



WILTSHIRE FIRE & RESCUE SERVICE

REFERENCE GUIDE TO THE



Awarded for excellence

Scope

This code of practice applies to authorisations
For surveillance (not involving entry on or
Interference with property or wireless telegraphy
As regulated by the Police Act 1997)

INTRODUCTION

Background

The Human Rights Act 1998 (HRA) was introduced to give effect to European Convention on Human Rights (ECHR) and came into force in October 2000. From that date the ECHR became part of our domestic law. Consequently, individuals may enforce their rights under ECHR in domestic courts rather than having to go before the European Court of Human Rights in Strasbourg.

The HRA imposes a duty upon the Wiltshire Fire & Rescue Service to act in a way that is compatible with the rights under the ECHR. Failure to do so may enable a person to seek damages against the Service or to use our failure as a defence in any proceedings that we may bring against them.

European Convention on Human Rights (ECHR)

Under Article 6 of the ECHR, everyone is entitled to a fair and public hearing, within a reasonable time, of any criminal charge against him or her or into the determination of any civil dispute.

Under Article 8, everyone also has the right to respect for their private and family life, their home and their correspondence. The Article recognises that there may be circumstances in a democratic society where it may be necessary for the State (which includes the Wiltshire Fire & Rescue Service) to interfere with this right. Surveillance on a person by monitoring, observing or listening to persons, recording their movements, their conversations or other activities or communications or using a surveillance device e.g. a camera, can only be done in accordance with the law and for clearly defined purposes. These purposes with regard to the Wiltshire Fire & Rescue Service are:

- For the purpose of preventing or detecting crime or of preventing disorder.
- In the interests of public safety.
- For the purpose, in an emergency, of preventing death or injury or any damage to person's physical or mental health, or mitigating any injury or damage to a person's physical or mental health.

Impact on Investigations

To be able to justify any interference with the right to respect for an individual's privacy, and comply with the HRA, the Wiltshire Fire & Rescue Service will need to demonstrate that any intrusion into an individual's privacy is necessary for the purposes of an investigation. Surveillance is often a necessary part of any investigation. Covert surveillance is regulated by the Regulation of Investigatory Powers Act (RIPA) 2000. Where covert surveillance is considered appropriate it will be necessary for it to be authorised before it can commence. Authorising officers will need to satisfy themselves that a defensible case can be made for covert surveillance activity.

The Secretary of State has issued codes of practice on the use of covert surveillance under RIPA. The codes are admissible as evidence in criminal and civil proceedings. A court or tribunal must take any relevant provision of the codes into account.

Policy and Code of Guidance

To ensure that authorisations and procedures are applied in a consistent way, the Wiltshire Fire & Rescue Service has adopted a policy covering the authorisation and use of covert surveillance, as well as approving a Code of Guidance.

This Policy and Reference Guide is in three parts:

The Wiltshire Fire & Rescue Service's Policy on the Use of Surveillance
Easy reference guide to the code of practice and procedure
Forms

The Statutory Codes of Practice are available in Part II, sub paras a and b, of this Reference Guide. In cases of conflict between this Reference Guide and the Statutory Code of Practice, the latter will take precedence.

This Policy and Reference Guide has been prepared by the following officer:

PHILLIP WIRTH – Wiltshire Fire Brigade Solicitor

PART 1 – STATEMENT OF POLICY

The Wiltshire Fire & Rescue Service and officers undertaking investigations will endeavour to comply with the following statement of policy at all times:

In carrying out investigations the Wiltshire Fire & Rescue Service will seek to ensure that any interference with the rights of any person is in accordance with the law and is justified by reason of it being undertaken for a legitimate purpose. The means to be employed in any investigation will be proportionate to the seriousness of the matter under investigation. The use of covert surveillance in particular will be in accordance with any statutory code of practice then in force.

PART 2 – EASY REFERENCE GUIDE TO PROCEDURES AND THE CODES OF PRACTICE

Introduction

This easy reference guide seeks to set out the Wiltshire Fire & Rescue Service's procedures for the authorisation of surveillance investigations and to provide a brief summary of the main points in the Statutory Codes of Practice on Covert Surveillance. The Statutory Code of Practice for Directed Surveillance, the use or conduct of a Covert Human Intelligence Source (CHIS) and Accessing Communications Data can be located on the Home Office Website at:

- a. Directed Surveillance and Covert Surveillance
http://www.opsi.gov.uk/si/si2006/uksi_20061874_en.pdf

- c. Accessing Communications Data
<http://security.homeoffice.gov.uk/ripa/communications-data/data-code-of-practice/>

This guidance aid is for clarification and is not a substitute for the Codes themselves.

General

Surveillance includes monitoring, observation or listening to persons, their movements, their conversations or their other activities or communications. If surveillance is carried out without the person's knowledge, it will be covert and require prior authorisation.

RIPA applies to 'Directed Surveillance', Accessing Communications Data and the use of a CHIS. The Wiltshire Fire & Rescue Service can only authorise directed surveillance, accessing communications data and the use of a CHIS.

What is 'Directed Surveillance'

Surveillance will be 'directed surveillance' if:

It is covert

Undertaken for a specific investigation, and

Is carried out in such a way as to make it more likely that private information will be obtained about a person.

'Private information' includes any information relating to a person's private and family life. This phrase echoes that of Article 8 of the ECHR and should therefore be considered to include questions of personal and sexual identity, personal information, telephone calls from business premises, health and injury and sexual activity.

Directed surveillance excludes surveillance carried out on residential premises or in any private vehicle where the observer is present in the premises or vehicle or is carried out using a surveillance device.

What is a Covert Human Intelligence Source

A person is a source if he covertly establishes or maintains a personal relationship where the other party is unaware, for the purpose of obtaining information. Also to covertly disclose information he obtains as a result of the relationship.

When might the Service use a CHIS

The Service is involved with Fire Regulations enforcement. The use of a CHIS may be required to obtain information in respect of this enforcement. The Service may also use a CHIS to see if there is an abuse of someone's official position, e.g. stealing money.

Accessing Communications Data

Accessing communications data is any conduct in relation to a postal service or telecommunication system for obtaining communications data and the disclosure to any person of such data. Communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with websites. "Data" in relation to a postal item, means anything written on the outside of the item.

Is the surveillance permitted and does it require authorisation?

The process and procedures outlined in the Code of Conduct are shown diagrammatically in the attached help charts for Directed Surveillance, the use of or conduct of a CHIS and Accessing Communications Data.

Completion of Risk Assessments

Where a request for surveillance is requested either directed, CHIS or accessing communications data, the Authorising Officer will have to be satisfied that the risks of outside interference have been properly considered. Outside interference is where a third party's privacy is being infringed. For example, where an officer takes still or video photographs, or observes one or more innocent parties, this could be considered as being outside interference. If, in the course of investigating a case, a third party's privacy has been inadvertently invaded, the action should be defensible (from a legal viewpoint), providing the grounds for investigation are sound – i.e. the investigation has been undertaken to detect and or prevent breaches of fire regulations for which the Service is the enforcing authority and the actions are reasonable.

Accordingly, Investigating Officers may need to identify whether a location is suitable for surveillance, for example 'drive by's'. This action is not prevented under the Code of Practice.

Obtaining Authorisation for Surveillance – General Points

Written Authorisation

Unless a warning letter has been sent out to an individual advising them that a complaint has been received and informing them that monitoring of a type described in the letter will be undertaken, before surveillance can be carried out, the Investigating Officer must:

- Complete an application for authorisation to use directed surveillance on Form RIPA 1, and for use of a CHIS Form RIPA 5
- For accessing communications data Forms RIPA ACD must be used. Applications for communications data may only be made by persons in the same public authority as an Authorised Officer.
- Obtain authorisation from an Authorised Officer. The Wiltshire Fire & Rescue Service has designated the following officers to authorise surveillance:

| | | |
|------------------------|---------------------------|--------------|
| Service Manager | Deputy Chief Fire Officer | All Purposes |
| Clerk to the Authority | Clerk | All Purposes |
| Service Treasurer | Treasurer | All Purposes |

Single Points of Contact (SPOC)

Notices and where appropriate, authorisations for communications data should be channelled through the SPOC who will act as the focal point for all contact with the postal or telecommunications operators on a regular basis. The SPOC will also advise the applicant and Authorising Officer whether an authorisation is appropriate. Each SPOC will receive Home Office accredited training and issued with a Personal Identification Number. This will provide a safeguard between organisations before being given access to postal and telecommunications data.

Time Limit on Written Authorisation

Written authorisation for directed surveillance is valid for a maximum of three months, and must be reviewed by the Authorising Officer at least every month. If necessary to continue the surveillance for longer than three months, an application for renewal of authorisation for surveillance must be made on Form RIPA 2. Authorisation for the use of a CHIS will cease to have an effect unless renewed at the end of a period of 12 months beginning with the date on which it took effect. Application for the renewal of a CHIS must be made on form RIPA 6. The duration of authorisations and notices for accessing communications data is one month. This period will begin when the authorisation is granted or the notice given. If necessary, shorter periods should be specified by the designated officer. For future data disclosure may only be required up to one month. For historical data disclosure should comply within a time as is

reasonably practicable. Renewal of an authorisation or notice may be at any time during the month by following the same procedure as in obtaining a fresh authorisation.

Time Limit on Oral Authorisation

If urgent surveillance is required oral authorisation can be given but the Authorising Officer must complete Form RIPA 1 or RIPA 5 as soon as practicable. Oral authorisation is for use where, for instance, there has not been sufficient time to obtain written authorisation, but an Investigating Officer knows that immediate surveillance is required in order to obtain the required evidence. This is a situation, in relation to surveillance in or into a private place, which will be rare in relation to the Service's work.

Oral authorisation may only apply for 72 hours from the time given. If the surveillance is required to continue past that period written authorisation must be sought. An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain communications data for the purpose set out in section 22(g) of the Act. "For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".

Cancellation of Authorisation of Surveillance

At the end of any directed surveillance, which has been carried out, the Authorising Officer, must complete Form RIPA 3 to cancel the authorisation for surveillance. To cancel the use of a CHIS then Form RIPA 7 must be used. Authorisations and notices regarding communications access should be cancelled as soon as it is no longer necessary. The duty to cancel falls on the designated person who issued it. Relevant postal or telecommunications operatives should also be informed of the cancellation.

When Authorisation of Surveillance In or Into a Public Place is Not Required

The use of CCTV surveillance systems is overt and does not require authorisation. Equally, where a person suspected of having committed an offence has been notified that his/her activities are being monitored, no authorisation will be required. For example, the Service receives a noise complaint, or it is alleged that Service appliances are being used for inappropriate private purposes. If a letter is sent to the person responsible for the alleged nuisance or notifying him that his activities are now being monitored any surveillance will not be covert.

Surveillance where it is likely that Confidential Material will be Obtained

If, exceptionally, an Investigating Officer thinks that in the course of conducting directed surveillance or the use of a CHIS, in or into a private place he may obtain confidential information, the Investigating Officer will have to obtain authorisation on Form RIPA 1 or 5 as required. When considering whether authority should be given the Authorising Officer will need to consider the likelihood of confidential information being acquired.

Temporary Unforeseen Surveillance In or Into Private Places

On occasions, it may be that an Investigating Officer needs to continue surveillance on premises or land in order to:

- Keep in contact with a moving subject, or
- To determine whether the subject has been lost

Surveillance in these circumstances can be conducted without authorisation but continues only for as long as necessary to keep contact with the subject or establish whether the subject has been lost.

Reviews

Regular reviews of authorisations should be undertaken to assess the need for the use of directed surveillance and the use of a CHIS to continue. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained. The results of a review should be recorded on the authorisation record. Particular attention is drawn to the need to review authorisations frequently where the use of a CHIS or directed surveillance provides access to confidential information or involves collateral intrusion.

Reviews of directed surveillance must be made on Form RIPA 4 and for the use of a CHIS, Form RIPA 8. In each case the authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Keeping Records

All Investigating Officers have a legal obligation to keep accurate and full records of investigations under the Criminal Investigations and Procedures Act 1996 Code of Practice.

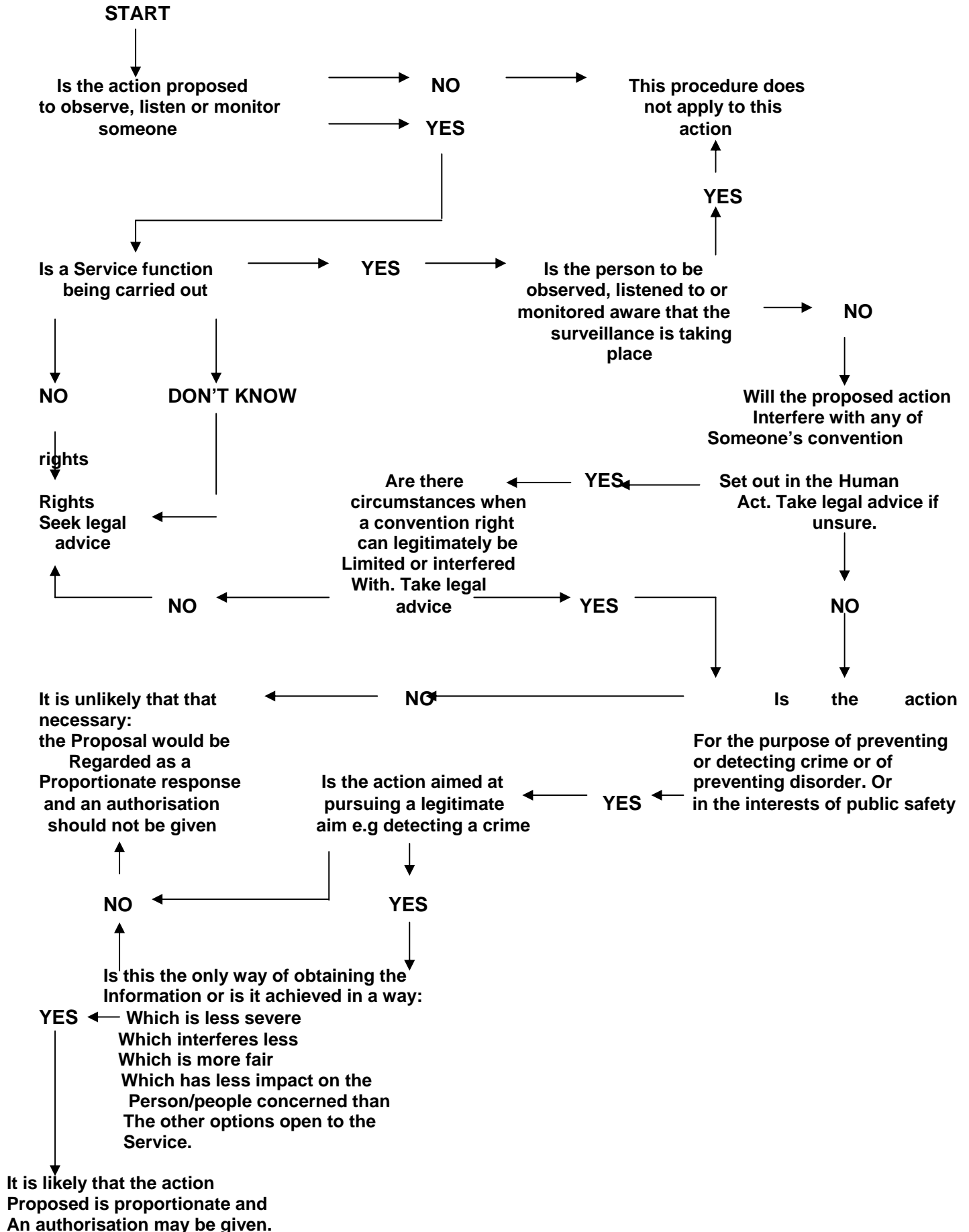
Copies of the risk assessments, authorisations, renewals, reviews and cancellations given should be retained on the investigating file. In particular, for the purposes of the Surveillance and Communications Codes of Practice, Investigating Officers must keep, in the investigation file:

- Reasons for any application for an oral application for authorisation
- An account of events observed and/or conversations overheard
- A full account of any surveillance, which has taken place in or on a private place (undertaken in order to maintain contact with the moving subject or to assess whether the subject has been lost).
- Reasons for and the nature of, intrusion in or into a private place, and the results
- Reasons for selecting a subject when authorised only for general observations, without a specified subject.

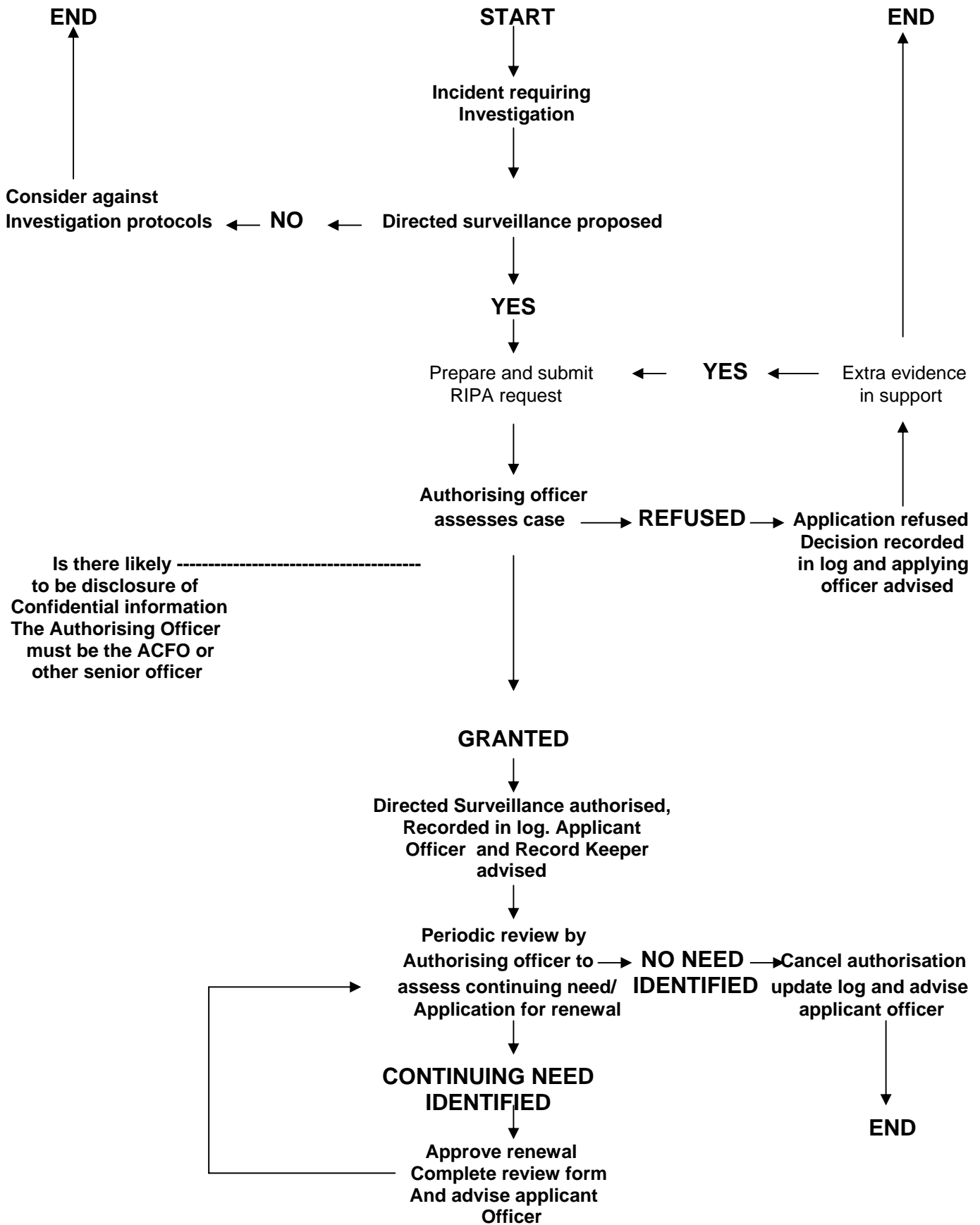
The Investigating Officer's official notebook is used to maintain the account of the events observed, and heard.

HELP CHART

This help chart is for guidance when considering the use of Directed Surveillance



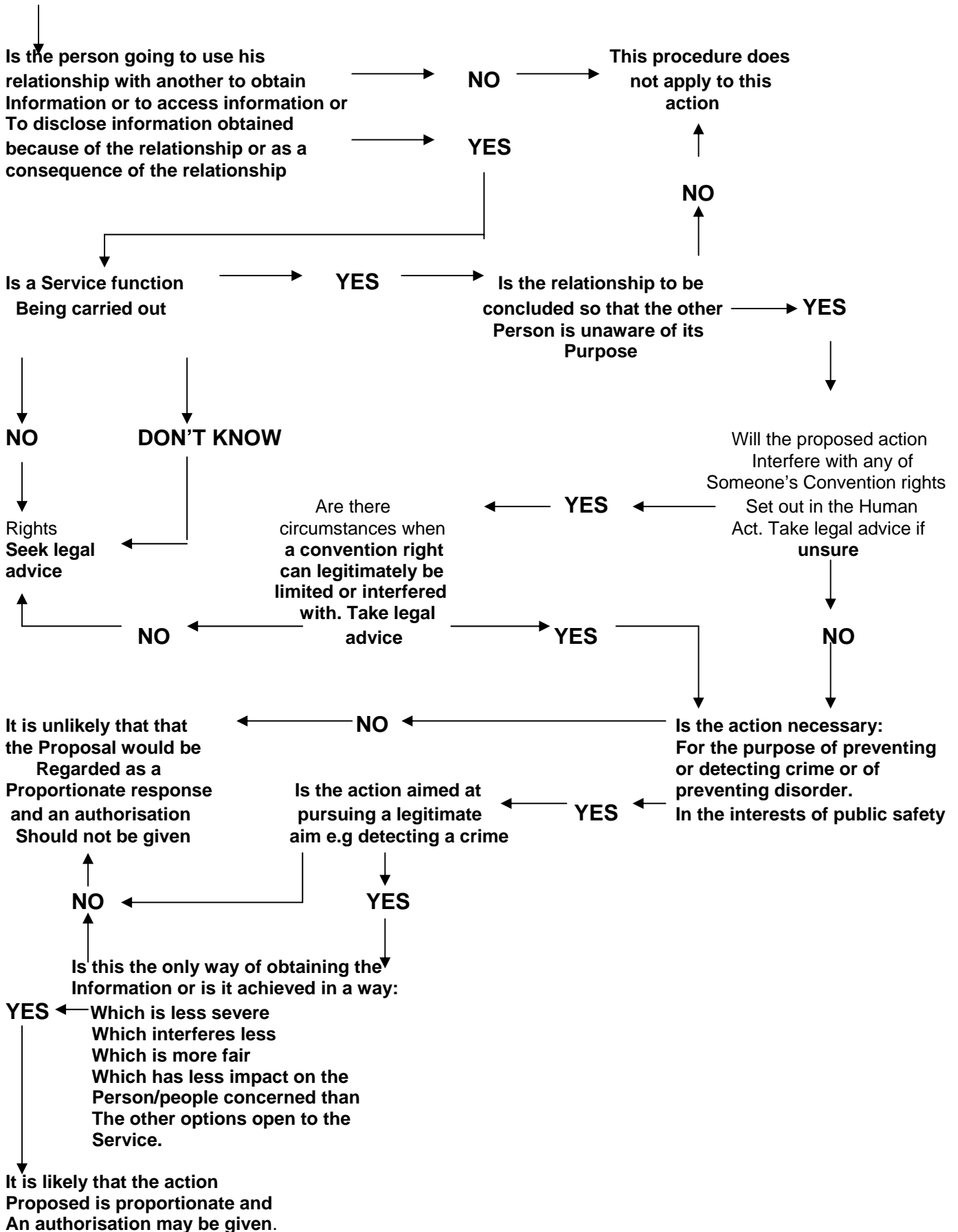
FLOW CHART



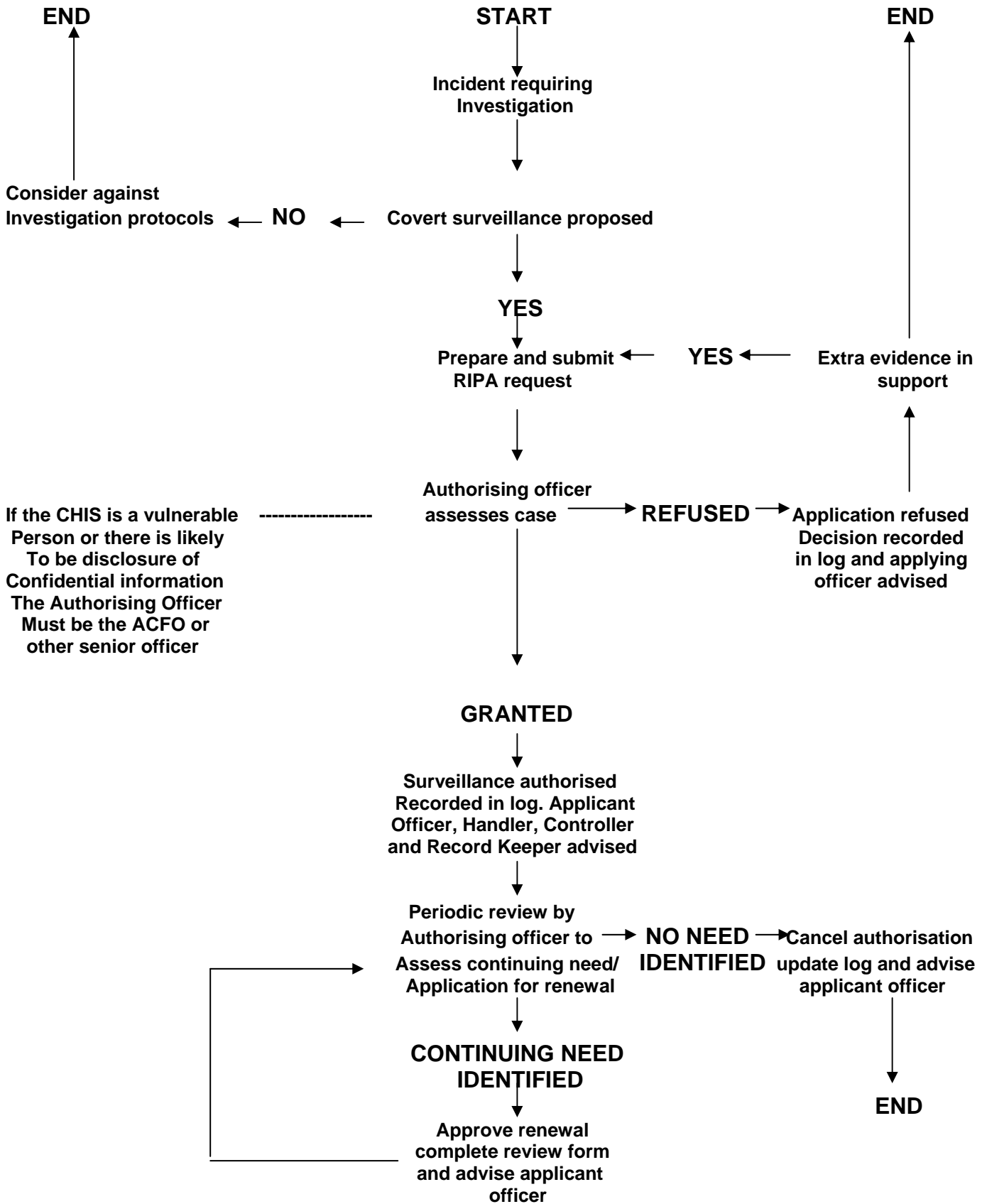
HELP CHART

This help chart is for guidance when considering the use of or the conduct of a CHIS.

START

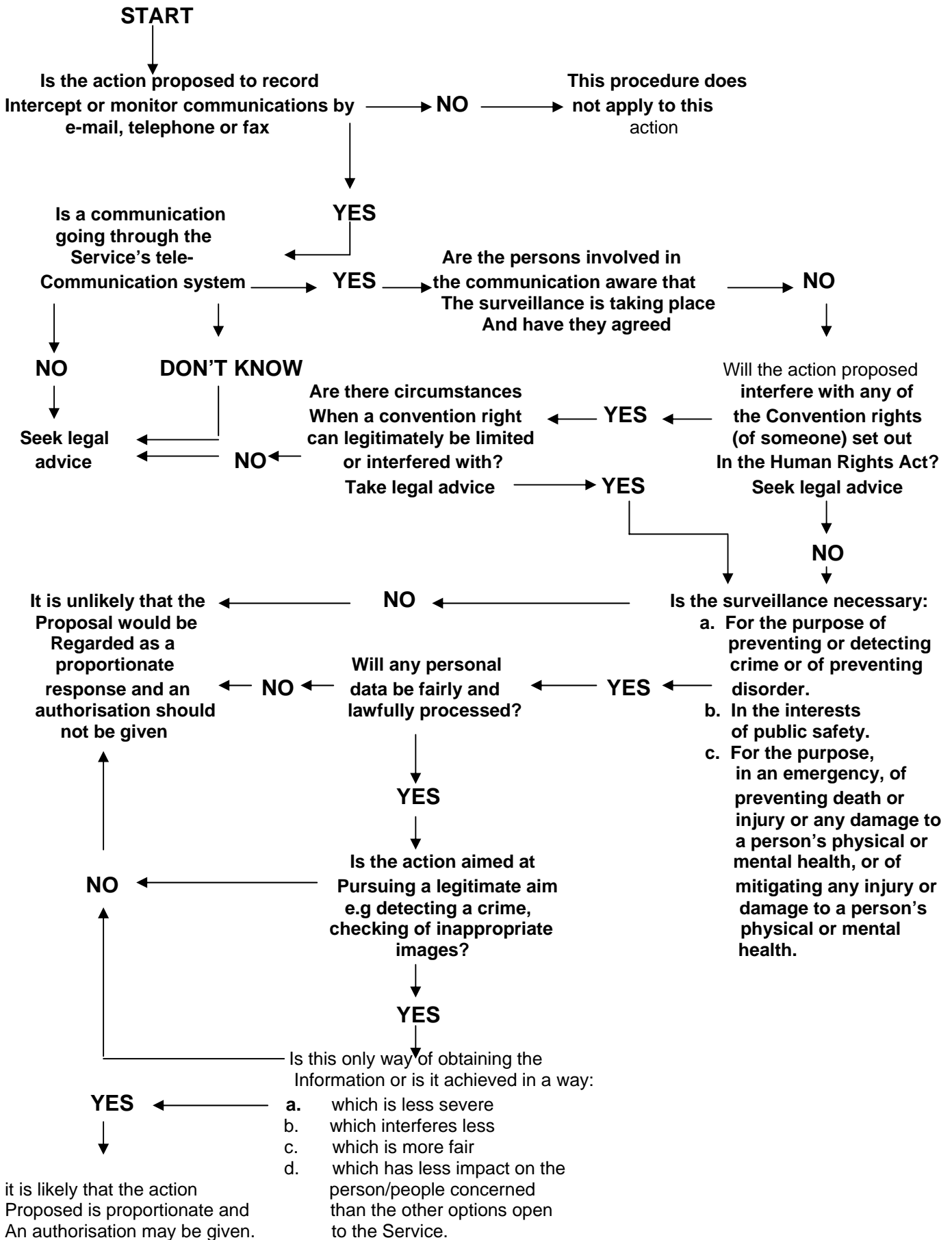


FLOW CHART



HELP CHART

This help chart is for use when considering authorisation to acquire communications data.



FLOW CHART

