered that this process is the best method of ensuring that due consideration has been given to the Human Rights of the individuals concerned. Provided this complies with the Human Rights Act 1998 it will still be lawful. Use of the RIPA process in determining whether surveillance is justifiable will be useful in establishing this. If in doubt, seek advice.
  4. Deciding when authorisation is required involves making a judgment. Section 6 provides further information on specific considerations and the process for applying for and granting authorisations.

## Covert Surveillance of social networking sites

* 1. Care should be taken when conducting checks on social networking sites. Although private information may be available on such sites, it must not be assumed that it is therefore, public information. As such, directed surveillance or the use of a CHIS may be necessary.
  2. Consideration must be given to how the individual sites work and what expectation of privacy is attached to them.
  3. Where the author has set privacy controls or restricted access to their personal information then they have a reasonable expectation of privacy. If it is deemed necessary & proportionate to covertly breach such privacy settings then the minimum requirement would be an authorisation for directed surveillance. If a relationship is established or maintained (that is the activity is more than just reading the content of the site) then a CHIS authorisation is necessary.
  4. Where the author has not applied privacy controls, then such information can be considered as ‘open source’ and as such a directed surveillance authorisation will not normally be required. This applies where the social networking site is being used as one off source of intelligence. However, regular monitoring of social networking sites is more likely to fall within the definition of covert directed surveillance and therefore, in such cases an authorisation must be sought.
  5. It is permissible to set up a false identity (although this may breach an individual site’s own rules). However, any false identity must form part of an authorisation.
  6. It is not permissible to use the identity of a person known to (or likely to be known to) the subject without that persons explicit consent. Consideration must also be given to the protection of that person. Only the Head of Paid Service (or in their absence a person acting as the Head of Paid Service) or the Monitoring Officer can authorise the use of such an identity.

# When IPA applies

* 1. The IPA applies to the acquisition of any communications data necessary for the prevention/detection of crime. Officers must not require, or invite, any telecommunications or postal operator to disclose communications data under any other legislation. Failure to use the correct legislation, will result in the data obtained being unauthorised and will impact on the investigation.
  2. All applications for communications data require independent authorisation, but no longer require judicial approval. The Office for Communications Data Authorisations (OCDA) has been formed to make decisions on such applications from March 2019.
  3. Additionally, the IPA creates new offences for the unlawful acquisition and disclosure of communications data. For the acquisition to be unlawful, it must having been knowingly or recklessly obtained or disclosed. It is therefore, essential that all requests for communications data follow the guidance in section.

# Definitions

## Communications data

* 1. Communications Data includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content; i.e. what was said or written. Communications Data falls into two categories:
* entity data – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices)
* events data – events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

## Entity Data

* 1. Entity data covers information about a person or thing (such as phone, computer, tablet etc), and about links between a telecommunications service and a person or thing, that identify or describe the person or thing. The links between a person and their phone are therefore entity data.
  2. Entity data can include:
     + subscribers of e-mail and telephone accounts;
     + account information including payment details;
     + address for installation and billing;
     + abstract personal records e.g. sign up data.
  3. Communications between devices on a network at a specific time and for a specified duration would be events data.
  4. From 16th February 2023, there has been a change in the interpretation of what constitutes communications data. The main change relates to mandatory information provided whilst accessing a telecommunications service (this includes access to a website) as many organisations are now considered as a partial telecommunications operator.
  5. This new interpretation refers to any data that is provided in order to create online accounts. For example, it is a requirement to provide a forename, surname, e-mail address and telephone number to set up a PayPal account. This information is mandatory and an account cannot be set up without it. As a result, this information now falls under communications data and must be obtained via an IPA application.
  6. The same applies to online only bank accounts such as Monza, or other services where the account is set up online. Therefore, subscriber information from such information providers is now only available via IPA.
  7. The change does not apply to transaction data, only subscription data. Transaction data such as bank statements or other account transactions can be requested using previous powers or exemptions.

## Events Data

* 1. Events data identifies or describes events with consist of one or more entities engaging in an activity at a specific time or times.
  2. Events data includes:
     + itemised telephone call/text records
     + itemised connection records
     + itemised timing and duration of calls
     + connection/ disconnection/ reconnection data
     + mobile data records
     + device data
     + use of forwarding or redirection services
     + additional telecom services
     + records of postal items
  3. This list is not exhaustive. Any event that causes a mobile device to communicate, can constitute events data. This can include each time a device connects with a phone mast, updates an app etc.
  4. Events data can only be requested where the offence being investigated meets the definition of serious crime. A serious crime for the purpose of obtaining events data is defined as:
     + An offence capable of attracting a prison sentence of 12 months or more;
       - An offence by a person who is not an individual (i.e.. A corporate body);
       - An offence falling within the definition of serious crime in section 263(1) of the IPA 2016;
       - An offence which involves, as an integral part of it, the sending of a communication;
       - An offence which involves, as an integral part of it, a breach of a person’s privacy.

## Surveillance

* 1. Surveillance includes:
     + monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication and, for the purposes of RIPA, the term persons includes “any organisation and any association or combination of persons”, this will include limited companies, partnerships, co-operatives etc;
     + recording anything monitored, observed or listened to in the course of surveillance;
     + surveillance by or with the assistance of a surveillance device.

## Covert Surveillance

* 1. Covert surveillance is that carried out in a manner calculated to ensure that person subject to surveillance are unaware it is or may be taking place.
  2. If activities are open and not hidden from the person(s) subject to surveillance, the RIPA framework does not apply.

## Directed Surveillance

* 1. Surveillance is ‘Directed’ for the purposes of RIPA if it is covert, but not intrusive and is undertaken:
     + for the purposes of a specific investigation or a specific operation; and
     + in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
     + otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.
  2. Where directed surveillance would not be likely to result in the obtaining of private information about a person, no interference with Article 8 rights occurs and an authorisation is not appropriate.

## Intrusive surveillance

* 1. Surveillance is intrusive if it:
* is carried out in relation to anything taking place on any ‘residential premises or in any ‘private vehicle’; and
* involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
  1. is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where 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.
  2. **Local Authorities cannot grant an authorisation under RIPA for intrusive surveillance.**

## **Examples of surveillance**

|  |  |
| --- | --- |
| **Type** | **Examples** |
| **OVERT** | * Patrolling enforcement officer or market inspector * Recording noise from outside premises creating noise or where the subject has explicitly been warned that they are being monitored * Most test purchases where the investigator behaves no different from a member of the public. |
| **OVERT** (but regulated by other legislation outside the scope of RIPA) | * Town Centre CCTV systems in formal use * ANPR cameras used for enforcing road traffic offences * CCTV systems operated by local authorities in public places (camera visible and presence indicated). |
| **COVERT** (not requiring prior authorisations under RIPA) | * CCTV cameras providing general traffic, crime or public safety information. |
| **DIRECTED SURVEILLANCE** (requiring authorisation under RIPA) | * Officers maintaining observations on a specific place or location * Repeated visits to a subject’s social medial platforms to establish their involvement in an offence * Test purchases with the use of a concealed camera and/or audio device where there is a risk of private information being gathered about the suspect. |
| **INTRUSIVE SURVEILLANCE or INTERFERENCE WITH PRIVATE PROPERTY** (which requires authorisation under RIPA but cannot be authorised or used by a local authority) | * Use of surveillance device inside a suspects home, private vehicle or private business premises * Using a surveillance device outside a suspects home, vehicle or private business address which is capable of recording and retaining the same level of material as if the device was planted inside those premises. |

## Covert Human Intelligence Source (CHIS)

* 1. The use or conduct of a CHIS do not relate specifically to the obtaining of private information but to the covert manipulation of a relationship to gain information. Article 8 includes the right to establish and develop relationships and therefore, any manipulation of such a relationship by a public authority is likely to engage Article 8 whether or not it intends to acquire private information.
  2. A person is a Covert Human Intelligence Source if they establish or maintain a personal or other relationship with a person for the covert purpose of:
     + - using such a relationship to obtain information or provide access to any information to another person; or
       - disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
  3. Arrangements should be put in place for the proper oversight and management of CHIS, including appointing individual officers to be the “handler” and the “controller”. The handler will have day to day responsibility for dealing with the CHIS, directing the day to day activities, recording information supplied and monitoring the CHIS’s security and welfare. The handler will usually be a position below that of the authorising officer. The controller will normally be responsible for the management and supervision of the handler and general oversight of the CHIS.

## Covert Purpose

* 1. A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose behind the relationship.

## Private Information

* 1. Private information is any information relating to a person’s private or family life. Generally, this includes all aspects of a person’s private or personal relationship with others and includes family, professional and business relationships.

## Confidential Material

* 1. Confidential material includes:
     + - matters subject to legal privilege;
       - confidential personal information; or
       - confidential journalistic material.
  2. Matters subject to legal privilege includes both oral and written communications between a professional legal adviser and his/her client (or any person representing his/her client) made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications.
  3. Legally privileged communications will lose their protection if there is evidence, for example, that such communications are held with the intention of furthering a criminal offence. However, it is important to note that the privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.
  4. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.
  5. Confidential Personal Information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:
     + - to his/her physical or mental health; or
       - to spiritual counselling or other assistance given or to be given; and
       - which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office. It includes both oral and written information and also communications as a result of which personal information is acquired or created.
  6. Information is held in confidence if:
     + - it is held subject to an express or implied undertaking to hold it in confidence; or
       - it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.
  7. Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient’s medical records.
  8. Confidential Journalistic Material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.
  9. Any application for an authorisation that is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Such applications are subject to special authorisation by the Head of Paid Service (or person acting on their behalf).

# RIPA application process (directed surveillance & CHIS only)

## Authorising Officers and single point of contact (SPOC)

* 1. The Head of Paid Service, Monitoring Officer, or person to whom the power to grant an authorisation for directed surveillance is delegated to, is for the purposes of this guide known as the Authorising Officer.
  2. A list of the names of the Authorising Officers will be kept on the central register (held in Legal Services). If you do not know who to contact for an authorisation, seek advice from the legal section OR contact one of your Directorate representatives on the Corporate Working Group.

## Initial considerations

* 1. Prior to completing an application, the applicant should ask these questions.
  2. **Is the surveillance for the purpose of a specific investigation or operation?**
  3. If the surveillance is directed at a known individual or group the provisions of RIPA will cover the investigation. In respect of other situations, such as CCTV cameras that are readily visible to anyone walking around the area, their general use is not governed by RIPA. However, if the cameras are used as part of the surveillance operation to observe a known individual or group it is very likely that RIPA will apply and an appropriate authorisation will be required.
  4. **Is the surveillance likely to obtain private information about a person?**
  5. If it is likely that surveillance will result in the obtaining of private information about any person, then RIPA may apply. For example, if surveillance is required to build up a picture of an individual’s routine, this will result in private information about that person being obtained and as such RIPA would normally apply.
  6. **Is the planned surveillance intrusive?**
  7. Surveillance is intrusive if it is carried out on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.
  8. **The Council cannot authorise intrusive surveillance under RIPA.**
  9. **Is the surveillance an immediate response to an event?**
  10. Home Office guidance indicates this is to take account of an immediate response to something happening during the course of an observer's work, which is unforeseeable. If this occurs, the surveillance will not require prior authorisation.
  11. However, if as a result of an immediate response, a specific investigation subsequently takes place, that investigation may be within the scope of RIPA.
  12. **Is the offence under investigation punishable by a maximum sentence of at least 6 months’ imprisonment?**
  13. Officers must have regard to the specific criminal offences that they are investigating. RIPA cannot be used where the maximum offence on conviction is less than 6 months, except where the offence would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.
  14. Once it has been decided that a surveillance operation falls within the scope of RIPA, the applicant is required to complete an Application for use of directed surveillance form or application for the use of a CHIS form.
  15. Each application must have a unique reference number (URN) relating to a specific investigation or operation. The URN must be obtained from Legal Services prior to completion, who will record the URN on the central register. Copies of the relevant application forms can be downloaded from the [Home Office](https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2) website.
  16. The applicant fully completes Part 1 of the form. The form then goes to the Authorising Officer, who will decide whether or not to authorise the application and complete Part 2. The [*RIPA application* – *detailed guidance* document and *RIPA application – aide memoir*](https://www.nelincs.gov.uk/your-council/fraud-and-corruption/)(under Investigatory Powers) provide further information on the completion of the application. There is also an example of best practice as identified by the Office of the Surveillance Commissioner[[1]](#footnote-1) .
  17. The Authorising Officer’s decision must be communicated to Legal Services as soon as possible (same day) and a copy sent them (by e-mail). If the application has been authorised the original application form should be held for production in Court as part of the judicial approval process. Once approved, the original application should be sent Legal Services.
  18. For each URN obtained there must be an outcome recorded on the central register. Therefore, whether the application is authorised or not, a copy of the application should be sent to Legal Services. This ensures the central record is a record of all RIPA activity, not just those applications authorised.
  19. Should a URN have been obtained, but subsequently no application completed, an e-mail should be sent to Legal Services advising them of the reason the application was not pursued.
  20. An example of a fully completed RIPA application cited by the OSC as an example of good practice can be found [here.](https://nelincsgovuk.sharepoint.com/:w:/r/sites/WikiHub/Shared%20Documents/RIPA%20application%20good%20practice%20example%20-%20internal%20only.docx?d=wdb8c686a8863416c8f5c38c63791e3ea&csf=1&web=1&e=JR5KgQ)

## Judicial Approval

* 1. If the application is approved the applicant must complete part 1 of the [*RIPA judicial approval form*](https://www.nelincs.gov.uk/your-council/fraud-and-corruption/)(under Investigatory Powers) and contact the Magistrates’ Court on 320444 in normal working hours to arrange a hearing.
  2. The Authorised Officer and the Investigating Officer will attend the Court hearing with the authorised RIPA application and Judicial Approval Form and any other supporting material as relevant. It is appropriate for the Authorising Officer to attend as they are in the best position to argue the necessity and proportionality considerations that led to their decision. However, where the Authorising Officer is unable to attend, or their availability would unduly delay an investigation, the investigating officer will attend, should the Judge require clarification. The Authorising Officer should ensure that the investigating officer is fully briefed. However, the forms and supporting papers must themselves make the case. Oral evidence is not sufficient unless it is supported in the documentation provided to the Court.
  3. The Judge will make one of three decisions:
     + - Refuse to approve the application. In this case the Council cannot use the covert technique. However, it can reapply if the refusal is on a technical issue;
       - Refuse to approve the application and quash the authorisation. Such action may be appropriate if the Judge considers an application is fundamentally flawed. In this case the Council cannot use the covert technique and will need to seek a fresh authorisation before reapplying to the Court;
       - Approve the application. In this case the Council can use the covert technique. Any change in the technique used will require a further authorisation to be submitted to the Court.
  4. Before leaving Court, ensure that a copy of the completed signed Judicial Approval form is obtained. The original RIPA application form should also be retained although the Court may wish to keep a copy.
  5. The original RIPA application form and Judicial Approval Form must be lodged with Legal Services for audit and inspection purposes.

## **Urgent authorisations**

* 1. The requirement to obtain judicial approval for all RIPA authorisations means that urgent authorisations may no longer be authorised orally by an Authorising Officer.
  2. If an authorisation is urgent the Court may consider it in exceptional circumstances. However, it must not be used as a remedy for poor planning.
  3. The Courts’ Service out of hours legal contact must be telephoned. A brief summary of the facts and the reason for the urgency will be requested.
  4. If urgency is agreed, arrangements will be made for a suitable Judge to consider the application. The applicant will be advised when and where to attend and give evidence. At the hearing they must have two copies of both the authorised application form and the Judicial Approval Form.

# Reviews

* 1. Once authorised and approved, directed surveillance is granted for a period of three months from the date of approval by the Court.
  2. In all cases the Authorising Officer is required to sets review dates for all authorisations as frequently as they consider is necessary. The Authorising Officer is also responsible for undertaking the review within the timescales set.
  3. The review must take place at intervals **not longer than one month**, but depending on the circumstances of the case, the review can be conducted more frequently. This must be considered where:
     + - The surveillance is likely to obtain the necessary information in a short period of time and must be cancelled as soon as possible, in order to avoid breaching proportionality;
       - There is a change of circumstances involving the case under investigation.
  4. The review should assess whether the criteria on which the original authorisation was granted has changed sufficiently to cause the authorisation to be revoked.
  5. Whilst it is the Authorising Officer who is responsible for reviewing the authorisation, the applicant should provide the necessary information to them to complete the review process.
  6. All reviews must be recorded on the Review of directed surveillance form. Reviews do not require judicial approval unless there is a change to the techniques to be used. A copy of the review from can be downloaded from the [Home Office](https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2) website.
  7. The authorising officer must contact Legal Services immediately by telephone or e-mail to notify them that the review (or cancellation) has been completed and ensure the original review (or cancellation) form is received in Legal Services within 24 hours.
  8. Where, it is possible that the surveillance may no longer be necessary or proportionate before the expiry period of three months, then a review date should be arranged before then to consider whether the authorisation should be cancelled.

# Cancellations

* 1. Authorisations must be cancelled as soon as they are no longer required, or no longer proportionate.
  2. Authorisations must be cancelled on or before the expiry date of the authorisation (unless it is being renewed). In other words, even when an authorisation is due to expire, a cancellation form must be completed to demonstrate that surveillance is no longer taking place.
  3. The investigating officer is responsible for completing parts 1-3 of the cancellation of directed surveillance form. This can be downloaded from the [Home Office](https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2) website. The investigating officer is required to advise the Authorising officer of any collateral intrusion, the value of the operation and the product obtained. The form should then be forwarded to the Authorising Officer. Further guidance on completing the form can be found in the [*RIPA cancellation – aide memoir*](https://www.nelincs.gov.uk/your-council/fraud-and-corruption/)(under Investigatory Powers).
  4. When cancelling an authorisation, the Authorising Officer should consider the following:
     + - Providing direction for the management of the product obtained;
       - Recording the value of the surveillance (i.e.. Did it achieve its objectives?);
       - Formally record their instruction to cancel the surveillance.
  5. A copy of the completed cancellation must be sent to Legal Services and an instruction issued to those involved to cease all surveillance on the subject(s).
  6. Cancellations do not require judicial approval.

# Renewals

* 1. There may be occasions where it is considered necessary for the authorisation to continue beyond the initial three months. At any time prior to an authorisation expiring, an Authorising Officer may renew the authorisation. The Authorising Officer must complete the Application for renewal of Directed Surveillance form.
  2. On the form it should be recorded:
     + - Whether this is the first renewal or each occasion on which it has been renewed previously;
       - Any significant changes to the information in the initial application;
       - The reasons why authorisation should continue;
       - The content and value of information so far obtained;
       - The results of the reviews in to the investigation/operation.
  3. The renewal requires judicial approval. Therefore, the process for [judicial approval](#judicial) should be followed. A copy of the renewal form should also be provided for the Judge.
  4. A CHIS application should not be renewed unless a thorough review has been carried out and the authorising officer has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

# Use of Covert Human Intelligence Sources (CHIS)

* 1. It is not the Council’s normal practice to seek, cultivate or develop a relationship with a potential external or professional source, although this action is not precluded if it meets the RIPA conditions. It is possible that a Council employee may, in exceptional circumstances, be used as a CHIS and nothing in RIPA prevents material obtained by an employee acting as a CHIS being used as evidence in Court proceedings.
  2. Only the Head of Paid Service (or in their absence a person acting as the Head of Paid Service) or the Monitoring Officer may authorise the use of a CHIS. If the CHIS is a vulnerable individual or juvenile, only the Head of Paid Service can authorise the application.
  3. It is strongly recommended that legal advice is obtained prior to an application for the authorisation of a CHIS is made.
  4. The same principles as Directed Surveillance apply to a CHIS application.
  5. In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such the Application for Authorisation of the use of a CHIS must be completed. The form can be downloaded from the [Home Office](https://www.gov.uk/government/collections/ripa-forms--2) website.
  6. The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment must be carried out ***before*** authorisation is given. The safety and welfare of the employee, even after cancellation of the authorisation, must be considered from the very outset.
  7. Before authorising the use of a CHIS, the authorising officer must ensure that, as far as is possible, measures are taken to avoid unnecessary intrusion into the lives of those not directly connected with the operation.
  8. It is also sensible to make any authorisation sufficiently wide to cover all the means required as well as being able to provide effective monitoring of what was done against the actions that had been authorised.
  9. **Authorisation of a CHIS requires judicial approval.**

# Registers of Authorisations and Notices

* 1. The Senior Responsible Officer (SRO) is responsible for maintaining a central register of authorisations. Two separate registers are kept, one for RIPA authorisations and one for non-RIPA authorisations, whereby it is felt best practice to still undergo the same considerations as if RIPA applied. For example, an authorisation to carry out surveillance on an employee is likely to be in respect of disciplinary issues and not for the purpose of preventing or detecting crime and therefore fall outside of the RIPA legislation. Nevertheless the considerations which need to be made under RIPA are equally important and the same level of scrutiny to human rights, privacy etc still needs to be applied. Another example might be in relation to a child protection matter.
  2. The registers will record:
     + - * The type of authorisation;
         * The date the authorisation was given;
         * The date of judicial approval;
         * The name and seniority level of the authorising officer;
         * The Unique Reference Number including those rejected;
         * The title of investigation/operation including subject names where known;
         * The details of any renewal;
         * The likelihood of obtaining confidential information;
         * If the authorising officer is directly involved in the investigation/operation;
         * The date the authorisation was cancelled.
  3. Details should also be recorded of all rejections, whether at authorising officer stage or judicial stage.
  4. The only exception to this rule is in respect of applications for communications data. The central register and applications are held by National Anti-Fraud Network( NAFN) for audit purposes.
  5. Legal Services will hold a copy of the e-mail trail with the application to maintain an audit trail. E-mails held by other officers including the requesting officer and authorising officer must be deleted (see [section 15 – handling the and disclosure of the products of surveillance](#_Handling_and_disclosure)).

# Benefits of Obtaining Authorisation under RIPA

* 1. RIPA states that:

“if an authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be “lawful for all purposes”.

* 1. However, this does not mean that if you do not (or cannot) obtain a RIPA authorisation that the conduct is unlawful. It just means you cannot take advantage of any of the RIPA protections. You may also have to justify infringing a person’s Human Rights and any evidence you place before the courts may be subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).
  2. RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which:
     + - * is incidental to any conduct that is lawful by virtue of an authorisation; and
         * is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.
  3. It is therefore, essential when applying for authorisation that all conduct that could be authorised in relation to an investigation /operation is included in the application.
  4. The Council’s policy is that a RIPA authorisation must be obtained in all cases to which it applies and that the same process must be used even where RIPA does not apply (such as internal disciplinary cases, child protection, etc) to mitigate the risk of challenge.

# IPA application process (all communications data)

* 1. All applications for communications data must be made under the IPA and approved by the Office for Communications Data Authorisations (OCDA).
  2. **Communications data must not be requested using any other legislation.**
  3. NAFN operate a single point of contact (SPOC) service for all NELC communications data applications. The application is completed via the NAFN website. Therefore, officers wishing to make an application must register on the [NAFN](https://www.nafn.gov.uk/) website. There is no requirement for the request to be authorised by an Authorising Officer within the Local Authority.
  4. However, there is a requirement for an approved rank officer (service manager or above) within the authority to be ‘made aware’ that the application has been made. Once the application has been submitted to NAFN, the approved rank officer will receive an e-mail asking for them to confirm that they are aware of the application and content for it to proceed. The approved rank officer can access the NAFN website to provide confirmation, or alternatively they can reply to the e-mail confirming that:

“I am aware of CD Application 000XXX/XXX and I am content for the application to proceed for authorisation by OCDA”.

* 1. Each application must be stand alone and not refer to other applications. The OCDA will only have the application to base their decision on, so all applications should fully describe the offences under investigation, including where necessary a justification for the offence being classed as serious. The application must also include the full necessity and proportionality to justify the request. The application should be completed in plain English avoiding the use of jargon, abbreviations and acronyms.
  2. The SPOC role is to ensure that applications comply with IPA standards and contain sufficient information to meet OCDA & IPCO scrutiny. The SPOC will also monitor the reasons for rejected or reworked applications and provide training where necessary. They are also the point of contact between the LA and OCDA. Applicants will not be able to contact OCDA directly.
  3. The SPOC will submit the application to OCDA, who will either:
     + - * Authorise the request;
         * Reject the request; or
         * Return the request for re-work.
  4. If OCDA reject the request the LA ‘made aware’ officer may appeal the decision.
  5. Once an application is authorised, NAFN will make the relevant enquiries and return the data requested to the applicant.
  6. Further guidance is available of the [NAFN](https://www.nafn.gov.uk/) website.

# Joint Working

* 1. Situations may arise where NELC employees are involved in joint operations. Examples include, operations with the Police, Department for Work and Pensions, Her Majesty’s Revenue & Customs etc. Where directed surveillance is required the Authorising Officer (of NELC) can authorise all persons (including those of another organisation) engaged in the investigation/operation to carry out the surveillance on behalf of NELC. This may be appropriate where NELC is leading the operation.
  2. Where employees of other agencies are to be included, the authorisation should be specific as to who will be acting under the authorisation.
  3. A NELC Authorising Officer may only authorise an application completed by a NELC employee. They cannot authorise an application made by an employee of another agency.
  4. The Police can authorise all persons (including NELC employees) engaged in the investigation/operation to carry out the surveillance on behalf of Police. An example of this could be where the Police request the operators in the Council’s CCTV control room to carry out directed surveillance using the Council’s CCTV cameras. There is no need for the Council employee to be separately authorised by a Council authorising officer. More detail about this can be found in the [Council’s CCTV Partnership Protocol](https://www.safernel.co.uk/crime-and-staying-safe/closed-circuit-television-cctv/).
  5. Although NELC employees undertaking directed surveillance must have judicial approval, they can be included on another organisations RIPA authorisation even if that organisation may not require judicial approval (such as the Police, DWP, etc).

# Handling and disclosure of the products of surveillance

* 1. A copy of all RIPA related documents should be held on the working file in line with the Council’s Corporate Retention Schedule and Records Management Policy. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.
  2. With the exception of prosecution files and the RIPA central register of authorisations, RIPA related documents, including the product of the authorisation must not be held in any other place other than the working file. This includes as part of sent or received e-mails. Any e-mail received that contains RIPA related personal information must be deleted once it has been actioned. Likewise, any e-mail sent that contains RIPA related personal information must be deleted after it has been sent. This is to ensure that RIPA data is not retained longer than is necessary.
  3. Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material obtained by surveillance is wholly unrelated to a criminal or other investigation, or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.
  4. Material obtained through the proper use of the RIPA authorisation procedures can be used for relevant Council purposes. However, the transfer of such information outside the Council, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances and should always only occur following consideration of the appropriate Data Protection legislation.

# Training

* 1. Training is available and will of great use to authorising officers and those involved in investigations where surveillance may be necessary.
  2. The training dates will be arranged in response to demand for the places. If any officer experiences difficulty in obtaining the training they should contact their representative on the Enforcement Working Group.
  3. Authorising Officers MUST have training and should consider, from time to time, whether the training and knowledge needs updating or refreshing.
  4. NAFN have produced a ‘general awareness briefing’ that summarises the changes to communications data. This is available on the [NAFN website](https://www.nafn.gov.uk).

# Scrutiny and Tribunal

* 1. RIPA set up the Office of the Surveillance Commissioner to regulate the conduct of public bodies and to monitor their compliance with RIPA. These duties are now discharged by the Investigatory Powers Commissioners Office (IPCO). The IPCO will keep under review, among other things, the exercise and performance of duties, imposed in RIPA, by the persons on whom those duties are conferred or imposed. This includes authorising directed surveillance and the use of covert human intelligence sources. They will also review the use of powers to obtain communications data.
  2. Further information can be found on [The Investigatory Powers Commissioners Office](https://www.ipco.org.uk/) web-site.
  3. A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.
  4. The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:
     + - * A Council officer has granted any authorisation under RIPA.
         * Council employees have engaged in any conduct as a result of such authorisation.
         * A disclosure notice requirement is given.

1. The Office of the Surveillance Commissioner has been replaced by the Investigatory Powers Commissioner’s Office (IPCO). [↑](#footnote-ref-1)