CHESTERFIELD BOROUGH COUNCIL
SURVEILLANCE POLICY

1 Why does the council need a Surveillance Policy?

All public bodies like the council must comply with The Human Rights Act 1998 (HRA). That act confers the right to respect for private and family life, home and correspondence (Article 8).

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for intrusive investigative procedures carried out by various authorities as part of their normal functions. This is to ensure that such procedures are carried out in a way that complies with the Human Rights Act. RIPA procedures were substantially changed by the Protection of Freedoms Act 2012.

The Investigatory Powers Commissioner carries out inspections of local authority procedures and policies, and oversees the exercise by public authorities of their powers under the Act.

2 What does RIPA cover?

RIPA aims to ensure that when public bodies carry out investigations:

- they respect the privacy of individuals and
- that there is an interference with privacy only where the law permits it and there is a clear public interest justification.

RIPA controls the use of various methods of investigation, in particular the use of:

- covert surveillance
- covert human intelligence sources ("CHIS" – see paragraph 12 below) and
- accessing communications data. [1]

If the activities proposed by investigating officers fall within the definitions then this policy and guidance must be followed.

[1] The Act states that it regulates: "the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be encrypted or accessed."

If investigating officers have any doubts about the application or meaning of this policy, they should seek advice from the council's legal service before proceeding.

The Act covers public bodies ranging from the police and secret services to district councils. The council's use of RIPA will deal mainly with carrying out surveillance and, possibly, some use of covert human intelligence sources. However, RIPA only applies to the council's core functions – its statutory duties - and not staffing issues or contractual disputes.

The changes to RIPA by the Protection of Freedoms Act 2012 took effect on 1st November, 2012. These are described in more detail in this Policy but in summary:

- RIPA authorisations must be approved by a Magistrate.
- Authorisations can only be given for preventing or detecting more serious crimes which are punishable by at least 6 months' imprisonment or concern sales of alcohol or tobacco to children.

The council may not seek authorisation for directed surveillance to investigate disorder that does not involve criminal offences or to investigate low level offences such as littering, dog fouling or fly-posting.

3 Human Rights Principles

RIPA requires compliance with the following human rights principles in investigatory work:

- Is the proposed action lawful?
- Is the proposed action proportionate?
- Is the proposed action necessary?
- Is the proposed action non-discriminatory?

Codes of Practice have been published by the Home Office and this Surveillance Policy is intended to establish procedures to ensure council officers are able to carry out their jobs without risking claims that their actions are breaching any person's rights to respect for their private and family life. **RIPA should be seen as assisting the council by providing a statutory defence against such claims**.

The requirements of RIPA and the HRA impact on all officers of the Council but mainly those who undertake investigatory or enforcement activities, including, Environmental Health, Planning and Internal Audit.

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime.

4 Restrictions on Surveillance

council officers may **only** authorise or engage in:

- covert surveillance,
- CHIS, and
- access to communication data

where it is:

- necessary for the "prevention or detection of crime or disorder" (and the criminal offences concerned are punishable by a maximum term of at least 6 months' imprisonment OR are related to underage sales of tobacco or alcohol). Examples of such offences are:-
    - dumping of dangerous waste
    - serious criminal damage
- and proportionate in what it seeks to achieve.

Whether or not the crime threshold is met should be kept under review during the course of the investigation. If the relevant criminal offence is downgraded and the threshold no longer met the authorisation for surveillance should be cancelled.

5 Definitions

"Surveillance" is:

- monitoring, observing or listening to persons, their movements, their conversations or other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

Surveillance can be general (not directed at an individual or group) or ***covert***. Only *covert surveillance* is covered by RIPA.

Types of Surveillance

Surveillance may be ***overt*** or ***covert***.

Overt Surveillance

RIPA is not concerned with ***overt*** surveillance. Most of the surveillance carried out by or on behalf of the council will be overt. That is, there will be nothing secretive, clandestine or hidden about it. In many cases, officers will

simply be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about council business openly (e.g. a council officer walking through one of the council's housing estates or inspecting council land).

Similarly, surveillance will be ***overt*** if the subject has been told that it will happen (e.g. where a noisemaker is warned, preferably in writing, that noise will be recorded if it continues, or where an premises licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the licence holder to check that licence conditions are being met).

Covert (or 'hidden') Surveillance

However, covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is not aware it is or may be taking place. That is, it is done **secretly**.

Directed Surveillance

Directed Surveillance is surveillance which is:-

- covert;
- NOT **intrusive surveillance** (see definition below) –
- Not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act not reasonably practicable (e.g. spotting something suspicious and continuing to observe it) and
- undertaken for the purpose of a **specific investigation or operation** and
- in a manner **likely to obtain private information**about a person (whether or not that person is specifically targeted). (Private information is any information about a person's family or private life – see definition below).

Private information

Private information is defined in section 26(10) of the 2000 Act as including any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others, and can include running of business affairs. Family life should be treated as extending beyond the formal relationships created by marriage.

6 Effect of Valid Authorisations

An authorisation will provide lawful authority for a public authority to carry out covert surveillance. A covert surveillance operation will not always require an

authorisation. However, authorisation is required where the purpose of the covert surveillance (wherever it takes place) is to obtain private information about a person, whether or not that person is the target of the investigation or operation.

The key issue in Directed Surveillance is the targeting of an individual with the likely effect of gaining private information (as defined above**).**

7 CCTV and other Cameras

7.1 RIPA does not cater for the use of overt CCTV surveillance systems, as members of the public should be made aware that such systems exist. General use of CCTV does not require authorisation. However, data protection considerations relating to personal information will apply to overt CCTV.

7.2 However, if CCTV is used for a covert pre-planned operation to follow an individual already identified then an authorisation should be sought for Directed Surveillance.

7.3 While the covert pre-planned operation may be carried out jointly with the police, if the surveillance is in relation to possible criminal prosecution by the police, then it is the police who should seek a prior authorisation under police RIPA procedures.

7.4 It is only when the council is planning carrying out covert pre-planned operation in relation to its own possible criminal proceedings that authorisation should be sought under the council's policy.

7.5 Relevant law relating to the use of CCTV (eg Protection of Freedoms Act 2012 and guidance (eg ICO's CCTV Code of Practice, Surveillance Camera Commissioner's Code of Practice) as well as the council's own code of practice should be followed when any CCTV is used.

7.6 These considerations are also relevant when considering use of other forms of cameras. For example, body cams, deployable cameras, and drones (if used).

7.7 Care needs to be taken if cameras are to be hidden, notwithstanding signs in the locality, as these may be considered to be covert. Signs are always necessary to make surveillance by cameras overt. This means that care should always be taken to ensure signs are in place in the vicinity of deployable cameras and body worn cameras.

7.8 If for any reason these cameras are to be used in circumstances where they are not overt and without signage, as they are likely to be below the RIPA threshold, careful discussion with an Authorising Officer and documented in case of challenge or complaint.

7.9 *Drones*

Use of airborne crafts to carry out surveillance can be regarded as covert due to their reduced visibility at altitude. Therefore the rules about directed surveillance authorisations apply to their use.

8 Intrusive Surveillance

This **cannot** be carried out by the council and only relates to investigations as described below.

Covert surveillance is intrusive if it:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle;

- **involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (i.e. any apparatus designed or adapted for use in surveillance and will include cameras, tape recorders etc.**

However, surveillance carried out in relation to residential premises by use of a device (i.e. a camera) which is not in or on the premises **is not intrusive** (although it will be directed) unless it is of the same quality of information as would be obtained if the equipment was in the premises.

9 Examples of Types of Surveillance

Type of Surveillance:	***Examples:***
Overt	• Street Warden, Enforcement Officer or Ranger on routine patrol • Sign-posted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.
Directed must be RIPA authorised	• Officers follow an individual or individuals over a period, to establish whether they are working when either claiming benefit or whilst off sick from employment • Test purchases where the officer has hidden camera or other recording device to record information that might include information about the private life of a shop-owner, e.g. where they are suspected of running their business in an unlawful manner

<u>Intrusive</u> - the council cannot do this!	• Planting a listening or other device ('bug') in a person's home or in their private vehicle or using a sophisticated listening device outside a person's home or in their private vehicle that will provide results equivalent to being 'on-site'.

- Going onto residential premises to take action to address an immediate nuisance, where it would not be reasonably practicable for an authorisation to be sought, is not covert surveillance (it might breach Article 8 (right to privacy) but would come within the permitted derogations provided the action could be shown to be proportionate to the harm being caused).

10 Communications Data

Local authorities are only permitted to acquire communications data for the purpose of preventing or detecting serious crime. This is an offence punishable by a maximum term of 12 months imprisonment or more.

Special additional rules apply to acquiring communications data. The Home Office Acquisition and Disclosure of Communications Data Code of Practice[2] sets these rules out.

The request must also be made through a qualified single point of contact accessed via the National Anti-Fraud Network and must also receive prior judicial approval[3].

What is communications data?

The Regulation of Investigatory Powers (Communications Data) Order 2010 extends to local authorities certain powers set out within RIPA to access ***communications data***.

Communications data includes information relating to the use of a ***communications service*** <u>but **does not include the contents of the communications itself**</u> (see section 21(4) RIPA [4] for the detailed definition of "communications data").

[2] https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

[3] See www.nafn.gov.uk

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

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person— (i0) of any postal service or telecommunications service; or (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;(c) any information not falling within paragraph (a) or (b) that is held or obtained, in

Local authorities are allowed to access certain types of communications data **only for the purposes of the prevention or detection of crime or the prevention of disorder.**

The types of data concerned are as follows:

Subscriber ("Customer") data
being any information, which does not include any of the contents of a communication, about the use made by any person of a postal or telecommunications service. In respect of a telecommunications service provider this is normally referred to as the "billing information"). This will include:

- Name of subscriber
- Address for billing, delivery or installation
- Contact telephone numbers
- Abstract personal data provided by the subscriber e.g.
- demographic information
- Subscriber account information e.g. billing arrangements
- including bank, credit/debit card details Other services provided to the customer

Service data being any other information held by the service provider relating to the persons to whom the service is provided. (This is normally referred to as **"subscriber information**"). This will include:

---

relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

Traffic Data is *(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, (b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted, (c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and (d) any data identifying the data or other data as data comprised in or attached to a particular communication,*

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

(7) In this section— (a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a telecommunication system by means of which a communication is being or may be transmitted include references to any telecommunication system in which that apparatus is comprised; and (b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other; and in this section "data", in relation to a postal item, means anything written on the outside of the item

- The period during which the customer used the service Information about forwarding services provided by telecommunication service providers and re-direction services provided by postal service providers
- Itemised billing information
- Information on connection, disconnection and redirection Information on conference calls, call messaging, call waiting and call barring services
- Top-up details for pre-pay mobile phones including credit/debit cards used
- For postal items, records of registered, recorded or special delivery of postal items and the delivery or collection of parcels.

Access to communications data may be authorised by seeking the specialist services of the National Anti-Fraud Network of which the council is a member.

11 Procedures for Authorising Directed Surveillance

11.1 Need for Proper Authorisation

It is crucial that **all directed surveillance**, **using a CHIS or accessing communications data** is properly authorised. The authorisation and supporting documents setting out the case will then form the basis of the application to a Magistrate for consideration and approval.

Failure to secure proper authorisation and to comply with this procedure could lead to evidence being excluded by the court, significant costs being awarded against the council and complaints against the council.

11.2 General rules on Authorisations

11.2.1 Necessity and Proportionality

Obtaining an authorisation under RIPA will ensure that there is a justifiable interference with an individual's rights to privacy only if the interference is necessary, proportionate and in accordance with the law.

11.2.1.1 Necessity

The person granting an authorisation must believe that the authorisation is necessary **for the purpose of preventing or detecting crime or of preventing disorder of the type that could involve criminal offences.** In order to be satisfied there must be an identifiable offence to prevent or detect before an authorisation can be given. **The offence must be of a sufficiently serious category.**

11.2.1.2 Proportionality

Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out: not the proverbial 'sledgehammer to crack a nut'. This involves balancing:

- the intrusiveness of the activity on the target and others who might be affected by it against

- the need for the activity in operational terms.

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

The HRA defines an action as proportionate if it:

- Impairs as little as possible the rights and freedoms of the individual concerned and of innocent third parties

- Is carefully designed to meet the objectives in question

- Is not arbitrary, unfair or based on irrational considerations

All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

A potential model answer would make clear the four elements of proportionality had been considered:

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

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

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

(d) evidencing what other methods have been considered and why they were not implemented.

11.2.1.2 In accordance with the law

The exercise of these powers must always be in relation to matters that are statutory or administrative functions of the council.

Officers seeking authorisation must present their application in a fair and balanced way. The application should set out any information which supports or weakens the case for authorisation

11.2.3 Collateral Intrusion

Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion).

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the surveillance.

Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

11.2.4 Confidential Information

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved.

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. So, for example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation by the Chief Executive (see Appendix 1).

11.3 Detailed Authorisation Procedures

11.3.1 Completing Application Forms

All procedures under RIPA must be documented on standard forms and records kept. This is necessary to show compliance with RIPA. Standard forms can be downloaded from the Home Office Security site at https://www.gov.uk/government/collections/ripa-forms--2

The RIPA Codes of Practice are at
https://www.gov.uk/government/collections/ripa-codes

An applicant should complete the application form giving full details about the proposed surveillance and its duration. Particular care should be given to the following points:

11.3.2 Time Limit

A written authorisation granted by an authorising officer and approved by a Magistrate will take effect when signed by the Magistrate. It will automatically cease to have effect unless renewed or cancelled at the end of a period of three (3) months beginning with the day on which it took effect.

An authorising officer must set suitable review dates on which the authorisation can be formally reviewed with the applicant.

11.3.3 Application Details

- Why the action is being begun: why is it felt to be **necessary**?
- Why the action is **proportionate** to what it seeks to achieve: for instance could the required information reasonably be obtained by other means? It must be shown that there cannot be any other reasonable way of doing this. The questions to consider are:
- Is this excessive in relation to the offence? (For example, suspected theft from the workplace may merit surveillance at work but not at the person's home. The length of the investigation also needs to be proportionate.)
- Is there any less intrusive way of doing this and has it been thought through?
- What **collateral intrusion** is likely – other people and their Article 8 (1) rights (respect for private and family life, home and correspondence). Information about others should be minimised.
- Proportionality is **not** the same as necessity – there are separate boxes on the form for these two aspects.
- What action is to be authorised(i.e. observation or following, reference to any premises or vehicles involved and whether they are public or private) – describe the intended actions
- What information is sought from the action – for example, is there a breach of planning control?
- What is the likelihood of acquiring any religious or confidential material such as medical or financial records, legal documents etc.? **In such a**

case authorisation should be obtained only from the Chief Executive or (in his or her absence) any Executive Director or the Local Government & Regulatory Law Manager

The applicant should discuss the contents of the form with the authorising officer, who if satisfied should sign the form. The authorising officer must fill in the box for his comments, addressing the issues of necessity and proportionality.

11.3.4 Urgent Cases

These will be extremely rare and an urgent case may be one where delay may, in the authorising officer's opinion, jeopardise the operation for which authorisation is being given. A lack of forethought or planning does not constitute urgency. If out of hours access to a JP is required, the council must make arrangements with HM Courts and Tribunals legal staff.

However, no RIPA authority is required an immediate response to events or situations where it is not reasonably practicable to obtain it, for instance, where criminal activity is observed during routine duties and officers conceal themselves to observe what is happening.

11.4 Action during and after the Surveillance Period.

Each surveillance should have a dedicated log-sheet for officers' use. This should be kept in chronological order detailing who is the subject of the surveillance, where it is and what happens. When notes cannot be written up at the time of surveillance it should be completed as soon as possible afterwards.

All alterations in the log sheet should be crossed through and initialled and then the corrected material written to the side in the normal manner. Correction fluid should not be used at any time. Completion of the log should ensure that no empty lines are left where additional material could be written in at a later date. These logs could be used in the event of a criminal prosecution and should be kept correctly, signed as true statements and secure at all times.

In all cases there is a duty of care to those observed. All details and approvals must be kept strictly confidential. The privacy of individuals must not be put at risk and unnecessary information should not be documented i.e. if the observed person was incidentally observed in a private context such as an extra-marital affair.

When photographs or videos are taken then a photographic log needs to be maintained and all negatives retained. Technology is available to alter photographs and the logs are important to prove the originality of the photographs/videos.

Log sheets should be kept locked with the rest of the supporting documents for a period of at least three years.

Time limits should be placed on any authorisation for surveillance. In all cases written authorisations last for three months and then must be renewed if deemed necessary, using the appropriate form. Authorisations must be cancelled when no longer necessary or appropriate. Authorising officers should keep diary reminders for cancellation/renewal dates.

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. The requirements of the Code of Practice under the Criminal Procedure and Investigations Act 1996[5], regarding recording and retention of material obtained in the course of an investigation, must be observed.

While there is nothing in RIPA to prevent use of material properly obtained through the authorised process in other investigations, material obtained will be protected by the Data Protection Act 2018 (DPA) and in addition to other considerations must be used, stored and destroyed in compliance with the relevant requirements of the DPA and the council's data protection, information security and records management policies.

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Section 9 of the Home Office Code of Practice sets out safeguards must be in place. Confidential and privileged information must be given particular protection.

11.5 Renewals

Any person who would be entitled to grant a new authorisation can renew an authorisation. However, it should be the person who originally granted the authorisation. Authorisations (other than oral authorisations in urgent cases) may be renewed more than once, provided they continue to meet the criteria for authorisation. Renewals must also be authorised by a Magistrate.

Authorisations may be renewed more than once; if necessary, and the renewal should be kept/recorded as part of the central record of authorisations.

Consideration of any renewal application must consider the matter afresh, taking into account the content and value of the investigation, the information obtained so far. It must consider the same criteria as for new applications.

[5] https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-code-of-practice

11.6 Cancellations

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. If in doubt about who may cancel an authorisation, Legal Services must be consulted. There is no requirement for a Magistrate to consider cancellations.

12 Use of Covert Human Intelligence Sources (CHIS)

12.1 A person is a covert human intelligence source if they:

- establish or maintain a personal or other relationship with a person either to use the relationship to obtain information or disclose information obtained as a result of such a relationship;

- the surveillance is covert if and only if it is carried on in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

Examples of use of a CHIS are the use of professional witnesses or in 'entrapment cases' when a person pretends to be a customer (but see paragraph 9 and below)

Other circumstances in which the council could be considered to be using a covert human intelligence source is where a neighbour is requested to provide information about a neighbour and information is obtained not by personal observation as in the case of neighbour nuisance, but is information obtained through conversation with the neighbour under investigation such as personal relationships. This means that asking a neighbour for information regarding who is living in a property and the relationship between the parties would be using that person as a covert human intelligence source, which would need special authorisation.

Asking a neighbour to keep records of nuisance suffered by the neighbour would not be using a covert human intelligence source because the neighbour would not be relying on a relationship with the person under investigation to obtain information. However, every case should be considered on its merits. If it becomes apparent that information is being obtained in the course of a relationship, the neighbour may in reality be a CHIS and legal advice should be sought before acting on their information.

12.2 Juvenile Sources

Special safeguards apply to the use or conduct of a juvenile CHIS (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. The advice of Legal Services must be sought if the use of juveniles is being considered.

There are additional requirements if a person under 18 is a CHIS. Authorisation for an application to the Magistrates Court can only be granted by the Chief Executive or in their absence by an officer acting as head of paid service. This also applies to vulnerable individuals, below.

12.3 Vulnerable Individuals

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 herself, or unable to protect himself or herself against significant harm or exploitation.

A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. The advice of Legal Services must be sought if the use of vulnerable individuals is being considered.

The same additional requirements apply when considering appointing a vulnerable individual as an under 18 year old (see above).

12.4 Test Purchases

Carrying out test purchases will not generally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business e.g. walking into a shop and purchasing a product over the counter.

However, developing a relationship with a person in the shop, to obtain information about the sellers suppliers of an illegal product e.g. illegally imported products will require authorisation as a CHIS. Similarly, using mobile, hidden recording devices to record what is going on in the shop will require authorisation as directed surveillance. Note that a CHIS may be authorised to wear a hidden camera without the need for a separate directed surveillance authorisation.

The use of covert human intelligence source for a particular investigation must be subject to prior authorisation by a senior officer of a rank specified in Regulations made under RIPA. CBC's authorising officers are listed at the end of the document.

12.5 Appointment of a CHIS

A named officer (i.e. a 'handler') will have day to day responsibility for dealing with the CHIS. That officer will:

- Fully recognise the council has a duty of care to the CHIS, whose security safety and welfare is paramount,

- Undertake a risk assessment prior to the use of the CHIS to determine the risk to them and the likely consequences should their role become known,

- Take fully into account, at the outset, whether there will be ongoing security and welfare considerations related to the CHIS, once the authorisation has been cancelled, and

- Maintain a record of the use made by the CHIS, and regulate access to them, ensuring that the Regulation of Investigatory Powers (Source Records) Regulations 2000[6] are fully complied with.

A further named officer will have general oversight of the use made of the CHIS (i.e. a 'Controller').

12.6 Safety and Welfare of CHIS

The safety and welfare of the CHIS is paramount. Risk assessments should be carried out to assess the risk of tasking a CHIS and the activities being undertaken taking into account the particular person appointed. The risk assessments should be regularly reviewed during the course of the investigation.

A single point of contact (SPOC) should be appointed for the CHIS to communicate with. They will be responsible for carrying out the risk assessments and taking all steps to ensure CHIS welfare and safety. A senior officer must also have oversight of the arrangements and be regularly updated by the SPOC. There should be regular face to face meetings with the CHIS, in addition to any appropriate remote contact (telephone or email).

13 Social Media and the Internet

13.1 While it is recognised that online information is a valuable source of information for public authorities carrying out their statutory purposes, persistent studying of an individual's online presence, extracting and recording material may engage privacy considerations and a RIPA authorisation might be necessary. Social media sites should only be viewed where necessary and viewing must be proportionate. Repeated viewing/recording without consent will engage RIPA. Automatic internet search tools (e.g. Google alerts) can also engage RIPA.

13.2 However, because the information is available in the public domain does not mean that the intention was to make it available for covert investigative activity.

13.3 Use of a false identity, or a fake social media profile, may require authorisation. Using the identity of a person known or likely to be known to the subject of interest without authorisation or their consent is likely to breach

[6] SI 2000/2725 http://www.legislation.gov.uk/uksi/2000/2725/made

RIPA. Officers should not use their own personal social media accounts for these purposes.

13.4 If the investigator engages in any form of relationship with the account operator without disclosing their identity then they become a CHIS requiring authorisation as such. They will require management by a Controller and Handler with a record being kept and a risk assessment created.

13.4 Where consent has been given, or the public authority has taken reasonable steps to inform the individual that surveillance is or may be taking place, the activity is likely to be seen as overt.

13.5 Care should be taken where there is collateral intrusion. While consent may have been given to access material, it might contain private information relating to third parties (e.g. in comments under a Facebook post) who have not given consent.

14 Employee Surveillance and Monitoring

14.1 While outside the RIPA controls, any surveillance – or monitoring - involving employees must comply with Part 3 of the Employment Practices Code[7], and the Data Protection Act 2018. Monitoring is not only associated with disciplinary investigations, but also routine activities such as monitoring to ensure those working in hazardous environments are not put at risk due to unsafe working practices.

14.2 Where monitoring goes beyond one individual simply watching another and involved the manual or automatic recording/processing of personal data it must be done in a way that is lawful and fair to workers. Any adverse impact on workers must be justified by the benefits to the employer and others.

15 Record Keeping – Central Record

15.1 The council keeps a record of all authorisations; renewals, cancellations and rejections.

15.2 This is an electronic **Central Record** and is monitored by the RIPA Co-ordinator in the Local Government and Regulatory Law Team.

15.3 The record shows:

- the type of authorisation;
- the date the authorisation was given;
- name of the authorising officer; the unique reference number (URN) of the investigation or operation;

[7] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

- the title of the investigation or operation, including a brief description and names of subjects, if known; whether the urgency provisions were used, and if so why.

- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name of the authorising officer;

- whether the investigation or operation is likely to result in obtaining confidential information as defined in this policy

- the date the authorisation was cancelled.

15.4 The Central Record is password protected, and access to it is strictly limited.

15.5 The Central Record is linked to scanned-in copies of RIPA documents themselves.

15.6 The council will keep records for a period of 6 years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) may at any time audit/review the council's policies and procedures, and individual authorisations.

15.7 The Local Government and Regulatory Law Team will make arrangements for applications for approval by a Magistrate once an authorisation has been granted by a designated council Authorising Officer.

15.8 The Magistrates' Court will make a copy of a RIPA authorisation, the original of which is to be retained by the council.

16 Records maintained by the Investigating Department

16.1 The following original documents must be retained by the Local Government and Regulatory Law Team and copies kept by the relevant Service Manager:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- a record of the dates on which an authorisation or notice in relation to access to communications data was started and cancelled;

- the frequency of reviews prescribed by the Authorised Officer;

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

- a copy of any renewal or an authorisation, together with supporting documentation submitted when the renewal was requested;

- the date and time when any instruction was given by the Authorised Officer;

- the Unique Reference Number for the authorisation (URN).

16.2 Each form will have a URN which will be generated by the Central Record. **A URN should be requested by an applicant from the Local Government and Regulatory Law Team** before the application is made, so that authorised and rejected applications will be recorded.

16.3 The Central Record and all other records are to be kept STRICTLY CONFIDENTIAL and may only be disclosed by or with the written consent of Legal Services.

17 Arvato, Kier and others

17.1 In some cases other investigative and enforcement staff may carry out authorised surveillance on when acting on behalf of the council.

17.2 Relevant Arvato and Kier staff must also maintain awareness relating to RIPA and receive relevant training and any directed surveillance must be properly authorised.

17.3 The Senior Responsible Officer should be satisfied that clear and effective procedures are in place to ensure any RIPA related activity is properly conducted by such partners.

18 Responsibilities of Elected Members

18.1 The Cabinet Member for Finance and Governance has portfolio responsibility for RIPA matters.

18.2 RIPA Codes of Practice in force from December 2014 recommend a scrutiny role for councillors in relation to RIPA. Accordingly at least once a year, the council's use of RIPA will be reviewed and its Surveillance Policy amended, if necessary, by Cabinet member and/or Standards and Audit Committee as appropriate.

18.3 On a regular basis, members should scrutinise internal reports on the use of RIPA to ensure that it is being used consistently in accordance with the council's policy. The RIPA Senior Responsible Officer will report to Standards and Audit Committee at least once a year, whether or not there has been any authorised surveillance activity.

19 Training

19.1 Relevant officers under this policy shall receive regular training to ensure their awareness is current and the authority is in a position of readiness to use these controls. This will also help ensure that investigating officers do not inadvertently undertake directed surveillance without proper authorisation.

19.2 Officers should undertake relevant mandatory training at least once a year, using in-house or external online and/or face to face training. Legal advisors should undertake specialist legal training as necessary to ensure awareness of the law within the legal service is up to date.

19.3 Relevant training is necessary, even if there is no directed surveillance or use of CHIS, to ensure the authority is prepared to take action should the need arise.

20 Error Reporting

29.1 Care must be taken to avoid errors. Relevant errors must be reported to the IPC because errors can have significant consequences for an individual's rights. Full details are contained in the 2018 Code of Practice.

20.2 Errors include:

- Surveillance without lawful authority
- Failure to comply with safeguards in statute or the code of guidance

Also

- any authorisation obtained due to an error of a person providing information, relied on in good faith by public authority
- Legally privileged materials obtained
- Failure to keep to safeguards for the use of a CHIS

20.3 Errors must be reported to the IPC through the SRO as soon as reasonably practicable and within 10 working days (or longer as agreed with IPC) after it has been established that an error has occurred. An interim notification to the IPC, pending full facts being established, can be made but this must give an estimated timescale of when the full report will be submitted.

20.4 This means that the SRO must be made aware of the error **as a matter of priority** so that these timescales will be met and/or the IPC informed. The SRO will also decide whether or not a relevant error has occurred and give advice, if appropriate, on how to avoid repetition of the error.

20.5 The report should contain:

- Details of the error
- Reasons why the report has not been available within 10 working days (if applicable)
- Cause of the error
- The amount of surveillance carried out and material obtained
- Any unintended collateral intrusion
- Any analysis or action taken
- Whether material retained or destroyed

- Steps taken to prevent recurrence

20.6 The IPC has power to inform the individual affected by a serious error and their rights to take the matter to the Investigatory Powers Tribunal. Home Office guidance sets out what action the IPC may take.

20.7 Material obtained under a covert surveillance authorisation must be handled in line with the council's other safeguards and policies, including breaches of data protection requirements. Any actions must also comply with GDPR and Data Protection Act 2018, including the new law enforcement processing requirements for criminal investigations and prosecutions. This means that errors and breaches might also have to be reported to the Information Commissioner.

20.8 The council must also report to an inspector at the commencement of a RIPA inspection all activity which should have been authorised but was not. This is to ensure that it can be demonstrated that any direction from the IPC has been followed.

21 Role of Senior Responsible Officer

21.1 In addition to the roles described elsewhere in this policy the SRO will have responsibility for:

- error reporting
- reviewing procedures and policy
- keeping intranet and website information updated
- issuing guidance to relevant officers
- monitoring online training material
- ensuring that all authorising officers are of an appropriate standard

22 Government and ICO Codes of Practice and Guidance

It is vital to take full account of relevant codes of practice and guidance because they set out current best practice and authoritative advice. They will also be taken into account by the courts and IPC when considering the actions of a public authority.

22.1 The Home Office has issued codes of practice including:

- Covert surveillance and property interference (2014, updated 2018)
- Covert human intelligence sources (2014, updated 2018)
- Acquisition and disclosure of communications data (2015)
- Interception of communications (2016)

These and any other relevant guidance are at:
https://www.gov.uk/government/collections/ripa-codes

It has also issued other guidance, for example:

- Judicial approval process (in the Magistrates Court) (2012)

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

22.2 The ICO Code of Practice on Surveillance Cameras and personal information (2017):

https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

22.3 The Surveillance Camera Commissioner's Code of Practice (2013):

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157901/code-of-practice.pdf

23 Amendment of this policy

23.1 This policy and any relevant authorisations, procedures and guidance will be reviewed and amended as necessary from time to time by the Senior Responsible Officer and/or as the result of consideration by the Cabinet Member and/or Standards and Audit Committee (see paragraph 17).

Appendix 1: Officers with RIPA Responsibilities

Authorising Officers where knowledge of confidential information is not likely to be acquired

An authorisation should not be granted by an officer directly involved in the surveillance because there should be an independent review of whether the surveillance is both necessary and proportionate.

Where an officer listed below considers that he or she is directly involved in the surveillance the Local Government & Regulatory Law Manager (Monitoring Officer and Senior Information Risk Owner (SIRO)) will nominate an alternative authorising officer.

All officers listed below will have been or will be trained in RIPA.

A solicitor from the Local Government and Regulatory Law team

Arvato	Head of Customer Services
Kier	Head of Contract (Kier)

Authorising Officers in cases where knowledge of confidential information is likely to be acquired

The Head of Paid Service (Chief Executive) or (in his or her absence) the Local Government and Regulatory Law Solicitor (Monitoring Officer) in exceptional circumstances (see below), or the Information Assurance Manager

RIPA Senior Responsible Officer

The Local Government & Regulatory Law Manager or other officer of equivalent level to be nominated by the Chief Executive to have responsibility for the integrity of the process in place within the council for covert activity. The functions of this individual are as follows:

(a) To ensure compliance with RIPA and relevant Codes of Practice.

(b) To assess the risks that the council is taking and to quality assure the work of the authorising officers.

(c) To review authorisations to assess whether lessons can be learned from the tactics sought and/or granted.

(d) To review whether the requirement for RIPA authorisation is being considered appropriately.

(e) To support authorising officers and facilitate applications to a Magistrate for approval as soon as possible after an authorisation has been made.

(f) To appraise the Chief Executive of the impact of covert activity and any risks that are being taken.

(g) To engage with Commissioners and Inspectors when they conduct their inspections and if necessary implement post-inspection recommendations.

(h) To facilitate members' review and scrutiny powers.

(i) To liaise with the National Anti-Fraud Network where there is a need to access communications data in order to use the services of that organisation as an expert single point of contact for such data requests.

While Home Office guidance implies that the SRO should also be an authorising officer and this dual role can provide additional resilience, the SRO should only authorise in exceptional circumstances.

Document Control

Amendments to policy:

April 2014	*Cabinet 20th May 2014*
Updated 2015	*Changes to CMT*
2016	*new CMT structure*
February 2017	*RIPA Inspection recommendations and current best practice.*
April 2019	*S&A Committee: Changes to take account of 2018 Codes of Practice and current best practice*
June 2019	*Changes to ease reading of the document – eg s/he and him/her etc replaced with non gender specific terms*