# Harlow District Council

# Guidance and Procedure on Regulation of Investigatory Powers Act 2000

**Updated 2021**

**Version 1.4**

# Harlow District Council

## Guidance and Procedure on Regulation of Investigatory Powers Act 2000 (RIPA)

**Contents:**

**Appendix 1: Guidance on filling out forms**

**Appendix 2: Links to authorisation and judicial approval forms.**

# Harlow District Council

## Guidance and Procedures on Regulation of Investigatory Powers Act 2000 (RIPA) (herein referred to as guidance)

### 1. Purpose

To provide guidance on the application process and forms to be used when making an application under RIPA.

This is not a statement of the Council's policy regarding RIPA which can be found in a separate document.

### 2. Introduction

RIPA came into force on 25 September 2000, and the main purpose of the Act is to ensure that surveillance is carried out in compliance with the Human Rights Act 1998 which came into force 2 October 2000.

The Council has issued this guidance to Officers on how to make applications and which forms to use for authorisation and judicial approval. This guidance does not form part of the Policy document but is to assist Officers when making applications or authorising applications for the use of investigatory powers under RIPA.

Chapter 2 Part 1 RIPA has been amended by the Protection of Freedoms Act 2012, which introduced the need for approval of any authorised action under RIPA by a Justice of the Peace (JP) and the introduction of a crime threshold for directed surveillance.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order[s] 2010 SI 2010/521 and SI 2012/1500 have now restricted the local authority grounds under section 28(b) RIPA for

using directed surveillance Authorising Officers must now be satisfied that the crime threshold is met.

Officers should be aware of the scope and extent of activities covered by the Provisions of RIPA and must read the Council's Policy documentation prior to making an application for the use of RIPA powers. In most cases investigations carried out by Council Officers will not need authorisation as they are carried out overtly not covertly.

All mobile surveillance equipment must be kept in a secure area, access to which will be controlled by the Head of Community Wellbeing, who will ensure that there is a register detailing when equipment is taken and when returned including the name and post of the Officer having control of the equipment.

**What RIPA does**

- It requires the prior authorisation and judicial approval of directed covert surveillance.
- It prohibits the Council from carrying out intrusive surveillance.
- It requires the prior authorisation and judicial approval of the conduct of Covert Human Intelligence Sources [CHIS].
- It requires safeguards for the conduct and use of CHIS.

**What RIPA does not do:**

- It does not make an unlawful act lawful.
- Make acts that are lawful unlawful.
- Prejudice existing powers available to the Council to obtain information by any means not involving conduct requiring authorisation under RIPA.
- Authorise the use of directed surveillance unless the crime threshold is met.

**Powers which are regulated**

- The interception of communications.
- The acquisition of communications data.
- Intrusive surveillance.
- Directed surveillance.
- Use of CHIS.
- Access to encrypted data.

The Council **is not** allowed to intercept record or otherwise monitor the content of communications data.

The Council **may** obtain communications data relating to service use information and subscriber information.

The Council **is not** permitted to carry out intrusive surveillance.

**Part II RIPA**

The purpose of Part II is to regulate the use of surveillance methods and safeguard the public from unnecessary invasions of privacy.

Compliance with Part II will ensure that the Human Rights Act 1998 is not breached and affords the Council protection from legal challenge if complied with correctly.

## 3. Relevant legislation

When deciding on whether to seek authorisation to use RIPA the following should be taken into account.

**Data Protection Act 2018 and the UK GDPR**

### 3.1 Fairly and lawfully processed

- make sure you do not do anything unlawful with the data.

This is the first data protection principle. In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;

- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and

### 3.2 Processed for limited purposes

In practice, the second data protection principle means that you must:

- Be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

### 3.3 Adequate, relevant and not excessive

- This is the third data protection principle. In practice, it means you should ensure that:

- You hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and

- You do not hold more information than you need for that purpose.

- So you should identify the minimum amount of personal data you need to properly fulfil your purpose.

  You should hold that much information, but no more.

  This is part of the practice known as "data minimisation".

- The third data principle states that personal information must be adequate, relevant and not excessive. Please find examples below:

  **Excessive**
  A shop asks you for postcode when you are buying shoes
  A school asks you where you live and if it is a house, flat or bungalow

  **Not Excessive**
  The local fitness centre asks for medical information
  A DVD rental shop asks for your date of birth.

### 3.4 Accurate & up to date

This is the fourth data protection principle. Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

- Take reasonable steps to ensure the accuracy of any personal data you obtain;
- Ensure that the source of any personal data is clear;
- Carefully consider any challenges to the accuracy of information; and
- Consider whether it is necessary to update the information.

### 3.5 Not kept for longer than necessary

Is the fifth data protection principle.

In practice, it means that you will need to:

- Review the length of time you keep personal data;
- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

### 3.6 Processed in line with data subject rights.

This is the sixth data protection principle, and the rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

### 3.7 Secure

This is the seventh data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being

accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who in your organisation is responsible for ensuring information security;
- make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

### 3.8 Not be transferred outside the EEA

This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas.

For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas.

The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using subcontractors abroad.

## Human Rights Act 1998

The HRA enables individuals to enforce in domestic courts the rights enshrined in the European Convention on Human Rights. When deciding to seek authorisation Officers will need to balance the rights of the individuals against the rights of the wider community. In order to be able to do so and have justification the Council's response to a breach of human rights must follow the four stages of proportionality and must be necessary.

i. Is the interference justifiable in the circumstances
ii. Is the measure considered rational
iii. Is the means being used to impair that right no more than necessary to accomplish the objective
iv. Whether a fair balance has been struck between the rights of the individual(s) and the interests of the community which is inherent in the Convention.

## 4. Types of surveillance

### 4.1 Section 26 RIPA – Directed surveillance

RIPA only applies to directed surveillance that is **covert** which is:

- A specific investigation or operation
- In a way **likely** to result in the obtaining of private information about an individual [or group] whether specifically identified for the purpose of the investigation or not **and**
- Otherwise than by an immediate response to events or circumstances would not make it practicable to seek an authorisation.

Section 48 of RIPA defines surveillance to include the following:

(a) Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
(b) Recording anything monitored, observed or listened to in the course of the surveillance; and
(c) Surveillance by or with the assistance of a surveillance device.

Covert means anything done without the knowledge of the individual or individuals being so monitored.

#### 4.1.1 Examples of Directed surveillance

- CCTV to track individuals that are unaware of the usage in a planned investigation.
- Covert observation of individuals in their own home for the purpose of establishing evidence regarding for example benefit fraud or employment matters.
- Covert observations of individuals to see if co-habiting for benefit fraud purposes
- Covert monitoring of emails, telephone or internet access to gain information around inappropriate usage.

#### 4.1.2 Examples of what is not Directed surveillance

- Observations by licensing Officers to monitor illegal private hire trading.
- CCTV where it is overt or incidental
- Urgent covert surveillance

- Overt investigations when officers make it clear to an individual why they are carrying out an investigation ie benefit officers home visits, environmental officers visits.

RIPA applies to local authorities, its Officers and contractors. It **does not** apply to private individuals.

### 4.2 Section 26(3) RIPA – Intrusive surveillance

Local authorities **are not** permitted to carry out intrusive surveillance. The definition of intrusive surveillance is directed surveillance that takes place in a residential property or private vehicle while an individual is present. It can also include using surveillance equipment though not sited on private land or within a private vehicle where it provides quality data as if it were so sited.

If Officers wish to carry out covert surveillance on private property advice should be sought prior to requesting authorisation.

## 5. Section 21(4) RIPA – Communications Data

### 5.1 Definitions of Communications Data

(a) Any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted.

(b) Any information which includes none of the contents of a communication (part from any information falling within paragraph (a)) and is about the use made by that person:

(i) Of any postal service or telecommunication service; or

(ii) In connection with the provision to or use by any person of any telecommunication service, of any part of a telecommunication system;

(c) Any information not falling within paragraph (a) or (b) that is held or obtained in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

This includes all emails, letters, documents, telephone calls, social media, telephone bills or address that can be used to identify an individual or the address from which the communication emitted.

The Council cannot authorise the interception of communications except in the following circumstances. The Council **will not** in any circumstances approve the covert surveillance of traffic data.

## 5.2 Interceptions of Communications

The Council will conduct any covert investigation involving the interception of emails, telephone or internet facilities within the eight principles of the Data Protection Act. These will be restricted to the exemptions within the Human Rights Act and RIPA. Covert surveillance will only be carried out for the following purposes:

- For the purpose of the prevention and detection of crime or the prevention or detection of disorder;
- To establish facts, or ascertain compliance by Council staff with procedures applicable to carrying out the Council's business or for training purposes;
- To detect the unauthorised use of telecommunications or electronic communications systems;
- To ensure the effective operation of such a system.

Under the Telecommunications (Lawful Business Practice) (Interception of Telecommunications) Regulations 2000 the above are permitted exceptions to the need to seek approval under RIPA. However, to ensure and monitor the use of such surveillance Officers will be required to seek authorisation from an Authorising Officer and give reasons why such approval is being requested.

## 6 Section 26(8) Covert Intelligence Human Source (CHIS)

A person is a human intelligence source if:

(a) s/he establishes or maintains a personal or other relationship with a person for the purpose of facilitating the doing of anything in (b) or (c).
(b) covertly using such a relationship to obtain information or to provide access to any information about another person or
(c) covertly discloses information obtained by the use of such relationship or as a result of its existence.

Advice should be sought from Legal Services if the use of a CHIS is being considered.

## 7 Codes of Practice

The Home Office manages procedures and guidance with regard to the arrangements for covert surveillance and property interference conducted by public authorities. The latest guidance was issued in August 2018 and can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

If an authorisation is challenged or referred to any Court or Tribunal these codes of practice will be referred to; it is important in considering any application for authorisation that you refer to them, this procedure and the Council's Policy on RIPA.

Officers should satisfy themselves prior to making an application for authorisation that they are familiar with the latest policies and guidance issued by the Home Office

## 8 Applications for authority

Applications for authorisation must be made to a designated Authorised Officer. The Officer applying for authorisation must be different from the Authorising Officer.

## 9 Why use RIPA?

RIPA provides the statutory mechanism for authorising certain types of surveillance and information gathering. RIPA safeguards the public from undue interference from a public authority, by balancing the public interest in carrying out surveillance against the rights of the individual not to have their rights infringed unless it is necessary and proportionate to do so.

By following the authorisation procedures the Council will protect itself from legal challenges of infringement of Article 8 and Article 6 of the Human Rights Act 1998. By adhering to the processes under RIPA the conduct authorised will be lawful and less open to challenge. It also enables the Council to show

in any proceedings either internal or via the Courts or Tribunals that the evidence relied on was gathered in a lawful manner.

## 10 Who is responsible for overseeing the use of RIPA?

The IPCO oversee the application of RIPA, to ensure that RIPA is applied appropriately and properly. They carry out inspections of the use of RIPA by the Council and yearly statistics have to be supplied.

Anyone who is affected by directed surveillance and believes the Council has incorrectly or improperly used the powers under RIPA can apply to the Investigatory Powers Tribunal [the Tribunal] for redress within a year of the act complained of, or if the Tribunal believes it is just and equitable to do so they may extend the time limit for making the application.

The Tribunal can award compensation, quash an authorisation and can order the destruction of any information held or obtained.

## 11 Implementation of this Guidance and the Policy on RIPA

These procedures and guidance and the Council Policy document, alongside the Codes of Practice referred to above **must** be followed when considering applying for authorisation for directed surveillance.

The documents referred to apply equally to all Council staff and any contractors or agents of the Council.

## 12 Authorisations

An Authorising Officer must not be directly involved with the investigation and cannot be responsible for authorising their own activities; paragraph 13 of this guidance lists the Council's nominated Authorised Officers.

An Authorising Officer shall not grant authorisation for carrying out of directed surveillance unless s/he believes:

- The action is necessary and proportionate.
- The criminal offence[s] is punishable on summary conviction or indictment of six months in prison or
- The criminal offence[s] relates to underage sale of alcohol or tobacco
- Necessary for the prevention or detection of crime or disorder.

- The authorised surveillance is proportionate

The first three points only apply to Directed Surveillance.

The Authorising Officer may authorise a CHIS if they believe it is necessary and proportionate s29(3) RIPA.

Authorising Officers must be satisfied that the authorisation is necessary and proportionate in all cases.

Activity that should be authorised but which is not should be reported to the Chief Surveillance Commissioner in writing as soon as the error is recognised. An initial email should be sent followed by a report. This does not apply to covert surveillance that the Authorising Officer believes does not meet the statutory criteria.

Once authorised by an Authorised Officer an application must be made to a Justice of the Peace prior to the authorised activity taking place.

Forms to be used for CHIS and directed surveillance are at appendix 2 of this document and must be filled with sufficient information to enable the Authorising Officer to make a reasoned decision. Guidance for filling out the forms is at appendix 1.

Each department must keep a central record of all authorisations and where more than one department is involved in the investigation each must hold a copy. A copy **must** also be sent to the Head of Governance to be logged on the Central Register.

If a request is received from a third party wishing to conduct surveillance on Council premises or property an authorisation **must** be obtained especially if Council Officers or equipment is involved.

**Guidance on the authorisation test.**

Authorisation will be required if the answer is yes to any of the following:

- **Is the proposed activity surveillance?** Does the activity involve monitoring, observing or listening to persons, their movements, their conversations or other activities or communications, recording anything monitored, observed or listened too in the course of the activity and whether a surveillance device will be used?

- **Is it covert?** Does the activity mean that the proposed target is unaware that it is or may be taking place?

- **Is the activity likely to result in obtaining private information about the person?** Will any information obtained be about the target's private or family life? There must be a real possibility that it will rather than a fairly remote chance.

- **Is it a foreseen or planned activity?** A decision will need to be made that the activity proposed is not an immediate response to a situation arising but is planned in advance.

If the answer to the above questions is **no** then proposed activity will not be afforded the protection under RIPA. Advice should be sought regarding any activity that is proposed but does not fall within the RIPA regime.

### 12.1 Oral applications

Urgent oral authority may be given and is valid for seventy two hours. A written application must be produced as soon as practicable after the oral authorisation is given. The applicant must fill out why the application is urgent on the form.

### 12.2 Written applications

Written applications are valid for three months only after they are signed by a Justice of the Peace.

### 12.3 Procedure for applying for Judicial approval

**Making the application**

Approval by a JP will be required for any authorisation; the authorisation will not be effective unless an order approving the authorisation is obtained.

The application to the Court must contain all information to be relied on. The JP must be supplied with the original copy of the authorisation and all supporting documents setting out the case. The judicial application form at appendix 2 must be completed.

The investigating Officer must notify the Magistrates Court as soon as possible that a hearing is required. If it is an emergency application the hearing can take place out of hours and if appropriate at the home of the JP. The judicial application will need to be in duplicate so that the JP can keep a

copy. As soon as practicable the Officer who attends the out of hours hearing must supply a signed copy of the form to the Court the next day.

## Hearing

Officers who attend the hearing **must** have the delegated authority to do so on behalf of the Council. They will be required to swear in and present evidence to the JP. The hearing of the application will be in private.

The Investigating Officer will most likely be the appropriate Officer to give evidence and answer questions from the JP. They may not necessary be the Officer who will present the evidence to the JP but will be a witness. If the case involves communications data the nominated SPOC (Single Point of Contact) should attend.

## Decision

The JP will consider if there were reasonable grounds for believing that the authorisation or notice were necessary and proportionate at the time of the authorisation and whether those grounds continue to be reasonable. They will also consider if the crime threshold is satisfied.

If there is insufficient information to determine if the authorisation meets the relevant tests the application will be refused. The decision will be recorded on the order section of the judicial application/order form. The court will retain a copy of the application and the order.

The JP can do one of three things after considering the application:

(a) Approve the application
(b) Refuse to approve the application
(c) Quash the application

If there is a technical error on the form this can normally be rectified and the application resubmitted for consideration.

If the Officer making the application does not agree with the decision made an appeal could be made to the Magistrates Advisory Committee on a point of law by way of judicial review. This will only be considered once legal advice has been obtained. The Officer **must not** consider making an application by way of judicial review him/herself.

## 13 Statutory definitions

**Authorising officer:**

These are specified as being assistant Chief Officers and more senior Officers, Assistant Heads of Service, Service Managers or equivalent responsible for the management of the investigation.

The authorisation of directed surveillance or, use of a CHIS who is likely to obtain confidential information or the deployment of a vulnerable person (by virtue of mental or other condition) or one under the age of 18 as a CHIS requires the authorisation by the Chief Executive as Head of Paid Service or in his absence the Chief Operating Officer.

**Applicant Officer:**

Is an Officer of the Council who is making the application for RIPA authorisation; this is likely to be investigating Officer.

**Crime Threshold:**

The purpose of the authorisation is for the prevention or detection of crime which either carries a maximum sentence of at least six months imprisonment or an offence relating to the sale of alcohol or tobacco products to minors.

Authorisation **cannot** be given or the purpose of preventing disorder unless this involves a criminal offence punishable (whether on summary conviction or indictment) by a maximum term of six months imprisonment.

Authorisation for directed surveillance therefore can be given for the more serious crimes only.

The Council **cannot** authorise directed surveillance for disorder that does not involve criminal activity such as dog fouling, littering or fly-posting.

The crime threshold applies only to authorisations for directed surveillance under RIPA, not to the use of CHIS or obtaining communications data.

## 14 Timelimits

For directed surveillance the time limit is three months and twelve months for CHIS, unless the CHIS is under 18 then it is one month. Applications or notices for communications data will be one month from the date the JP granted the approval.

A renewal must be authorised prior to the expiry of the original authority, but runs from the expiry date and time of the original authorisation. Authorisations may be renewed more than once if it is still considered necessary and proportionate and approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire, but you must take into account factors that may delay the renewal process which could include the availability of the Authorising Officer, consideration of the Court time table, and the availability of a JP.

## 15 Training

The Head of Governance will be responsible for ensuring all relevant Officers in the Council are properly trained.

## 16 Central Register and Records

A central register of all authorisations including applications for judicial approval will be held by the Head of Governance. The contents of the forms and authorisations will be monitored to ensure that they comply with RIPA.

## 17 Responsibilities

The Head of Governance will ensure that there is:

- Compliance with RIPA, Policy, the guidance and legislation
- Engage with and meet with the Commissioner when inspections are due [every three years].
- Oversee any post inspection action recommended by the Commissioner

## 18 Authorising Officers

Senior Responsible Officer: Simon Hill Head of Governance and Monitoring Officer

Authorising Officer (Confidential Material only) Brian Keane: Chief Executive

Authorising Officers:

Simon Freeman: Head of Finance
Wendy Makepeace: Housing Operations Manager

Jane Greer: Head of Community and Wellbeing

Bev Thomas: Policy and Performance Manager

RIPA Administration Officer
Julie Galvin: Legal Services Manager

## 19 Overview and Scrutiny of this Guidance

This guidance will be reviewed and where necessary amended, at least yearly.

The guidance will be approved by the Head of Governance.

Elected Councillors will not be involved in any decision[s] made on specific authorisations granted.

**Appendix 1**

**Guidance on filling out the forms:**

## 1. Ground on which action is necessary

### 1.1 For prevention or detecting crime

This can be used in the context of prosecutions the Council may carry out or be involved in for example licensing, planning, housing or environmental.

It can also be used in a personnel context such as theft or improper use of Council equipment.

### 1.2 For the prevention or detecting of disorder

This could be used for justification for anti-social behaviour, possession or injunction proceedings.

## 2. Proportionality

There are two aspects to the proportionality test the proposed activity must be necessary and proportionate.

### 2.1 Necessity

The Authorising Officer must be satisfied that the proposed covert activity is a necessity. There must be a recognisable offence to either prevent or to detect, prior to the authorisation being granted. If there is no recognisable offence it does not prevent the use of covert surveillance but there is no protection for the Council under RIPA. No unauthorised covert surveillance should be undertaken.

Once the Authorising Officer is satisfied the proposed activity is necessary they will need to satisfy themselves that it is proportionate in the circumstances.

### 2.2 Proportionate

The Authorising Officer will need to demonstrate how they have reached the conclusion that the proposed activity is proportionate. A written explanation must be given with reasons why they have reached the decision that the

proposed activity is not disproportionate in the circumstances described by the applicant Officer.

The following four elements must be considered and evidenced in the consideration of the Authorising Officer:

(a) Balancing the size and scope of the operation against the gravity and extent of the perceived mischief

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

(c) That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result

(d) Evidencing what other methods have been considered and why they were not appropriate.

The proposed activity will not be proportionate if it is excessive in the circumstances or the information could be obtained by other means.

## 3. Identification

Identify who are to be the targets, if possible give the date of birth. If it is not a person that is the intended target give as much information as possible to identify the premise or property.

In this case property or premise for example would be a house that is being targeted for neighbour nuisance or drug complaints and the identities of those involved is not known.

## 4. The action to be authorised

Give as much information as possible about the proposed activity so the Authorising Officer can consider the necessity and proportionality of what is being proposed.

Remember the Council cannot authorise **intrusive surveillance** of a person's private home or vehicle or use a surveillance device that consistently provides data of consistent or high quality as if you were present.

## 5. Account of the investigation or operation

Include all activities that you propose to carry out, including the methods you propose to use, ensure there are sufficient details so a clear picture is presented of what needs to be done.

## 6. Collateral intrusion

The Authorising Officer should take into account the risk of interference with the private and family life of persons not the intended subject of the proposed activity.

Evidence will need to be included from the Authorising Officer on what measures have been considered to minimise the risk of such interference.

Where the authorised activity interferes unexpectedly with the privacy of individuals who are not the intended subject the Investigating Officer must inform the Authorising Officer.

## 7. Risk assessment

It is good practice for a risk assessment to be carried out in all cases especially to discharge the Council's responsibility to its employees under the Health and Safety etc at Work Act 1974.

A risk assessment **must** be done prior to authorisation of any CHIS activity.

## 8. Anticipated start

The authorisation is effective from the time when urgent authorisation is given or when an order approving the authorisation is obtained from a JP.

## 9. Authorising Officer comments

The Authorising Officer must record, explain and insert all considerations given in either agreeing to the authorisation or declining to approve the request.

Bland statements either approving or not approving the application for authorisation are not acceptable the Authorising Officer must show his or her considerations.

Failure to do so may lead to corrective action being imposed on the Council by the Office of Surveillance Commissioners.

## 10. Authorising Officer recommendations

The authorisation is for three months (unless it is an urgent application then it is for 72 hours) Reviews should be built into the process, either so that further authorisation can be granted or authorisations can be cancelled at the earliest opportunity.

Remember if authorisation is given on a Wednesday it will end at midnight on a Tuesday.

## 11. Urgent authorisations

Urgent authorisations can be obtained orally but must be followed as soon as practicable by a written application.

**Appendix 2**

**Authorisation Forms and Judicial Approval**

**Directed Surveillance**

(a) Application for the use of directed surveillance
https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

(b) Renewal of directed surveillance

https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

(d) Review of the use of directed surveillance

https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance

(e) Cancellation of directed surveillance.

https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

**Covert Human Intelligence Source.**

(a) Application for the use of CHIS
https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis

(b) Renewal of authorisation for use of a CHIS
https://www.gov.uk/government/publications/renewal-of-authorisation-to-use-covert-human-intelligence-sources

(c) Review of the use of a CHIS
https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis

(d) Cancellation of the use of CHIS.
https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence-sources-chis

**Communications data**

The forms to apply for either:

(a) Application for communications data
(b) A request for a schedule of subscriber information

Are available online at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

**Judicial approval**

The application forms can be found in the Home Office Guidance to Local Authorities in England and Wales on the Judicial Approval process for RIPA and the crime threshold for directed surveillance at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf