Regulation of Investigatory Powers Act 2000

(RIPA)

Policy and Guidance

Document Control

Purpose of document:	The approach to the use of RIPA powers and the process followed by Fenland District Council
Intended audience:	Officers who may use directed covert surveillance or covert human intelligence sources as part of an investigation
Type of document:	Policy and Procedure
Document lead/author	
Other documents that link to this one:	Data Protection Policy ICT Acceptable Use Policy Social Media Guidance for Members Social Media Guidance for Employees Data Retention Policy Open Data Research Policy
Document ratified/approved by:	
Version number:	
Issue date:	
Dissemination method:	
Date due for review:	
Reviewers:	

DOCUMENT REVISION RECORD:

Description of amendments:	Version No.	Date of re-approval and re-issue

Contents

Table of Contents

PART A Introduction & RIPA General

1. Introduction

1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of undercover officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) governs these activities and provides a means of ensuring that they are carried out in accordance with law and subject to safeguards against abuse.

All surveillance activity can pose a risk to the Council from challenges under the Human Rights Act (HRA) or other processes. Therefore, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

In preparing this policy the Council has followed the RIPA Codes of Practice (December 2022) and Investigatory Powers Commissioner Commissioners (IPCO) guidance.

There are Home Office Codes of Practice that expand on this guidance and copies are held by each Authorising Officer. They can be accessed here and officers should ensure that they are consulting the latest version.

The Codes do not have the force of statute but are admissible in evidence in any criminal and civil proceedings. As stated in the Codes, "if any provision of the Code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account".

1.2 Who to contact for advice?

If having read this document you are unclear about any aspect of the process or need support then you should contact one of the following officers:

- Sam Anthony, Approved Authorising Officer - SAnthony@fenland.gov.uk;
- Peter Catchpole, Approved Authorising Officer - PeterCatchpole@fenland.gov.uk;
- Amy Brown, RIPA Coordinator – amybrown@fenland.gov.uk;
- Carol Pilson, Senior Responsible Officer (SRO) - cpilson@fenland.gov.uk;

These roles are defined in greater detail in Section D, however the below provides a summary.

Senior Responsible Officer – a Senior Responsible Officer (SRO) provides senior management oversight of the use of RIPA and provides assurance and integrity for the process. This will include oversight of authorisations, errors, reporting, training and inspection.

RIPA Coordinator will maintain the central registers for covert surveillance and communications data and is responsible for coordinating of training, updates of policies, procedures and inspections in conjunction with the Head of HR/OD.

Authorising Officer (RIPA) – the Code of Practice requires that an Authorising Officer must be of service manager or above rank however the Council's approach taken is to consider Authorising Officers at head of service level as a minimum. In order to be an authorising officer, the individual must be named in this Policy. An Authorising Officer will consider the application made under RIPA. They will consider the information provided by the applicant and determine whether there is necessity and proportionality in authorising the surveillance request.

1.3 Useful Websites

General Guidance from the Investigatory Powers Commissioner's Office	https://www.ipco.org.uk/
Home Office guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf
RIPA Forms	https://www.gov.uk/guidance/surveillance-and-counter-terrorism
Covert surveillance and property interference Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Interception of Communications Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Covert Human Intelligence Sources Code of Practice	https://www.gov.uk/government/collections/ripa-codes

2. Scope of Policy

2.1 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity that is carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS). This will ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

2.2 This document provides guidance on the authorisation processes and the roles of the respective staff involved.

2.3 The Policy also provides guidance on surveillance which may be necessary to be undertaken by the authority but it falls outside of the scope of the RIPA legislation. This type of surveillance will still need to be considered as necessary and proportionate to what it seeks to achieve and be compliant with the Human Rights Act. (See Section 21).

2.4 The policy also identifies the cross over with other policies and legislation, particularly with data protection legislation including the UK General Data Protection Regulation, the Data Protection Act 2018 (including Part 3 "Law Enforcement Processing") and the Criminal Procedures & Investigations Act 1996.

2.5 All RIPA covert activity will have to be authorised and conducted in accordance with this Policy, the RIPA legislation and Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued under section 71 RIPA for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from:

Covert surveillance and property interference Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Interception of Communications Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Covert Human Intelligence Sources Code of Practice	https://www.gov.uk/government/collections/ripa-codes

3. Background to RIPA and Lawful Criteria

3.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR).

3.2 Article 8 of the European Convention on Human Rights states that: -

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

2) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

3.3 The right under Article 8 is a qualified right and Public Authorities can interfere with this right for the reasons given in 3.2 (2) above if it is necessary and proportionate to do so.

3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a Local Authority may not breach an individual's Human Rights, unless such surveillance is **lawful,** consistent with Article 8 of the ECHR and is both **necessary** (see Part D section 43) and **proportionate** (see Part D section 44) to the matter being investigated.

3.5 RIPA provides the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is HRA compatible.

3.6 However, under RIPA, Local Authorities can now only authorise Directed Surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum term of at least six month's imprisonment; (serious crime criteria) or involves the sale of alcohol or tobacco to children. (See Part B Section 15).

3.7 The **lawful criteria for CHIS** authorisation is **prevention and detection of crime and prevention of disorder.** The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.

3.8 In either event, the Council's authorisation can only take effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.9 RIPA ensures that any surveillance which is undertaken following a correct authorisation and approval from a Justice of the Peace is lawful. Therefore, it protects the authority from legal challenge. It also renders evidence obtained lawful for all purposes.

4. Consequences of Not Following RIPA

4.1 Although not obtaining authorisation does not make the authorisation unlawful per se, *it is a requirement of Fenland District Council and this Policy* and it does have significant consequences: -

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own claim on Human Rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council be subject to reputational damage and could face a claim for financial compensation;
- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints Part G section 67)
- It is likely that the activity could be construed as an error and therefore have to be investigated and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO). (See Part G Section 66 Errors),

5. Independent Oversight

5.1 RIPA is overseen by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

5.2 They have unfettered access to all locations, documentation and information systems as is necessary to carry out their full functions and duties and they will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly. Their website provides good general guidance, https://www.ipco.org.uk/.

5.3 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information they require for the purpose of enabling them to carry out their functions. Therefore, it is important that the Council can show it complies with this Policy and with the provisions of RIPA.

6. Council oversight

6.1 The use of RIPA powers will be a standing item on the agenda for the Audit and Risk Management Committee. An annual report will be produced detailing the usage along with any inspections, changes to policy and procedure.

6.2 An annual report will be produced for Senior Management detailing the usage along with any inspections, changes to policy and procedure.

7. Training

7.1 There will be a bi-annual programme of training for officers, which may include face to face or e-learning training. Refresher training will be provided on a biannual basis. Officers may be required to confirm they have read documentation and have understood the intervening times.

7.2 Only formally trained Authorised Officers will be permitted to authorise applications.

PART B Surveillance, Types and Criteria

8. Introduction

8.1 It is important to understand the definition of surveillance; what activities are classed as surveillance and the different types of surveillance covered by RIPA and the HRA. Surveillance can be both overt and covert and depending on their nature, are either allowed to be authorised under RIPA or not. There are also different degrees of authorisation depending on the circumstances.

9. Basic determination of RIPA

It is critical that prior to any activity being undertaken, the requesting officer and an Authorising Officer undertake an assessment of the activity proposed.

This assessment should follow the procedure as detailed below.

Question	Answer	Notes
1. Is the surveillance activity covert?	**Yes – proceed to question 2**	This means that a subject is unaware of the activity due to the way it being undertaken
2. Is the surveillance directed?	**Yes – proceed to question 3**	This means that the activity is for a specific investigation or purpose
3. Is the investigation into a criminal offence?	**Yes – proceed to question 4**	If it is not an investigation into the alleged commission of a criminal offence then RIPA does **not** apply however you should always be able to show that you have considered whether RIPA does apply.
4. Are you likely to obtain confidential or private information	**Yes – proceed to question 5**	If you are not likely to obtain such information then RIPA does not apply.
5. Does the offence meet the crime threshold?	**If yes then RIPA applies**	If it does not then RIPA does **not** apply however you should always be able to show that you have considered whether RIPA does apply.

10 . Surveillance Definition

10.1 **Surveillance is:**

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

10.2. Overt Surveillance

10.2.1 Overt surveillance is where the subject of surveillance is aware that it is taking place. Either by way of signage such as in the use of CCTV or because the person subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights Act and be necessary and proportionate. Any personal data obtained will also be subject to data protection legislation.

10.3. Covert Surveillance

10.3.1 Paragraph 2.2 of the Covert Surveillance and Property Interference Revised Code of Practice defines Covert Surveillance as “surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place” and is covered by RIPA. Covert surveillance is categorised as either **intrusive** or **directed.**

10.3.2 There are three categories of covert surveillance regulated by RIPA: -

1) **Intrusive surveillance** (Local Authorities are not permitted to carry out intrusive surveillance).

2) **Directed Surveillance;**

3) **Covert Human Intelligence Sources** (CHIS).

11. Intrusive Surveillance

11.1 **Fenland District Council has no authority in law to carry out Intrusive Surveillance and under no circumstance should any officer or other representative of the Council attempt to use it.**

It is only the Police and other law enforcement agencies that can lawfully carry out intrusive surveillance.

11.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

- 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.

11.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device 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. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

11.4 A risk assessment of the capability of equipment being used for surveillance on residential premises and private vehicles, such as high-powered zoom lenses, should always be carried out to ensure that its use does not meet the criteria of Intrusive Surveillance.

12. Directed Surveillance Definition

12.1 The Council can lawfully carry out Directed Surveillance **provided that it is compliant with the requirements set out in this Policy**. Surveillance is Directed Surveillance if the following are all true:

- It is covert, but not intrusive surveillance;
- It is conducted for the purposes of a specific investigation or operation;
- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted 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.

13. Private Information

13.1 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are in at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

13.2 The Code of Practice provides guidance on what is private information. They state private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

13.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a Public Authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognizing that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

13.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a Directed Surveillance authorisation may be considered appropriate.

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

13.6 Paragraph 3.3 of the Covert Surveillance and Property Interference Code of Practice confirms that information which is non-private may include publicly available information such as, books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

13.7 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance (see Part D section 45).

14. Confidential or Privileged Material

14.1 Consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes:

- where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. (9.29 to 9.35 of the Covert Surveillance and Property Interference Code of Practice);
- confidential journalistic material or where material identifies a journalist's source, (9.36 to 9.46 of the Covert Surveillance and Property Interference Code of Practice);
- where the material contains information that is legally privileged, (9.47 to 9.75 of the Covert Surveillance and Property Interference Code of Practice).

14.2 Guidance on each of these can be found in the Revised Codes of Practice as noted above. In the event that these types of information may be or are likely to be acquired, officers should consult the Revised Codes of Practice, the SIRO and RIPA Coordinator.

14.3 Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material **may be authorised only by the Chief Executive (or their appointed deputy in their absence) and shall be sought by via the Authorising Officer in consultation with the SIRO**.

14.4 In cases where the likely consequence of the conduct of a Covert Human Intelligence Source would be for any person to acquire knowledge of confidential material, the deployment of the Covert Human Intelligence Source **may be authorised only by the Chief Executive (or a deputy in their absence) and shall be sought via the Authorising Officer in consultation with the SIRO**.

14.5 In general, any application for an authorisation which 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. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

14.6 The following general principles apply to confidential material acquired under properly approved authorisations:

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. If there is doubt as to whether the material is confidential, advice should be sought before further dissemination takes place.
- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should be disseminated only where the requesting officer (having sought advice) is satisfied that it is necessary for a specific purpose.

14.7 The retention of dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

14.8 Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. **This should only be with the approval of the Chief Executive and Senior Responsible Officer**.

15. Lawful Grounds/Crime Threshold

151 The Lawful Grounds for Directed Surveillance is a higher threshold for Local Authorities and cannot be granted unless it is to be carried out for the purpose of preventing or detecting a criminal offence(s) and it meets the serious crime test i.e. that the criminal offence(s) which is sought to be prevented or detected is:

1) Punishable, whether on summary conviction or on indictment, by a maximum term **of at least 6 months of imprisonment**, or,

2) 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 (see 1.4 above). This is the only ground available to the Council and hence the only justification.

15.2 Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

16. General Observation Activities – When Might Authorisation Not be Required?

16.1 The general observation duties of council officers will not require authorisation under RIPA whether covert or overt. Such duties form part of the functions we are required to provide as opposed to pre-planned surveillance of a person or group. Paragraph 3.33 of the Covert Surveillance and Property Interference Code of Practice provides some examples of when an authorisation may not be required.

Example 1: Plain clothes police officers on patrol to monitor a fly tipping hot-spot or prevent and detect it would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive approach, to identify offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. **A directed surveillance authorisation need not be sought.**

Example 2: Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine their suspected involvement in flytipping. It is proposed to conduct covert surveillance of Z and record their activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. **A directed surveillance authorisation should therefore be considered.**

17. Test Purchases

17.1 Test purchase activity does not in general require authorisation as a CHIS under RIPA as vendor-purchaser activity does not normally constitute a relationship as the contact is likely to be so limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation as a CHIS should be considered. If the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a Directed Surveillance authorisation.

Example of CHIS authorisation not needed	Example of CHIS authorisation needed
Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.	In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

17.2 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. An application would need to demonstrate that covert activities are considered proportionate and demonstrate that other/overt methods have been considered or attempted and failed.

18. Urgent Cases

18.1 As from 1 November 2012 there is no provision for urgent oral authorisations under RIPA as all authorisations have to be approved by a J.P. If surveillance was required to be carried out in an urgent situation or as an immediate response, this would still have to be justified as necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA.

18.2 It is recognised that council officers find themselves in situations where they need to carry out some form of surveillance without the time to complete a form and obtain authorisations (see also paragraph 24). In these instances, the officer should obtain authorisation from their line manager and also record their reasons, actions, what was observed and be prepared to explain their decisions. These should be reported to the appropriate Senior Responsible Officer.

19. Surveillance for Preventing Disorder

19.1 Authorisation for the purpose of preventing disorder can only be granted if it involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Surveillance for disorder not meeting these criteria would need to be carried out as surveillance outside of RIPA. (See below)

20. CCTV

20.1 CCTV is now known as a Surveillance Camera Systems (Section 29(6) Protection of Freedoms Act 2012). The Surveillance Camera Code of Practice 2013 defines a 'surveillance camera system' as:

- any other systems for recording or viewing visual images for surveillance purposes;
- any systems for storing, receiving, transmitting, processing or checking the images or information obtained.

20.2 "Surveillance Camera Systems" is taken to include:

- closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;
- any other systems for recording or viewing visual images for surveillance purposes;

This definition will include body worn video (BWV) and overt cameras deployed to detect waste offences such as fly-tipping. This definition has far reaching implications as the use of any cameras that meet the requirement will have to be used in a manner that complies with the codes of practice mentioned above and the Data Protection Act.

This includes

- CCTV;
- Body Worn Video (BWV)
- Automatic Number Plate Recognition;
- Deployable mobile overt mobile camera systems.
- Any other system for recording or viewing visual images for surveillance purposes;
- Any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- Any other systems associated with, or otherwise connected with those systems.

20.2 The use of the conventional town centre CCTV systems operated by the Council do not normally fall under the RIPA regulations. However, it does fall under the UK General Data Protection Regulation, Data Protection Act 2018, the Surveillance Camera Code 2013, Information Commissioner's Office (ICO) 'In the picture: a data protection code of practice for surveillance cameras and personal information' and the Council's CCTV policy which is available via the following link: CCTV - Fenland District Council. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

20.3 Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

20.4 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, the Fenland District Council CCTV Policy should be followed where relevant as well as the RIPA Codes of Practice.

20.5 The CCTV staff are to have a copy of the authorisation form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority from the Police, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the central register for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

21. Automatic Number Plate Recognition (ANPR)

21.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle by plotting its locations, e.g. in connection with illegally depositing waste (fly-tipping).

21.2 Should it be necessary to use any ANPR systems to monitor vehicles, the same RIPA principles apply where a Directed Surveillance Authorisation should be sought.

22 Internet and Social Media Investigations

22.1 The use of the internet and social media such as Facebook, Instagram and Twitter in an investigation is permitted and may be a means of gathering intelligence. In accessing such sites, officers must consider the issues of privacy and collateral intrusion. The Covert Human Intelligence Source revised code of practice sections 4.29 to 4.35 provides good guidance on the subject. Even though a person may have placed information about themselves or others in the public arena, they have done so with an expectation of a degree of privacy. Viewing information on the internet may constitute covert surveillance, particularly if there is monitoring of subjects involved for example to establish patterns of behavior. Where information about an individual is placed on a publicly accessible database such as Companies House, then they are unlikely to have expectations of privacy.

22.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

22.3 If an investigating officer enters into a 'conversation' with a profile, and the officer informs them that he is contacting them in his role as an employee of the council, then this contact will be overt and no authorisation will be required.

22.4 Where the activity does not include monitoring of material in the public domain, RIPA will not apply. If repeated visits to a site are made then this will constitute monitoring and consideration needs to be given to the use of social media or the internet as part of that investigation.

22.5 If an investigating officer views for example a Facebook profile with whom they are not 'friends' which is not protected by any privacy settings the information can be treated as being in the public domain. Any initial viewing/visiting of this profile will be overt and authorisation under RIPA will not be required.

22.6 If the officer frequently or regularly views the same individual's profile this is considered targeted surveillance and a RIPA authorisation may be required should it meet the stated RIPA criteria in this policy. If it does not then the officer should be able to show that they have considered whether RIPA applied.

22.7 Activities of monitoring through, for example, a Facebook profile for a period of time and a record of the information is kept for later analysis or evidential purposes is likely to require a RIPA authorisation. Where covert contact is made with another person on the internet a CHIS authority may be required.

22.8 Where officers are building and maintaining a relationship with an individual without that individual knowing the true nature for the purposes of an investigation, this may require an application for the use of a CHIS. Guidance is provided in Part C.

22.9 If officers create a false or covert identity, this must only be created with the approval of an Authorising Officer and the RIPA Coordinator must be informed. All use of the identity must be logged and reported to the RIPA Coordinator.

22.10 Any use of the internet in an investigation must be fully documented – see Appendix 4 and authorised by the relevant Head of Service with overall responsibility for the investigation. The investigating officer then must provide regular updates to the line manager as to the need for continued use of the internet for the stated purpose and, once its use has been discontinued.

22.11 The following from the Code of Practice is a guide of factors to consider:

- Whether the investigation or research is directed towards an individual or organisation
- Whether it is likely to result in obtaining private information about a person or group of people

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

Any similar activity carried out on the Councils' behalf by a third party then this may still require a directed surveillance authorisation.

22.12 Misuse of council devices or misuse of social media may be considered in line with the relevant disciplinary policy. Any usage should be considered in line with the Councils' ICT Acceptable Use Policy and Social Media Guidance.

22.12 The council have the capability to "audit" the use of social media sites by individual user's profile in line with the appropriate IT policies. The council will undertake such an audit in the event of a complaint or concern that social media has been misused or accessed during an investigation where RIPA may apply and has not been appropriately applied for. The concern will be raised with the RIPA Coordinator and Data Protection Officer who will advise on the appropriate procedure.

22.12 The council may also undertake spot check audits and investigators or staff will be required to detail the reason for access.

23. Surveillance Outside of RIPA

23.1 For Directed Surveillance the criminal offence must carry **a 6-month prison sentence** (Directed Surveillance crime threshold) or relate to the sale of alcohol or tobacco to children. This means that there are scenarios within an investigation that do not meet this threshold, however it is necessary to undertake surveillance. This will fall outside of RIPA. Examples include:

- Surveillance for anti-social behaviour disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.
- Most licensing breaches.
- Safeguarding vulnerable people.
- Civil matters.

23.2 In the above scenarios they are likely to be a targeted surveillance which are likely to breach someone's Article 8 rights to privacy. Therefore, the activity should be

conducted in way which is HRA compliant, which will include necessary and proportionate. Officers should be able to demonstrate how they have considered this.

24 Disciplinary Investigations

24.1 Non RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Guidance dictates that this type of surveillance must be compliant with the Monitoring at Work Guidance issued by the Information Commissioner. This is to ensure that is complies with the HRA.

24.2 Should the investigation also involve a criminal offence which meets the RIPA criteria such as fraud, the option to carry out the surveillance under RIPA should be considered. However, it must be a genuine criminal investigation with a view to prosecuting the offender.

24.3 Should it be necessary to undertake disciplinary surveillance advice should be sought from the Head of HR/OD and/or the Assistant Director – Legal and Governance.

24.4 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations as per section 3.33 in the codes of practice that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation.
- Use of overt CCTV and Automatic Number Plate Recognition systems.
- Surveillance where no private information is likely to be obtained.
- Surveillance undertaken as an immediate response to a situation.
- Covert surveillance not relating to criminal offence which carries a maximum sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children (surveillance outside of RIPA).
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

24.5 As part of the process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by an Authorising Officer. (It has always been recommended that it should still be an AO. This will also improve their authorisation skills.) A copy of the non RIPA surveillance application form can be obtained from the RIPA Coordinator or Authorising Officer.

24.6 The SRO will therefore maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The RIPA Co Ordinator will maintain a central record of non RIPA surveillance.

25. Joint Agency Surveillance

25.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

25.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Co-Ordinator. This will assist with oversight of the use of Council staff carrying out these types of operations. Line Managers should be made aware if their staff are involved in this type of surveillance.

26. Use of Third-Party Surveillance

26.1 In some circumstances it may be appropriate or necessary for Fenland District Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of Directed Surveillance should be authorised. This is because the agent will be subject to RIPA in the same way as any employee of the Council would be. The Authorising Officer should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact the Senior Responsible Officer, RIPA Co-ordinator or Authorising Officer.

26.2 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a Public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation.

27. Surveillance Equipment

27.1 The Council will maintain a central register of all surveillance equipment such as cameras and noise monitoring devices. This will require a description, Serial Number, an explanation of its capabilities.

27.2 The register will be held and maintained by the RIPA Co-Ordinator. This equipment is available for all departments to use.

27.3 All equipment capable of being used for Directed Surveillance such as cameras etc. should be fit for purpose for which they are intended.

27.4 When completing an Authorisation, the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues, proportionality and whether the equipment is fit for the required purpose. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

PART C. Covert Human Intelligence Sources (CHIS)

28. Introduction

28.1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information.

28.2 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship. However, Officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with the Criminal Procedures and Investigations Act (CPIA) and the disclosure provisions.

28.3 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of this Policy and the CHIS codes of Practice.

28.4 Before use of a CHIS is authorised, advice must be sought from the Senior Responsible Officer or their appointed deputy. The application can be authorised by the Chief Executive (or an appointed deputy) and the applicant must ensure that the Authorising Officer has sufficient information to make an informed decision and the prescribed forms must be fully completed.

29. Definition of CHIS

29.1 Paragraph 2.1 of Covert Human Intelligence Source revised code of practice state that a person is a Covert Human Intelligence Source if the Council:

i) establish or maintain a covert relationship with another person to obtain information.

ii) covertly give access to information to another person, or

iii) disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists.

29.2 A relationship is established, maintained or used for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. This does not mean the relationship with the Council Officer and the person providing the information, as this is not covert. It relates to how the information was either obtained or will be obtained. Was it or will it be obtained from a third party without them knowing it was being passed on to the Council? This would amount to a covert relationship.

29.3 It is possible, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice

29.4 The following give examples of when a CHIS would and would not be needed.

Would not need a CHIS authorisation	**Would need a CHIS authorisation**
Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.	In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.
Would not need a CHIS authorisation	**Would need a CHIS authorisation**
A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.	A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

Would not need a CHIS authorisation	Would need a CHIS authorisation
A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual	Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague

30. Vulnerable and Juvenile CHIS

30.1 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Corporate Director – Monitoring Officer).

30.2 In line with, Paragraph 4.1 of the Covert Human Intelligence Source revised code of practice, the Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source. The Investigatory Powers Commissioner intends to keep such authorisations under close review and will report any relevant findings in his Annual Report. The Authorising Officer must therefore ensure that the SIRO/RIPA Coordinator are informed urgently should such an authorisation be made so that appropriate arrangements can be put in place.

30.2 Paragraph 4.3 of the CHIS Code of Practice refers to the use of juveniles in either scenario and how special safeguards also apply to the use or conduct of juveniles. The use of such a person could occur during test purchasing operations. The Code of Practice gives clear guidance:

- On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.

- In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.
- Authorisations for use of a juvenile as a CHIS should be granted by the Head of Paid Service i.e. the Chief Executive.
- The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review.
- For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

30.3 We must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the statutory instrument, and the rationale recorded in writing.

31. Lawful Criteria

31.1 The lawful criteria for CHIS authorisation is **prevention and detection of crime and prevention of disorder.** The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.

31.2 Authorisations for Juvenile Sources must be authorised by the Chief Executive of the Council (or, in their absence, the Corporate Director – Monitoring Officer).

32. Conduct and Use of a Source

32.1 The way the Council use a CHIS for covert activities is known as ‘the use and conduct’ of a source.

32.2 The use of a CHIS involves any action on behalf of a Public Authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

32.3 The conduct of a CHIS is establishing or maintaining a personal or other relationship with another person for the covert purpose of:

a. Using such a relationship to obtain information, or to provide access to information to another person, or

b. Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship or

c. Is incidental to anything falling within a and b above.

32.4 In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a Public Authority.

32.5 The use of a source is what the Authority does in connection with the source, such as tasking (see section 33), and the conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The Use and Conduct require separate consideration before authorisation. However, they are normally authorised within the same authorisation.

32.6 The same authorisation form is utilised for both use and conduct. A Handler and Controller must also be designated, as part of the authorisation process (see Part E and section 42), and the application can only be authorised if necessary and proportionate. Detailed records of the use, conduct and tasking of the source also have to be maintained (see section 37).

32.7 Care should be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed. (Section 210 CHIS Codes of Practice)

32.8 Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. (Section 3.18 CHIS Codes of Practice)

33. Handler and Controller

33.1 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

- That there will at all times be an officer (the **Handler**) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The Handler is likely to be the investigating officer.
- That there will at all times be another officer within the Council who will have general oversight of the use made of the source; **(Controller)** i.e. the line manager.
- That there will at all times be an officer within the Council who has responsibility for maintaining a record of the use made of the source. See CHIS record keeping (see Section 37)

33.2 The **Handler** will have day to day responsibility for:

- Dealing with the source on behalf of the Local Authority concerned;
- Risk assessments
- Directing the day to day activities of the source;
- Recording the information supplied by the source;
- Monitoring the source's security and welfare; and
- Informing the Controller of concerns about the personal circumstances of the CHIS that might effect the validity of the risk assessment or conduct of the CHIS.

33.3 The **Controller** will be responsible for:

- The management and supervision of the "Handler" and
- General oversight of the use of the CHIS;
- maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

34. Undercover Officers

34.1 Oversight and management arrangements for **undercover operatives**, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of the Council. The role of the handler will be undertaken by a person referred to as a **'cover officer'**. (Section 6.9 CHIS Codes of Practice).

35. Tasking

35.1 Tasking is the assignment given to the source by the Handler or Controller such as by asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant Local Authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

35.2 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, Directed Surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

35.3 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

36. Risk Assessments, Security and Welfare

36.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. It is a requirement of the codes that a risk assessment is carried out. This should be submitted with the authorisation request. The risk assessment should provide details of how the CHIS is going to be handled It should also take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

36.2 When considering deploying a CHIS, we should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking.

Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained.

36.3 The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS.

36.4 Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example this could be by means of disclosure to a court or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 9.26 to 9.29 of the of the Covert Human Intelligence Source revised code of practice.

36.5 The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

36.6 Appendix 3 provides a risk assessment form for an operation.

37. Use of Equipment by a CHIS

37.1 If a CHIS is required to wear or carrying a surveillance device such as a covert camera it does not need a separate intrusive or Directed Surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

37.2 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations. This should have been identified at the planning stage.

38. CHIS Management

38.1 The operation will require managing by the Handler and Controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The Authorising Officer should maintain general oversight of these functions.

38.2 During CHIS activity, there may be occasions when unforeseen actions or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorised (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

39 Operation Involving Multiple CHIS

39.1 A single authorisation may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several individual operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the interference with private or family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer. If an authorisation includes more than one relevant source, each relevant source must be clearly identifiable within the documentation. In these circumstances, adequate records must be kept of the length of deployment of a relevant source to ensure the enhanced authorisation process set out in the 2013 Relevant Sources Order and Annex B of the Code of Practice can be adhered to.

40 Social Media considerations

40.1 Considering a Covert Human Intelligence Source (CHIS) authorisation in social media/internet investigations

Any council officer or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation.

A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

40.2 Tasking someone to use a profile for covert reasons

Where someone, such as an employee or member of the public, is tasked by the council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

Example of when CHIS authorisation is needed
An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person. • Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose. • Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

40.3 Registering to Access a Site

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where an officer sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example of when CHIS authorisation is not needed	**Example of when CHIS authorisation is needed**
A Trading Standards officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that counterfeit goods are being sold. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.	A Trading Standards officer tasks a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

40.4 Use of Likes and Follows

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for a council officer or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example of when CHIS authorisation is not needed	Example of when CHIS authorisation is needed
An officer maintains a false persona, unconnected to law enforcement activities, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity they "follow" a variety of people and entities and "likes" occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.	The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

40.4 The identity Being Used

When engaging in conduct as a CHIS, a council officer should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

40.5 Risk Assessment

Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 7.16 of the Covert Human Intelligence Source revised code of practice should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

41. CHIS Record Keeping

41.1 Centrally Retrievable Record of Authorisations

41.1.1 A centrally retrievable record of all authorisations is held by Fenland District Council. This record contains the relevant information to comply with the Codes of Practice. These records are updated whenever an authorisation is granted, renewed or cancelled and are available to the Investigatory Powers Commissioner (IPCO) upon request.

41.1.2 The records are retained for 3years from the ending of the authorisation.

41.2 Individual Source Records of Authorisation and Use of CHIS

41.2.1 Detailed records must be kept of the authorisation and the use made of a CHIS. An authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

41.2.2 The particulars to be contained within the records are;

a. The identity of the source;
b. The identity, where known, used by the source;
c. Any relevant investigating authority other than the authority maintaining the records;
d. The means by which the source is referred to within each relevant investigating authority;
e. Any other significant information connected with the security and welfare of the source;
f. Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g. The date when, and the circumstances in which the source was recruited;
h. Identity of the Handler and Controller (and details of any changes)
i. The periods during which those persons have discharged those responsibilities;
j. The tasks given to the source and the demands made of him in relation to his activities as a source;
k. All contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l. The information obtained by each relevant investigating authority by the conduct or use of the source;
m. Any dissemination by that authority of information obtained in that way; and
n. In the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

41.2.3 The person maintaining these records is the RIPA Co-ordinator.

41.2.4 Public authorities are also encouraged to maintain auditable records for individuals providing intelligence who do not meet the definition of a CHIS. This will assist authorities to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain why authorisation is not considered necessary. Such decisions should rest with those designated as Authorising Officers within Public Authorities. (Section 7.5 CHIS Codes of Practice).

41.3. Further Documentation

41.3.1 In addition to the above, when appropriate records or copies of the following, as are retained by Fenland District Council for 3 years:

- A copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- The reason why the person renewing an authorisation considered it necessary to do so;
- Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- Any risk assessment made in relation to the operation or CHIS;
- The circumstances in which tasks were given to the CHIS;
- The value of the CHIS to the investigating authority;
- A record of the results of any reviews of the authorisation;
- The reasons, if any, for not renewing an authorisation;
- The reasons for cancelling an authorisation; and
- The date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.
- A copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

41.1.2 The records kept by the Council should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS. (Sec 7.7 CHIS Codes of Practice)

41.1.3 The forms are available in the Appendices: Current link to the Home office Forms is https://www.gov.uk/government/collections/ripa-forms--2

- Application for the conduct or use of Covert Human Intelligence Source (CHIS)
- Review of a Covert Human Intelligence Source (CHIS) operation
- Application for renewal of a Covert Human Intelligence Source (CHIS) operation
- Cancellation of an authorisation for a Covert Human Intelligence Source (CHIS) operation

References in these forms to the 'Code' are to the Covert Human Intelligence Sources Code of Practice, which should be consulted for further guidance.

PART D. RIPA Roles and Responsibilities

42. The Senior Responsible Officer (SIRO)

42.1 The nominated Senior Responsible Officer is Carol Pilson Corporate Director – Monitoring Officer. The SIRO with responsibilities for:

- The integrity of the process in place within Fenland District Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and
- Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

43. RIPA Co-Ordinator

43.1 The RIPA Co-Ordinator Amy Brown – Assistant Director – Legal and Governance is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the Authorising Officer or refused by a JP.

43.2 The RIPA Co-ordinator will: -

- Keep the copies of the forms for a period of at least 3 years
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and Issue the unique reference number.
- Keep a database for identifying and monitoring expiry dates and renewal dates.
- Along with, Directors, Service Managers, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 2018. (DPA)
- Provide administrative support and guidance on the processes involved.
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Ensure adequate training is provided including guidance and awareness of RIPA and the provisions of this Policy; and Review the contents of this Policy.

44. Managers Responsibility and Management of the Activity

44.1 Line Managers within each area of the Council are responsible for ensuring that in all cases where surveillance is required, due consideration is given to the need for covert surveillance before an application is made for authorisation. That includes the consideration of using overt action, routine enquiries or inspections which are less intrusive.

44.2 If authorised it is important that all those involved in undertaking Directed Surveillance activities, including Line managers, are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment for the need for the activity to continue including ongoing assessments of the intrusion. All material obtained, including evidence, should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence (Section 61)

44.3 Line Managers should also ensure that the relevant reviews (see section 53), renewals (see section 54) and cancellations (see section 55) are completed by the applicant in accordant with the codes and the dates set throughout the process.

451. Investigating Officers/Applicant

45.1 The applicant is normally an investigating officer who completes the application section of the RIPA form. Investigating Officers should think about the need to undertake Directed Surveillance or the use of a CHIS before they seek authorisation and discuss it with their Line manager. Investigating Officers need to consider whether they can obtain the information or achieve their objective by using techniques other than covert surveillance.

45.2 The applicant or some other person must carry out a feasibility study as this should be seen by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.

45.3 The applicant is likely to attend court to seek the approval of a JP. and if approved and involved in the covert activity they must only carry out what is authorised and approved. They, or some other person will also be responsible for the submission of any reviews (see section 53) renewals (see section 54) and cancellations (see section 55).

46. Authorising Officers

46.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

46.2 Appendix A lists the Authorising Officers within the Council who can grant authorisations all of which are Director or Head of Service level Officers.

46.3 The role of the Authorising Officers is to consider whether to authorise, review, or renew an authorisation. They must also officially cancel the RIPA covert activity. Authorising Officers must have been trained to an appropriate level so as to have an understanding of the requirements in the Codes of Practice and that must be satisfied before an authorisation can be granted.

46.4 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation, the central record of authorisations should highlight this, and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

46.5 Authorisations must be given in writing by the Authorising Officer by completing the relevant section on the authorisation form. When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

46.6 Authorising Officers must explain why they believe the activity is both necessary (see section 43) and proportionate (see section 44), having regard to the collateral intrusion. They must also consider any similar activity which may be taking place, or sensitivities in the area.

46.7 They also need to explain exactly what they are authorising, against who, in what circumstances, where etc. and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is made clear on the authorisation as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors.

46.8 If any equipment such as covert cameras are to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

46.9 The Authorising Officer may be required to attend court to explain what has been authorised and why.

46.10 Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that Authorising Officers hold their own copy of this document. This can be obtained from The RIPA Coordinator.

47 Necessity

47.1 Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

47.2 The Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds which for Local Authority Directed Surveillance is the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.

47.3 The lawful criteria for CHIS is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment.

47.4 The applicant and Authorising Officers must also be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there were no other means of obtaining the same information in a less intrusive method. This is a part of the authorisation form.

48. Proportionality

48.1 If the activities are deemed necessary, the Authorising Officer must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

48.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

48.3 When explaining proportionality, the Authorising Officer should explain why the methods and tactics to be adopted during the surveillance is not disproportionate.

48.4 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

49. Collateral Intrusion

49.1 Before authorising applications for Directed Surveillance, the Authorising Officer should also take into account the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance.

49.2 Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

45.3 All applications must therefore include an assessment of the risk of collateral intrusion and detail the measures taken to limit this to enable the Authorising Officer fully to consider the proportionality of the proposed actions. This is detailed in a section within the authorisation form (Contained within the following link) https://www.gov.uk/government/collections/ripa-forms--2

49.4 In order to give proper consideration to collateral intrusion, an Authorising Officer should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the Authorising Officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. It may also need retaining under CPIA. The Authorising Officer should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.

49.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.

49.6 In the event that authorised surveillance unexpectedly and unintentionally interferes with the privacy of any individual other than the intended subject, the authorising officer should be informed by submitting a review form. Consideration should be given in any such case to the need for any separate or additional authorisation.

49.7 Where a Public Authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

50 Other Factors

50.1 Spiritual Counselling

No operations should be taken in circumstances where investigators believe that surveillance will lead to them intruding on spiritual counselling between a Minister and a Member of his/her faith. In this respect, spiritual counselling is defined as conversations with Minister of Religion acting in his-her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

50.2 Community Sensitivities

Officers should always consider whether there are any particular sensitivities within our communities and take these into account if planning surveillance activities in those areas.

PART E. The Application and Authorisation Process

51. Relevant Forms

51.1 For both Directed Surveillance and CHIS authorisations there are 4 forms within the process. They are:

- Authorisation
- Review
- Renewal
- Cancellation

51.2 All the forms can be obtained from the Government Website at

https://www.gov.uk/government/collections/ripa-forms--2

52. Duration of Authorisations

52.1 Authorisations must be given for the maximum duration from the Date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a Directed Surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. Durations detailed below:

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	4 Months
Renewal	4 Months

52.2 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

52.3 In paragraph 4.17 of the Covert Surveillance and Property Interference Code of Practice, its is confirmed that a single authorisation may combine two or more different authorisations under RIPA however the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer. It does not preclude the obtaining of separate authorisations.

53. Applications/Authorisation

53.1 The applicant or some other person must carry out a feasibility study and intrusion assessment as this may be required by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.

53.2 When completing an application for authorisation, the applicant must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. This is a requirement of the codes.

53.3 All the relevant sections must be completed with sufficient information to ensure that applications are sufficiently detailed for the Authorising Officer to consider Necessity, Proportionality having taken into account the Collateral Intrusion issues **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

53.4 If it is intended to undertake both Directed Surveillance and the use of a CHIS on the same surveillance subject, the respective authorisation should be completed and the respective procedures followed. Both activities should be considered separately on their own merits.

53.5 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation. The form should then be submitted to the Authorising Officer.

53.6 Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Co-Ordinator) by the line manager. The number will be taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

53.7 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Co-Ordinator for recording and filing. If having received the feedback, the applicant feels it is appropriate to re submit the application, they can do so and it will then be considered again.53.8 Following authorisation, the applicant will then complete the relevant section of the judicial application/order form (Contained within the following link) https://www.gov.uk/government/collections/ripa-forms--2

Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to supply a copy and the original RIPA authorisation as well.

54. Arranging the Court Hearing

54.1 It will be necessary within office hours to contact the administration at the Magistrates' Court to arrange a hearing. The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

54.2 Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the Legal Services Team.

55. Attending the Hearing

55.1 The applicant in addition to the Authorising Officer will attend the hearing. Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, the original and a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case. The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

55.2 The JP will read and consider the RIPA authorisation and the judicial application/order form (contained within the following link) https://www.gov.uk/government/collections/ripa-forms--2

They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However, the forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided**.

55.3 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation was an appropriate Designated Person within the Council to authorise the activity and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for Directed Surveillance.

56. Decision of the Justice of the Peace (JP)

56.1 The JP has a number of options which are:

56.2 **Approve or renew an authorisation.** If approved by the JP, the date of the approval becomes the commencement date for the duration of the three months and the officers are now allowed to undertake the activity.

56.3 **Refuse to approve or renew an authorisation.** The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

56.4 Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal, the officer should consider whether they can reapply. For example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

56.5 For, a technical error (as defined by the JP), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

56.6 **Refuse to approve or renew and quash the authorisation.** This applies where the JP refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case, the officer will inform the Legal who will consider whether to make any representations.

56.7 The JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

56.8 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Services Team will decide what action if any should be taken.

56.9 There is a Home Office chart showing the above procedure at Appendix B.

57. Post Court Procedure

57.1 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the Authorising Officer is aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Co-Ordinator. A copy will be retained by the applicant and if necessary by the Authorising Officer. The central register will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

57.2 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice and reduce the risk of errors.

58. Reviews

58.1 When an application has been authorised and approved by a JP, regular reviews must be undertaken by the Authorising Officer to assess the need for the surveillance to continue.

58.2 In each case the Authorising Officer should determine how often a review should take place at the outset. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or confidential information. They will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required to ensure that the applicants submit the review form on time.

58.3 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application which would include a change to the level of intrusion so that the need to continue the activity can be re-assessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new application form should be submitted, and it will be necessary to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

58.4 Line mangers of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

58.5 The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.

58.6 The results of a review should be recorded on the central record of authorisations.

59. Renewal

59.1 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but Directed Surveillance or the use of a CHIS is still required.

59.2 Authorisation should not be allowed to lapse. They should be reviewed and cancelled or renewed.

59.2 Should it be necessary to renew an authorisation for Directed Surveillance or CHIS, this must be approved by a JP.

59.3 Applications for renewals should not be made until shortly before the original authorisation period is due to expire. However, they must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

59.4 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer for consideration.

59.5 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

59.6 If the Authorising Officer refuses to renew the application, the cancellation process should be completed. If the Authorising Officer authorises the renewal of the activity, the same process is to be followed as mentioned earlier for the initial application whereby approval must be sought from a JP.

59.7 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

60. Cancellation

60.1 The cancellation form (contained in the following link) https://www.gov.uk/government/collections/ripa-forms--2 is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the Directed Surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

60.2 As soon as the decision is taken that Directed Surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations**.**

60.3 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and detail if any images were obtained, particularly any images containing innocent third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc. See sections 58 to 65 Safeguarding and the Use of Surveillance Material below.

60.4 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what was authorised. This check will form part of the oversight function. Where issues are identified including errors (see Part G) they will be brought to the attention of the Line Manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight and comply with the Codes of Practice.

60.5 When cancelling a CHIS authorisation, an assessment of the welfare and safety of the source should also be assessed and any issues identified.

60.6 All cancellations must be submitted to the RIPA Co-Ordinator for inclusion in the central Record and storing securely with the other associated forms.

60.7 Do not wait until the 3 month period is up to cancel. Cancel it at the earliest opportunity when no longer necessary and proportionate. Line Managers should be aware of when the activity needs cancelling and ensure that staff comply with the procedure.

Part F Acquisition of Communications Data

61. Introduction

Communications data means any traffic or any information that is or has been sent via a telecommunications system or postal system, together with information about the use of the system made by any person.

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Companies").

S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a Communications Service Provider is technically unable to collect the data, an authorisation under the section would permit the local authority to collect the communications data themselves.

In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA must be issued.

The sole ground to permit the issuing of a S22 notice by a Permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.

There is no threshold for subscriber data which can still be acquired for any crime where it is necessary and proportionate to do so. However as of 1 November 2018, there is a crime threshold for the acquisition of service or traffic data which is restricted to "serious crime". This is defined as:

- An offence capable of attracting a prison sentence of 12 months or more. This can checked by accessing the Home Office counting rules notifiable offence list.
- An offence by a person who is not an individual i.e. a corporate body
- A Section 81 of RIPA – an offence defined as serious crime such as use of violence, substantial financial gain or large number of people in pursuit of a common purpose
- An offence which integrally involves the sending of a communication
- Breach of privacy offence

Examples of what are non-serious crimes are:

- Certain immigration offences under the Immigration Act 1971; and
- Certain gambling offences under the Gambling Act 2005 including provision of facilities for gambling, use of premises for gambling and offences relating to gambling machines.
- Some sections of the Public Order Act which do not amount to violence (including using offensive words or causing a fear of violence);

- Driving offences, such as: joy riding, driving when disqualified, failure to stop or report an accident and driving when unfit to do so through drink or drugs;
- Some sections of the Consumer Protection Act 1987 i.e. furnishing false information in response to notice, or to enforcement officer.

62. Application procedure

62.1 At present, the only route to obtain this type of information is through the National Anti-Fraud Network (NAFN). Fenland District Council is not currently a member of NAFN and as such cannot make an enquiry.

62.2 It should be noted that the council's provider of fraud investigation services, Anglia Revenue Partnership (ARP), is a member of NAFN and may make requests in relation to matters relating to Fenland District Council. In these instances, ARP should ensure that they inform the council of the request made and this be recorded by the RIPA Co-ordinator.

Part G Central Record and Safeguarding the Material

62. Introduction

62.1 Authorising Officers, applicants and Line Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. This includes the legal obligations under the Criminal Procedures and Investigations Act. However, this will not replace the requirements under the Codes of Practice, which includes the fact that the Council must hold a centrally held and retrievable record.

62.2 Applicants, Authorising Officers, SIRO and the RIPA Coordinator must comply with the requirements set out in this Part of the Policy and the Guidance at Appendix 5.

63. Central Record

63.1 The centrally retrievable record of all authorisations will be held and maintained by Amy Brown - RIPA Co-Ordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.

63.2 All original authorisations and copies of Judicial applications/order forms whether authorised or refused, together with review, renewal and cancellation documents, must be sent within 48 hours to Amy Brown – RIPA Co-Ordinator who will be responsible for maintaining the central record of authorisations. They will ensure that all records are held securely with no unauthorised access. If in paper format, they must be forwarded in a sealed envelope marked confidential.

63.3 The documents contained in the centrally held register should be retained for 3 years. The centrally held register contains the following information:

- If refused, (the application was not authorised by the AO) a brief explanation of the reason why. The refused application should be retained as part of the central record of authorisation;
- If granted, the type of authorisation and the date the authorisation was given;
- Details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- Name and rank/grade of the authorising officer;
- The unique reference number (URN) of the investigation or operation;
- The title of the investigation or operation, including a brief description and names of subjects, if known;
- Frequency and the result of each review of the authorisation;
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date renewed by the JP;

- Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- The date the authorisation was cancelled;
- Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

63.4 As well as the central record the RIPA Co-Ordinator will also retain:

- The original of each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the Authorising Officer;
- The frequency and result of reviews prescribed by the Authorising Officer;
- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the Authorising Officer;
- A record of the period over which the surveillance has taken place. This should have been included within the cancellation form.

63.5 These documents will also be retained for five years from the ending of the authorisation.

64. Safeguarding and the Use of Surveillance Material

64.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through Directed Surveillance or CHIS activity. This material may include private, confidential or legal privilege information. It will also show the link to other relevant legislation.

64.2 The Council should ensure that their actions when handling information obtained by means of covert surveillance or CHIS activity comply with relevant legal frameworks and the Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including Data Protection requirements, will ensure that the handling of private information obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. The material will also be subject to the Criminal Procedures Investigations Act (CPIA)

65. Authorised Purpose

65.1 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the RIPA codes, something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA Act in relation to covert surveillance or CHIS activity;

- Is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

66. Handling and Retention of Material

66.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the UK General Data Protection Regulation, Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the councils' policies and procedures currently in force relating to document retention. The Council's Document Retention Policy sets out the expected requirements.

66.2 All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained, together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

66.2 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

66.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

66.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

66.5 If an appeal against conviction is in progress when released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

66.6 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with legal disclosure requirements. All such material should be clearly labelled and stored in such a way to enable compliance with data retention and disposal.

66.6 If retention is beyond these periods it must be justified under DPA. Each relevant service within the Council may have its own provisions under their Data Retention Policy which will also need to be consulted to ensure that the data is retained lawfully and for as long as is necessary.

66.7 Any material obtained must be stored securely, either electronically or physically, and access only provided to those who have the appropriate clearance for access. Physical information must be protected by an adequate level of security such as locked rooms or a safe with a log of access kept.

66.8 Information will be destroyed securely in line with retention requirements and its retention will be reviewed accordingly.

67. Use of Material as Evidence

67.1 Material obtained through Directed Surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1996 and the Human Rights Act 1998.

67.2 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council will be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

67.3 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the Prosecuting Solicitor. They in turn will decide what is disclosed to the Defence Solicitors.

67.4 There is nothing in RIPA which prevents material obtained under Directed Surveillance authorisations from being used to further other investigations.

68. Dissemination of Information

68.1 Material obtained should only be shared with individuals within the authority and external partners where this is permitted by legislation, an information sharing agreement or a requirement to disclose. For example, a joint investigation with the Police would require information to be shared as part of that investigation and permitted by data protection legislation.

68.2 The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out in sec 59 above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

68.3 The obligations apply not just to Fenland District Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from Fenland District Council before disclosing the material further. It is important that the Officer In Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

68.4 A record will be maintained justifying any dissemination of material. If in doubt, seek advice.

69. Storage

69.1 Material obtained through covert surveillance and CHIS authorisations, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. It will be necessary to ensure that both physical and IT security and an appropriate security clearance regime is in place to safeguard the material.

70. Copying

70.1 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

70.2 In the course of an investigation, Fenland District Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

71. Destruction

71.1 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Part H. Errors and Complaints

72. Errors

72.1 Errors can have very significant consequences on an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA codes and this Policy should reduce the scope for making errors.

72.2. There are two types of errors within the codes of practice which are:

- Relevant error and
- Serious error.

73 Relevant Error

73.1 An error must be reported if it is a "**relevant error**". A relevant error is any error by a Public Authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA). This would include with the content of the Codes of Practice.

73.2 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

73.3 All relevant errors made by Public Authorities must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

74. Serious Errors

74.1 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

74.2 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

75. Complaints

75.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Borough Solicitor who will investigate the complaint. A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). They have jurisdiction to investigate and determine complaints against any Public Authority's use of RIPA powers, including those covered by this Policy.

75.2 Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

PART I Relevant case law

76. There is relevant caselaw which includes but is not limited to:

76.1 R v Johnson

In this case the Court of Appeal provided criteria that must be adopted if premises used for observation purposes by the Police are not to be disclosed in open court.

Should FDC wish not to disclose the premises used for the observation, then following the rational in this case it would appear that the Authorising Officer must be able to testify that immediately prior to trial:

- he/she visited premises to be used for observation;
- he/she obtained and recorded the views of the owner and/or occupier in respect; of the use made of the premises and the possible consequences of disclosure; which could lead to identification of the premises and occupiers.

Such views must be recorded and the record marked as sensitive. If this issue arises please contact the Senior Responsible Officer for appropriate advice.

76.2 R v Sutherland 2002

The recording and handling of confidential material (legal privilege) obtained as a result of recording equipment deployed in the exercise area of two police stations. In this matter, the activity exceeded that which had been authorised and the case against Sutherland collapsed. This emphasises the requirement to ensure that all activity is authorised prior to the operation and any errors are reported.

76.3 Peck v United Kingdom [2003]

The applicant was filmed by a CCTV camera operated by Brentwood Borough Council in a public street shortly after he had attempted to commit suicide. The council subsequently released two still photographs taken from the CCTV footage to show the benefits of CCTV. Peck's face was not specifically masked. These pictures subsequently appeared on regional television but his face was masked. Peck sought to challenge the authority's decision but was rejected by the Court of Appeal. He took the matter to the European Court of Human Rights where he was successful. The case establishes the right to privacy in a public area, even if it is a reduced level.

76.4 Martin v. United Kingdom [2004] European Court App

Alleged disorderly behaviour by M towards neighbour. Local Authority mounted covert surveillance of M on the basis that the surveillance by video was justified as the surveillance was targeted at behaviour which was visible to a neighbour or passer by. Claim of Article 8 infringement settled by agreement with damages awarded to Martin.

76.5 R v. Button and Tannahill 2005

Audio and video recording of defendants while in police custody. Audio recording had been RIPA authorised; video recording was not authorised. Video record admitted in evidence although common ground that it had been unauthorised and so obtained unlawfully (in breach of s.6 Human Rights Act 1998). *It was a*rgued on appeal that the trial Court was itself in breach of s.6 by admitting the evidence. Held that the breach of article 8 related to the intrusion upon private life involved in the covert surveillance. So far as a trial Court is concerned: any such breach of article 8 is subsumed by the article 6 (and P.A.C.E.) duty to ensure a fair trial. The trial judge had not acted unlawfully by admitting the evidence.

76.6 C v The Police and the Secretary of State for the Home Department (2006, No: IPT/03/32/H)

A former police sergeant (C), having retired in 2001, made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an enhanced pension due to the injuries. In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming that they had carried out Directed Surveillance under RIPA without an authorisation. The Tribunal ruled that this was not the type of surveillance that RIPA was enacted to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers

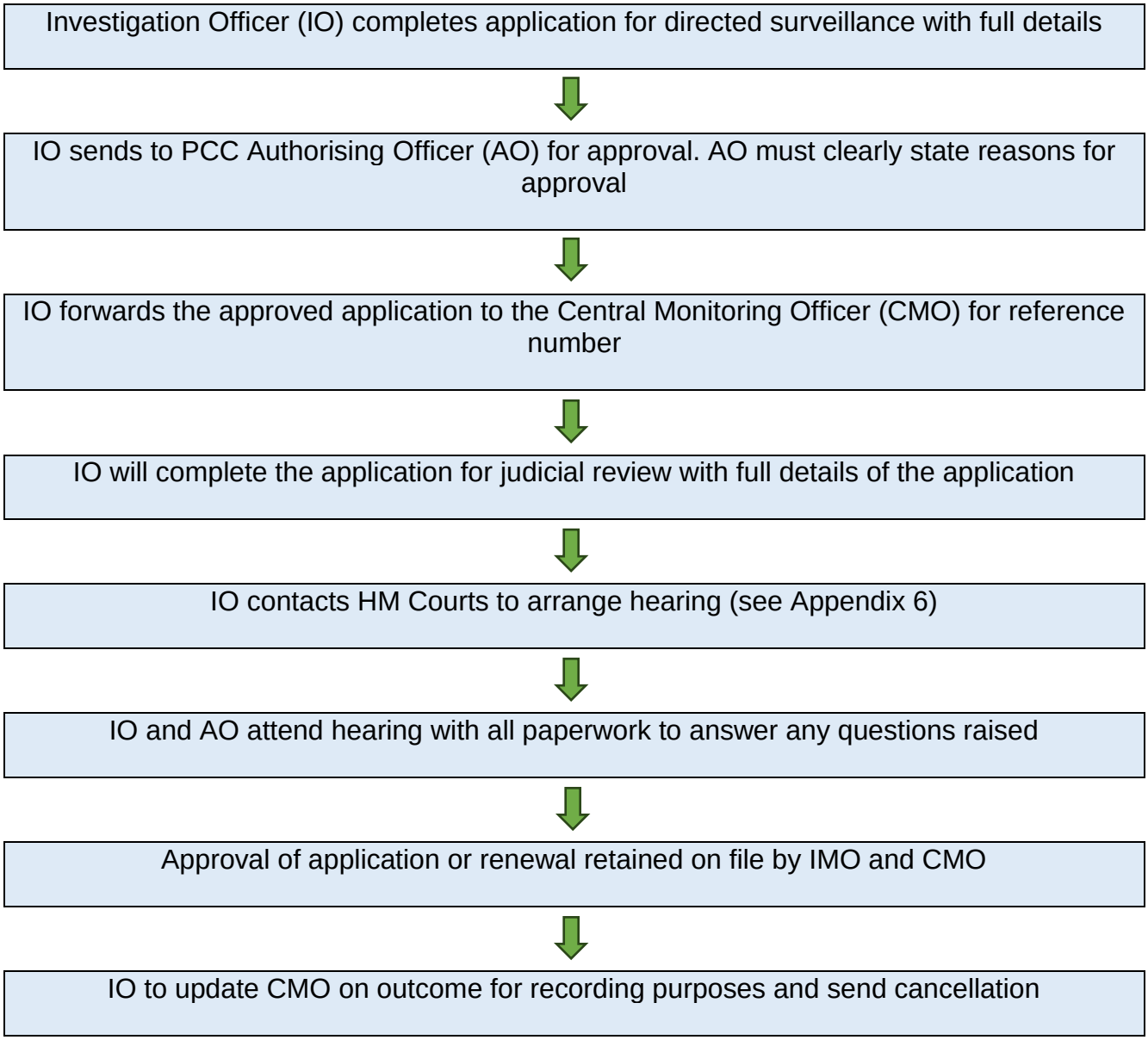
76.7 AB v Hampshire Constabulary (Investigatory Powers Tribunal ruling 5 February 2019)

This case relates to whether the use of body worn cameras can amount to surveillance as defined by legislation. In this matter, the Tribunal concluded that in this case video recording was capable of amounting to surveillance under Part II of RIPA (2000). The decision can be viewed here. https://www.ipt-uk.com/docs/IPT%20Judgment%20-%20AB%20v%20Hants%20Constabulary.pdf

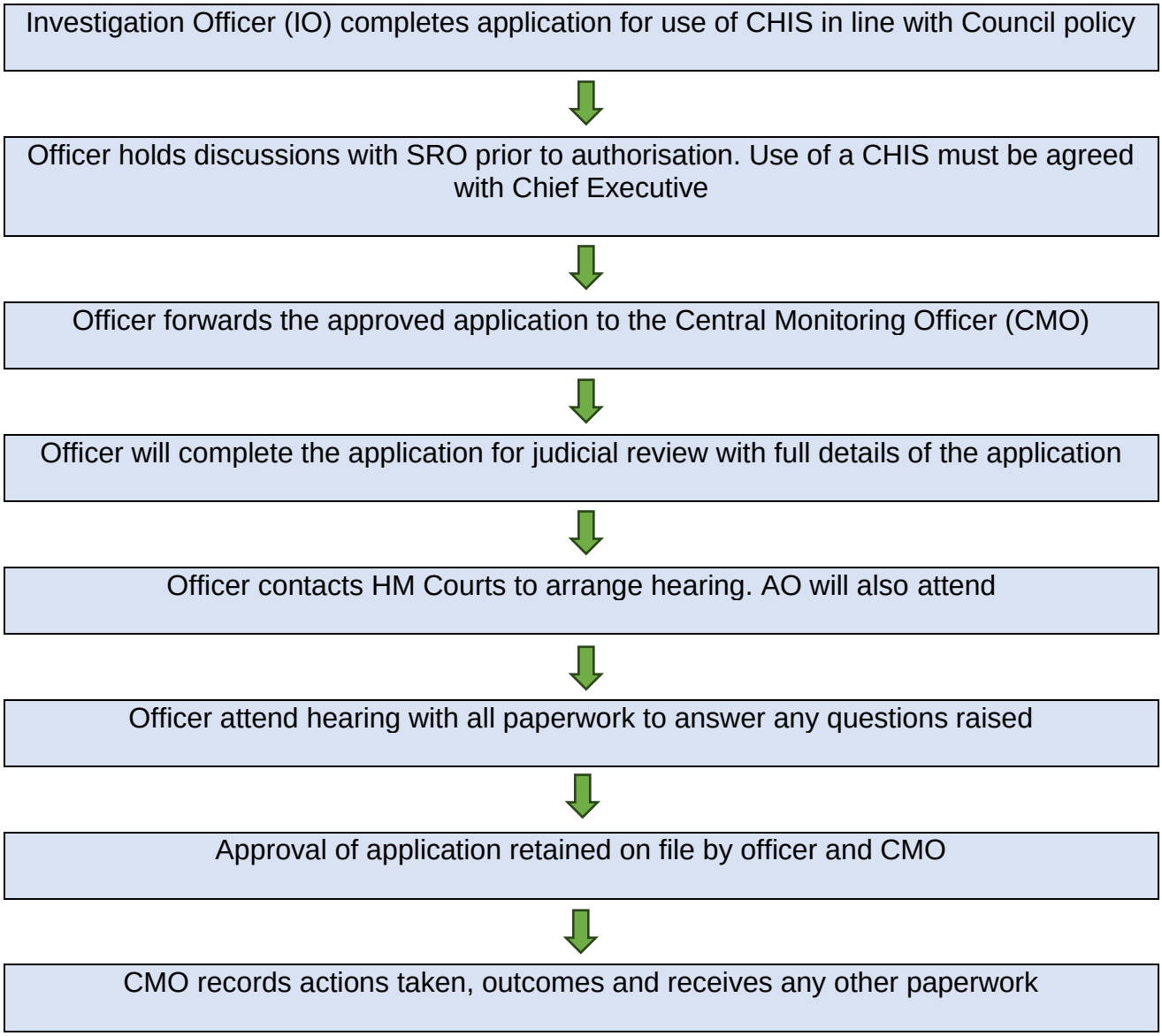
76.8 Gary Davies v British Transport Police (Investigatory Powers Tribunal 5 February 2019

British Transport Police undertook unauthorised surveillance which led to a public arrest and a press release publicising the alleged offences. Mr Davies was subsequently acquitted by a jury. British Transport Police officers had no proper understanding of the legal requirements for such surveillance and should have obtained authorisation. The surveillance was ruled unlawful. The Tribunal rejected the British Transport Police claim that the breach was technical as authorisation could and would have been obtained. This was rejected because the case against Mr Davies required further inquiries to have been made for authorisation to be possible. The Tribunal awarded Mr Davies costs of the criminal trial and also £25,000 in compensation for damages to his reputation suffered and harm caused.

APPENDIX 1 Procedure for Directed Surveillance Application



APPENDIX 2 Procedure use of Covert Human Intelligence Source



APPENDIX 3 Surveillance Assessment

		Notes
Specific location	• Type of property • Residents • Number and locations of entrances/exits • Vehicular access • Any obstructions • Any risks	
General Area	• Type of area e.g. residential or commercial • Shops in locality • Schools • Any potential hazards	
Subject	• Identity • Potentially violent • Vehicles used • Any known other sites	
Collateral Intrusion	• Detail any other individuals of whom private information may be captured • Associates • Family Children • How will it be limited e.g. times, techniques	
Observation Point	• Is location approved? • Does it require use of another building? • Routes to and from • In event of discovery of operation, agreed movement	
Equipment	• What is being used? • Do they work? • Any issues regarding signal reception on phones	

Health and Safety Assessment

Hazard (including who may be harmed)	Level of Risk	Mitigating controls

APPENDIX 4 - Social Media/Internet Access Log

Name of Applicant		Team	
Service			
Directorate			
Line Manager			
Case including reference			

Visits number	Date	Site Accessed	Reason	Information obtained	Public or Private?

Please note repeated visits will be considered monitoring and you should seek advice on making an appropriate application.
You should not use a false identity or build/maintain a relationship to obtain private information about someone.
If you have obtained private information then you should consider an appropriate application.

INVESTIGATING OFFICER	**SIGNATURE**	**DATE**
LINE MANAGER	**SIGNATURE**	**DATE**

APPENDIX 5 – RIPA/CHIS Authorisation Data – Safeguarding Guidance

What can we keep?

All documents and correspondence required to support the application and approval process to include:

- The original application and (1) if granted, they type and date of authorisation or (2) if not granted, the reasons for refusal;
- The name, title and contact details of the Authorising Officer;
- The URN of the investigation or operation together with its title and a brief description/overview of its purpose;
- Details of attendances at the Magistrates Court together with notes of the hearing to include the date, time and name of the Judge and, the Judicial Application and Order;
- Frequency and result of reviews and renewals together with the details of those involved in the process to include name, title and contact details;
- Details as to the period of the surveillance and any instruction to stop together with the details of those involved in the process to include name, title and contact details;
- Whether confidential information is likely to be obtained and, if it is obtained, ensure that it is identified and processed accordingly;
- Any other instructions given by the Authorising Officer together with a specific record of any instances when the Authorising Officer is also involved in the investigation (these to be specifically reported to the Commissioner).

No more information than is needed shall be retained.

Who can keep it?

- All information must be provided to the RIPA co-ordinator as soon as possible but in any event **within 48 hours**;
- Paper records should be addressed to the RIPA co-ordinator in a sealed envelope marked **Strictly Private and Confidential;**
- Electronic records should be sent securely within the Council's network or, if external, via a Clinked File marked **Strictly Private and Confidential;**
- So far as achievable, the RIPA Co-Ordinator's central record will be kept electronically. A separate folder will be kept for each authorisation and each folder will be password protected.
- Passwords will only be provided to those officers with a need to know the content of the folder and where it is not necessary for them to know the whole content, the RIPA-Coordinator will either provide a summary or an extract using secure means.

- Only where it is necessary for paper records to be kept will they be kept. These records will be kept in a locked filing cabinet for which access will be limited to the RIPA Co-Ordinator, SIRO and Authorising Officers.

No other records will be kept and no records should be shared with anyone outside the process.

How long should we keep it for?

The RIPA Coordinator will decide for how long the data should be kept. The decision will be taken in accordance with the Council's RIPA and Data Retention Policies.

- The central record for each authorisation will be retained for 3 years from the ending of the authorisation.
- Where a conviction is secured the central record for that authorisation will be retained for at least 6 months from the date of sentence;
- Where a custodial sentence is imposed, the central record for that authorisation will be kept until the person is released from custody or 6 months from the date of conviction, whichever is the greater;
- If the person appeals their conviction, all material which may be relevant must be kept until the appeal is determined even if that exceeds the ordinary period for retention.

No data will be kept for any longer than is necessary.

Reviewing and disposing of the data

The RIPA Co-ordinator will review the central record and arrange for the safe disposal of the data relating to each authorisation once the relevant retention period has passed.

- The RIPA Co-Ordinator will review the central record of authorisation annually from the date of the application or following each relevant stage in the enforcement process e.g. summons, trial, sentencing, appeal. Any information which the RIPA Co-Ordinator considers is no longer required will be securely destroyed.
- The RIPA Co-Ordinator will schedule a destruction date for each authorisation in accordance with the RIPA and Retention Guideline Policies. On that date the RIPA Co-Ordinator will make enquiries with the Investigating Officer as to whether there have been any developments (such as an appeal) which mean that the central record should be retained for longer.
- Where the RIPA Co-ordinator is satisfied that the documentation is no longer required, they will arrange for its secure destruction. Paper records will be disposed of in the Council's confidential waste bins and electronic records will

be deleted with assistance from ICT to ensure that the record is permanently removed.

Data will be securely destroyed when it is no longer legally required to be retained.