Guildford Borough Council
Covert Surveillance and Investigative Powers Policy and Procedure

Document Information

Version: 1.0

This document replaces: All previous policies and procedural guides from Guildford Borough Council

Service Policy Owner: Guildford Borough Council Legal and Democratic Services

Governance: Monitoring Officer in consultation with Corporate Governance & Standards Committee (GBC) – Followed by recommendation to the Executive

Date of approval: TBC

Next review date: October 2024

Target Audience: All staff

Covert Surveillance and Investigative Powers Policy and Procedure....1
Document Information....1
PART 1 – Definitions & Policy....3
Executive Summary....9
Commitment of the Council....10
Scope of this policy and procedural document....10
Governance roles, responsibilities and communication....11
Review of this policy and procedure....15
Part 2 – Procedure....16
Summary of the authorisation procedure....16
Authorisation of surveillance....17
Duration, reviews, renewals and cancellation of authorisations....21
Reporting Errors....23
The central record....24
Records retention and destruction....25
Part 3 - Appendices....27
Appendix A: Authorising officers....27
Appendix B:....28
Appendix C: Examples to help you decide whether your activities are covered by this policy....34
Appendix D: Forms....38

PART 1 – Definitions & Policy

Definitions:

"Article 8 – Right to respect for private and family life"

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is 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 or morals, or for the protection of the rights and freedoms of others.

"Collateral Intrusion"

The risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation

"Communications Data"

This covers the obtaining of Communications Data and disclosure to any person of such data. Communications Data relates to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

"Confidential Journalistic Material"

This relates to material acquired or created for journalism purposes and subject to an undertaking to hold it in confidence, as well as communications resulting in information acquired for the purposes of journalism and held subject to such an undertaking.

"Confidential Material"

This is information where the subject of the operation may reasonably expect a high degree of privacy, or where confidential information is involved - including matters subject to legal privilege, confidential personal information - e.g., medical records or journalistic material.

"Confidential Personal Information"

This is information held in confidence relating to the physical or mental health of any identifiable individual (living or dead). This may include oral or written communications subject to an express or implied undertaking to hold the information in confidence. The definition above applies only in the context of covert surveillance and differs from the definitions of sensitive personal data used in guidance on data protection matters.

"Covert"

In general, covert is defined as something carried out in a manner calculated to ensure that the subject of the surveillance is unaware of it.

If activities are not hidden from the subjects of your investigation, you are not within the RIPA Legislation framework at all.

Similarly, surveillance is overt if the subject has been told it will happen

"Covert Human Intelligence Source (CHIS)"

Under the 2000 Act, a person is a CHIS if: they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c); they covertly use such a relationship to obtain information or to provide access to any information to another person; or they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained 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. A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question. This can therefore include undercover officers, public informants and, in some circumstances, people who make test purchases.

"Covert Surveillance"

This includes the three covert surveillance techniques that councils have the power to use: Directed Surveillance, the use of a CHIS and the obtaining of Communications Data

"Data Protection Legislation"

Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

"Directed Surveillance"

As defined by the Home Office's Covert Surveillance Code of Practice (2018) this is surveillance which is covert (i.e. the subject does not know they are under surveillance), but not Intrusive, and is undertaken:

- For the purposes of a specific investigation or operation
- In a way likely to result in obtaining private information about a person (whether or not specifically identified for the purposes of the investigation)
- Not as an immediate response to events of such a nature that it would be unreasonable and impracticable for an authorisation under RIPA Legislation to be sought

"Entity Data"

This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

Entity Data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore Entity Data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be Events Data.

Examples of Entity Data include:

- 'Subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space?";
- 'Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- Information about selection of preferential numbers or discount calls.

"Events Data"

Events Data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

Events Data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications Data is limited to communication events describing the transmission of information between two or more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

Examples of Events Data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed); itemised telephone call records (numbers called);
- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.[1]

"Intrusive Surveillance":

Directed Surveillance becomes Intrusive if carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device.

If the device is not on the premises or in the vehicle, it is only Intrusive surveillance if it consistently produces information of the same quality as if it were.

Where surveillance is carried out by a device designed mainly for providing information about a vehicle's location, the activity is Directed Surveillance.

Surveillance involving commercial premises and commercial vehicles does not fall within the definition of Intrusive surveillance. (Unless legally privileged instructions/advice are likely to be given on the premises)

[1] Definition taken from Communications Data Codes of Practise

Please note Local Authorities are not allowed to carry out Intrusive Surveillance.

"Necessary"

The exercise is deemed "necessary" if it passes the necessary authorisation criteria (i.e., the detection or prevention of crimes – different seriousness levels depending on which technique you are using) – See Section below "The Necessity Test". The applicant and AOs must also be able to demonstrate that there were no other means of obtaining the same information in a less intrusive or overt method (e.g., obtaining statements from witnesses where possible) and should evidence as far as reasonably practicable what other methods were considered and why they were not implemented.

"Proportionate"

The exercise is not "Proportionate" if it is excessive in relation to the case. Consideration should be given into the scale of the operation, the methods used and the impact on privacy would be excessive in relation to the allegation.

The proposed methods used in the operation must meet required objective and must not be arbitrary or unfair nor must the impact on any individuals/groups be too severe.

Methods used should be the least invasive needed to achieve the investigation's aims.

"RIPA Legislation":

The Regulation of Investigatory Powers Act 2000 (RIPA), Protection of Freedoms Act 2012(POFA) , the Investigatory Powers Act 2016 (IPA) and other related legislation set out the process to be followed when using covert investigatory techniques.

RIPA Codes of Practise have also been published which must be read and followed.

"*Serious Crime Threshold* "–

The offence being investigated must pass this threshold is Events Data is sought:

- S263(1) of the IPA 2016

  "Serious crime" means crime where—

  (a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or
  (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

"Surveillance":

Surveillance includes:

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

Recording anything monitored, observed or listened to.

Surveillance by or with the assistance of a surveillance device

"The Necessity Test"

Directed Surveillance: the exercise is deemed Necessary if it is to prevent or detect a crime that would attract a maximum prison sentence of at least six months (or underage sale of alcohol or tobacco products)[2]

CHIS: the exercise will be deemed Necessary if it is for the purpose of preventing or detecting crime or preventing disorder

Communications Data: where "Events Data" is sought, it must be Necessary to prevent or detect a "Serious Crime", where "Entity Data" is sought it must be for the purpose of detecting or preventing crime or preventing disorder[3]

[2] Section 7A The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

[3] Section 60A 8 (b) Investigatory Powers Act 2016

Policy

Executive Summary

This policy is designed to give guidance to officers who use or authorise the use of Covert Surveillance in a lawful, Necessary, Proportionate and authorised manner. This will ensure that any evidence gained during an operation is lawful and admissible in Court and meets the aims of the investigation.

The use of investigatory powers by the local authority is governed by Legislation.

The Legislation allows the Council to interfere with the right to private and family life under article 8 of the Human Rights Act 1998 ("Article 8 rights" – see definitions) in limited circumstances that amount to covert surveillance. The use of covert surveillance must be Necessary and Proportionate to the alleged offence.

The Council is committed to implementing the provisions of the Legislation to ensure that any covert surveillance is undertaken properly and lawfully.

RIPA Legislation limits local authorities to using three covert investigation techniques, collectively referred to as Covert Surveillance. The use of Directed Surveillance and CHIS techniques must be authorised internally by an Authorising Officer (AO) and then by a Magistrate.

Directed Surveillance can only be used where Necessary to investigate a suspected crime or disorder with a maximum prison sentence of at least six months or offences related to underage sale of alcohol/tobacco[4] and Proportionate, balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means.

Communications Data can only be obtained where Necessary and Proportionate, and Events Data is subject to the "Serious Crime Threshold".

In the case of Communication Data, the application must be made to the Office of Communications Data Authorisation (OCDA) through an accredited Single Point of Contact (SPoC). The Council accesses theses services through NAFN (National anti-fraud network).

Where unauthorised evidence-gathering interferes with Article 8 rights, and where there is no other lawful authority for it, the consequence may be that the evidence was gathered unlawfully. Courts may therefore disallow the evidence, a complaint of maladministration could be made to the Ombudsman or Investigatory Powers Tribunal, and the Council may have to pay compensation.

---

[4] offences under—(i) section 146, 147, 147A of the Licensing Act 2003 (re sale of alcohol to children) ;(ii) section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen) (iii) section 91 & 92 of the Children and Families Act 2014 (purchase of tobacco, nicotine products etc. on behalf of persons under 18, prohibition of sale of nicotine products).

The Investigatory Powers Act 2016 also introduced new offences in relation to unlawfully obtaining and unlawfully disclosing Communications Data.

The Legislation presents some difficult judgments which must be made from time to time. Whilst individual services can and do operate their own procedures, this is an issue which affects the Council corporately and staff will never be criticised for seeking advice. Legal Services wish to stress that they welcome the opportunity to discuss scenarios with officers, as this is an area in which matters must be decided on a case-by-case basis and scenarios are not static and thus advice and solutions must be kept under review.

Commitment of the Council

The Council will:

1. Obtain judicial authorisation and ensure that any the action is carried out lawfully
2. Put in stringent safeguards against abuse
3. Comply with Legislation and any relevant statutory guidance issued.
4. Provide training for all staff that may use Covert Surveillance, as identified by the relevant Executive Heads of Service
5. Ensure all AOs are suitably trained and that this training is refreshed on an annual basis
6. Monitor its own working practice on a regular basis and review this policy
7. Welcome scrutiny from the Investigatory Powers Tribunal (IPT) and periodic inspections from the Investigatory Powers Commissioner's Office (IPCO).
8. Cooperate fully with the IPT and IPCO and implement any proposals or changes which may be suggested.

Scope of this policy and procedural document

This Policy applies to all employees working for the Council, including those working from home or at non-Council locations. It also applies to councillors, consultants, agency staff and contractors working for the Council and external organisations working with the Council, whilst engaged on Council business. If or where this policy conflicts with any statute, regulation or Code of Practice, those documents take priority over this policy.

This policy applies to the authorisations of Directed Surveillance, sources (CHIS) and acquisition of Communications Data.

Authorisations under RIPA Legislation should be made ***where relevant*** and will only be relevant where the **criteria** listed on the authorisation forms are fully met.

In particular, RIPA Legislation is not relevant to the following activities:

- Covert surveillance by way of an immediate response to events
- Covert surveillance as part of general observation

- Covert surveillance not related to core functions
- Overt use of CCTV and ANPR systems, which are regulated by Data Protection Legislation (includes body-worn cameras[5])

Where RIPA Legislation is not relevant, the Data Protection Legislation is likely to regulate the use and obtaining of any evidence relating to any living individual. In these cases, the officer responsible must carry out a Privacy Impact Assessment (PIA) and seek advice from the Data Protection Officer (DPO).

Governance roles, responsibilities and communication

Senior Responsible Officer (SRO)

The Executive Head of Legal & Democratic Services is the Senior Responsible Officer (SRO) who is responsible for:

- Integrity of processes for management of CHISs and Directed Surveillance and applications for Communications Data
- Compliance with Part 2 of RIPA 2000 and the associated Codes
- Oversight of the reporting of errors to the relevant Commissioner and identification of both the cause(s) of errors and the implementation of processes to minimise the repetition of errors
- Engagement with IPCO inspectors when they conduct inspections
- Engaging with Members - who in accordance with the Code of Practise should review/consider internal reports on use to ensure this is consistent with policy and that the policy remains fit for purpose
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner
- Ensuring appropriate training is available for AOs or relevant staff
- Ensuring that policies are fit for purpose and that AOs are competent.

RIPA Coordinating Officer

Legal Services - Litigation is the RIPA Coordinating Officer. The RIPA Coordinating Officer will:

- Provide a Unique Reference Number (URN) to the Investigating Officer (IO)
- Monitor and keep the central record of authorisations and refusals
- Record the date, time and local of Judicial approval
- Record all renewals and cancellations

[5] Unless specifically directed/targeted to a person - in a planned manner - as part of an investigation then would become Directed Surveillance (if not immediate response)– see example in the Appendices

- Provide advice on the use of covert surveillance
- Provide governance support to the SRO as required or directed
- Maintain a central register of all equipment capable of being used for Directed Surveillance
- Maintain a central register of all training
- Maintain a record and keep copies of agent agreement forms
- Keep a database for identifying and monitoring expiry dates and renewal dates
- Along with AOs and the IOs must ensure that any electronic and paper records relating to a RIPA Legislation investigation are used, retained or destroyed in line with the Council's Information Management policies, departmental retention schedules and the Data Protection Legislation.
- Monitor each department's compliance and act on any cases of non-compliance.

Single Point of Contact (SPoC) for Communications Data

The Council will use the SPoC service provided by the National Anti-Fraud Network (NAFN) each council will have an officer who manages the account.

The SPoC:

- Assesses whether access to the Communications Data is reasonably practical for the postal or telecommunications operator
- Advises applicants and AOs on the practicalities of accessing different types of communications data from different postal or telecommunications operators
- Provides safeguards for authentication
- Assesses cost and resource implications to both the authorisation and postal or telecommunications operator
- Provide quality assurance checks to ensure that applications consistently comply with IPA standards and to a sufficient level to meet OCDA and IPCO scrutiny;
- Monitor those applications which are returned for rework or rejected by OCDA and determine the reasons why;
- Provide organisational and/or individual training as and where necessary sharing best practice advice and support;
- Be the point of contact between public authorities and OCDA; (NOTE: Applicants will not be able to contact OCDA).
- Sends application on to the OCDA for approval

Authorising Officers (AOs)

- The role of the AOs is to authorise, review, renew and cancel Directed Surveillance or use of a CHIS.
- AOs should not be responsible for authorising investigations or operations in which they are directly involved. If this does happen, if urgency requires

it, 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.

- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for local authorities the AO shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.
- A designated AO must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level so as to have an understanding of the Act and the requirements that must be satisfied before an authorisation can be granted.
- The forms to be utilised by AOs can be found in Appendix D
- AO must complete the relevant section on the application form and explain exactly what they are authorising (what is within the application or less), against who, in what circumstances, where etc. It is important that this is very clear as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors. They must explain why the surveillance is Necessary and Proportionate to what it seeks to achieve, taking into account the Collateral Intrusion issues, and that the level of the surveillance is appropriate to achieve the objectives.
- If any equipment such as covert cameras, video cameras is to be used, the AO 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.
- AOs are also responsible for carrying out regular and meaningful reviews of applications which they have authorised and also for the cancellation of authorisations –authorisations should be cancelled when no longer Necessary or renewed in good time and should not be allowed to expire or lapse. AOs should record and retain notes of all decisions
- AOs must acquaint themselves with the relevant Codes of Practice issued by the Home Office and the latest updates in RIPA Legislation. See link in Appendix D (these are the current versions as of June 2023)
- AOs must demonstrate that the proposed activity is Necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment or is an offence relating to the sale of alcohol or tobacco products to minors, when authorising Directed Surveillance. (As to the definition of "detecting crime", see RIPA 2000 section 81(5).)
- AOs also need to consider if confidential information will be gained, (see definitions section) in which case the matter must be referred to the Chief Executive
- AOs must also satisfy themselves that the application is Necessary and Proportionate in the particular circumstances – taking into account Article 8 Rights and Collateral Intrusion. (See definitions section)

- The ICPO envisages that the AO will make the judicial application (although his may not always be possible, and can be delegated to IO or Legal Services)

Investigating Officers (IOs)

- IOs should think about the need to undertake Directed Surveillance or CHIS before they seek legal advice with a view to authorisation. IOs need to consider whether they can obtain the information by using techniques other than covert surveillance. There is nothing that prevents an IO discussing the issue of surveillance beforehand and this policy requires officers to discuss with Legal Services.
- IOs may need to:
  1. Identify the objective(s)
  2. Describe the nature of the surveillance and identities (if known)
  3. Provide supporting information and intelligence
  4. Conduct location research and feasibility study
  5. Identify Collateral Intrusion and detail how to manage this
  6. Consider who, what why where when and how
  7. Detail why the activity is Necessary and Proportionate
  8. Prepare risk assessments
- IOs must ensure a feasibility study has been conducted as this may be required to be seen by Legal Services and the AO. 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.
- The form should then be submitted to the AO for authorisation who must also take advice from Legal Services.

Training

The SRO is responsible for ensuring relevant members of staff are suitably trained as AOs and IOs so as to avoid common mistakes appearing on forms for RIPA Legislation authorisations.

Training will be given, and completed, before AOs are certified to sign any authorisation forms. A certificate of training will be provided to the individual and a central register of all those individuals who have had training, will be kept by the RIPA Coordinating Officer.

This training must be refreshed annually.

Activities by other Authorities

Care is needed to ensure that there is no conflict between the activities of this Council and other public authorities. The IO should make enquiries of other authorities (such as the police) to find out whether they are carrying out similar activities if he/she considers that there is such a possibility.

Joint Investigations (collaborative working)

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA Legislation, this document and the forms in it,

must be used (as for the normal procedure) and the agency advised or kept informed of the various requirements. They must be made aware explicitly of what they are authorised to do.

They must also fill out the Agent's agreement form, found in the Appendices, a copy of which should be passed to the RIPA Coordinating Officer.

When another agency (e.g., the Police, HM Revenue & Customs) wishes to use the Council's resources or premises, that agency must use their own Covert Surveillance procedure and forms and a copy should be passed to the RIPA Coordinating Officer.

If the police or other agency wish to use Council resources for general surveillance (as opposed to specific covert investigations), they must request this in writing. This must include remit, duration, details of who will be undertaking the general surveillance and the purpose of it before any Council resources are made available.

A copy of the letter must be sent to the RIPA Coordinating Officer for the central record.

Complaints

Complaints about Covert Surveillance should be made under the Council's Corporate Complaints Policy.

The SRO may review the conduct of particular operations at any time.

Review of this policy and procedure

RIPA Legislation and this document are important for effective and efficient operation of the Council's actions on surveillance. Therefore, the SRO will keep this document under review. AOs must bring any suggestions for continuous improvement of this document to the attention of the SRO at the earliest possible opportunity.

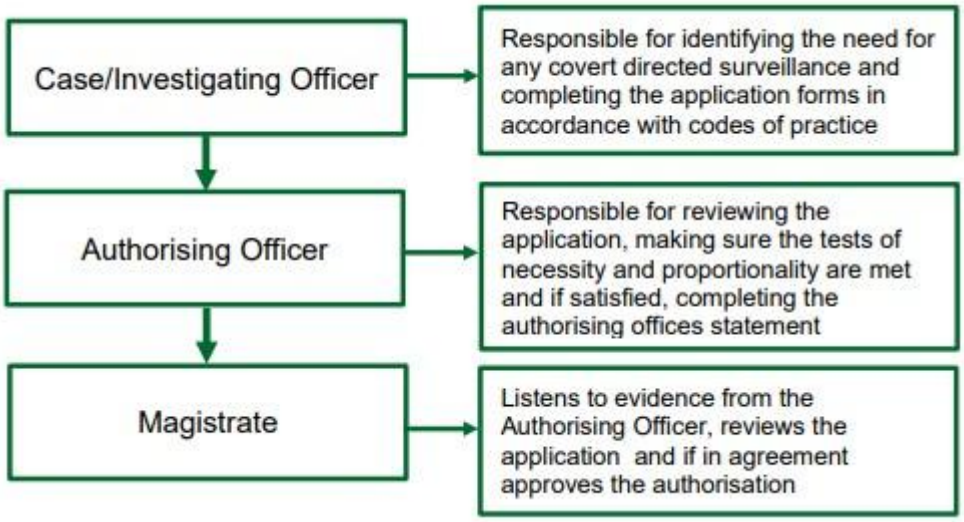
This policy will be reviewed by the Corporate Governance and Standards Committee at Guildford and then go before the full council for approval.

The SRO will review the policy every year in consultation with the Committees above.

Part 2 – Procedure

Summary of the authorisation procedure

Three individuals are involved in granting authorisation for covert **Directed Surveillance and the use of a CHIS**:



The following is an overview of the authorisation procedure.

IOs must obtain a unique reference number from the RIPA Coordinating Officer (Legal Services) for any planned, covert operation for which they intend to apply for authorisation.

Directed surveillance

For Directed Surveillance and use of CHIS , IOs must submit the application form for Directed Surveillance (latest version found on the internet)to a designated AO – There is a list of those eligible to act as AOs at Appendix A, but as eligibility will also depend on having completed the training, please contact the Legal Team for a list of AOs when needed.
Where a likely consequence of surveillance is the acquisition of Confidential Material[6], the IO must, always seek authority from the Chief Executive.
Applications for the renewals and cancellations of surveillance must be authorised by the same AO where possible.
Once authorised, the AO will ensure that the administration at the Magistrates Court is contacted (email: SurreySussexMC@justice.gov.uk.) to arrange a hearing for judicial approval. The current application for judicial approval form as published by the Home Office, must be used for this purpose.[7]

[6] See definitions section

[7] See Appendix D

Authorisation of surveillance

Activity requiring authorisation

INTRUSIVE SURVEILLANCE	DIRECTED SURVEILLANCE	COVERT HUMAN INTELLIGENCE SOURCE
Council cannot authorise	Authorisation needed	Authorisation needed

Authorisation is required for the following activities:

Directed Surveillance
Use of sources (CHIS)
The acquisition or disclosure of Communications Data

Officers conducting investigations on the Council's behalf must seek authorisation in writing for Directed Surveillance and use of CHISs. In the case of Communications Data, they must make a colleague of AO Level or above aware when submitting the application through the NAFN.

The authorisations must be set out on the latest forms : RIPA forms - GOV.UK (www.gov.uk) Home Office forms which should not be adapted or modified unless authorised by the SRO.

Unique Reference Numbers (URNs)

Each application for authorisation must have a Unique Reference Number (URN). The officer applying for authorisation must first obtain the next available URN from the RIPA Coordinating Officer. Rejected forms will therefore also have URNs.

Authorising Officers (AOs) – roles and responsibilities

Once an application in relation to Covert Surveillance has been received, the AO should consider the form and undertake the Necessity Test. The AO must complete the relevant section of the form explaining why in his/her opinion the surveillance is Necessary and Proportionate and that any Collateral Intrusion has been considered. They should also detail the exact activity being authorised, who against etc. in the relevant authorisation section on the form.

Authorising the acquisition of Confidential Material

If the application is for Confidential Material, the IO must seek authority from the Chief Executive. The fullest consideration must be given to any cases where the subject of the Surveillance might reasonably expect a high degree of privacy.

Applications where the Surveillance could result in the acquisition of Confidential Material will be considered only in exceptional and compelling circumstances. The IO and the Chief Executive must have full regard to the proportionality issues this raises.

Authorising the acquisition of Directed Surveillance

Surveillance is only covert if it carried out in a way calculated to ensure the subject specific investigation is unaware of it. RIPA authorisation is required for Covert Surveillance undertaken in a way likely to result in private information being obtained. It is not Directed Surveillance if it is in immediate response to events.

The AO must ensure that the Directed Surveillance has passed the Necessity test. The exercise is deemed Necessary if it is to prevent or detect a crime that would attract a maximum prison sentence of at least six months (or underage sale of alcohol or tobacco products).[8]

The AO must also consider if the Directed Surveillance is Proportionate and any associated Collateral Intrusion.

Local Authorities are not permitted to undertake Intrusive Surveillance (see definitions section). Operatives will have to take particular care when using surveillance devices that Directed Surveillance does not become Intrusive (i.e., if device can see inside a property or car with the detail and quality that would be expected were the device present inside these places)

Authorisation for the use of sources (CHIS)

Prior to authorising the use of a CHIS, the AO must be satisfied that the operation is Necessary for the purpose of preventing or detecting crime or preventing disorder. They must then consider the use to be Proportionate and any associated Collateral Intrusion.

A source may include those referred to as agents, informants and officers working undercover.

Whilst the council is not in the practise of using CHISs, arrangements must be in place and Legal Services should be consulted should the event arise. There may also be situations where a person who is not originally a CHIS becomes one, so officers need to be alert to this fact.

The AO shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The AO shall carry out a risk assessment **before** authorising the source. The assessment should include provisions for the source's safety and welfare, and as such should be updated throughout the duration of the authorisation.

The person responsible for the day-to-day contact between the public authority and the source should be named in the application

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out.

---

[8] Section 7A The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

The use of a CHIS may only be authorised if arrangements are in place including the following:

- That there will at all times be an officer 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).
- 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).
- 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; and
- That the records relating to the source maintained by the council will always contain particulars as laid down by the CHIS codes of practice

Only the Chief Executive can authorise the use of vulnerable individuals and juvenile sources. The Chief Executive shall consider the special safeguards or provisions applying to vulnerable individuals and juvenile sources, as set out in Cover Human Intelligence Sources revised Code of Practice, which sets out that:

(a) security and welfare should be taken into account when carrying out actions in relation to an authorisation or tasking including foreseeable consequences to others
(b) a risk assessment should be carried out before authorised to determine risk to source of tasking consequences should their role become known
(c) the person responsible for the source's welfare and security should bring to the AO's attention any concerns. Where appropriate concerns about security / welfare matters should be considered by the AO and a decision made on whether the authorisation should continue.

If a source is under 16 years, please seek advice from Legal Services as different and more stringent provisions apply

If instructing an agent to be the CHIS, the agent must complete and sign the form marked "Agent's Agreement Form" contained in Appendices. The agent will be subject to RIPA Legislation and this policy in the same way as any employee of the Council would be. They may also be inspected by the IPCO in respect of each particular operation. This should be pointed out during the instruction and contract stage. Advice should be sought from Legal Services.

Once authorised by the AO any application for use of a CHIS will need judicial approval.

Communications Data

Procedural guidance for obtaining authorisation from the OCDA is available here: NAFN Investigatory Powers Act Guidance Booklet.pdf (local.gov.uk)

The application forms are now completed electronically via the CycComms portal
The IO completes the application on the CycComms Portal.
Prior to an IO submitting an application for Communications Data they will discuss the investigation and the necessity / proportionality for the request with

an AO or the Chief Executive. Thereafter the application will be scrutinised by the SPOC before being submitted to OCDA for approval. Anyone completing these forms can be given guidance.

An AO or Chief Executive must be made aware of the application and must endorse the form to this effect.

There is no longer need for judicial approval, except in cases where journalistic source materials are sought -where the application will be referred to a Judicial Commissioner within the IPCO.

Where cases are novel or contentious an officer of at least the rank of SRO must be aware of the application.

Local authorities are now only allowed to seek Entity and Events Data.
Where Events Data is being sought to detect crime, that crime must meet the Serious Crime Threshold. The application must also pass the Necessity Test and be deemed Proportionate as well as giving consideration to any possible Collateral Intrusion.

NAFN will provide an annual return to the SRO so that they can comply with their reporting and submission duties.

IOs must keep records of their investigation in line with established retention periods. This includes copies of any Communications Data applications that have been made electronically.

Forms will remain on the central record for six years from date of cancellation.

Acquisition of Communications Data

The Investigatory Powers Act 2016 ('IPA') allows for the Council to acquire Communications Data from telecoms and postal operators via an authorisation procedure. Communications Data can include Entity Data or Event Data.

It does not include the content of the communications. The Council has no right to listen in to phone conversations without permission or read post or electronic communications before they have been received.

A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

Where "Events Data" is sought, it must be Necessary to prevent or detect a "Serious Crime", where "Entity Data" is sought it must be for the purpose of detecting or preventing crime or preventing disorder[9]

Communications Data, and all copies, extracts and summaries of it must be handled and stored securely.

[9] Section 60A 8 (b) Investigatory Powers Act 2016

Officers must observe the requirements of the Data Protection Legislation and the principles of the Criminal Procedure and Investigations Act 1996. Officers must seek advice from the Data Protection Officer (DPO) when they have questions about information security and integrity.

The Home Office has issued guidance to support the Communications Data codes of practise, both can be accessed here: Investigatory Powers Act 2016 – codes of practice - GOV.UK (www.gov.uk) This policy must be read in conjunction with the Code and all staff involved in the acquisition of Communications Data must have regard to the provisions.

Applications must be made through NAFN. The local authority making the application must ensure someone of at least the rank of AO in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA.

NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

Please contact the RIPA Coordinating Officer, DPO or an AO for more information.

Social Media

In some investigations, social media sites can form a useful source of intelligence. Usually, a review of open-source sites will not need authorisation. However, if reviews are carried out on the same individual with some regularity, this may amount to Directed Surveillance and authorisation should be obtained.

Please see Appendix B "Use of Social Media in Investigations – Procedure and guidance note" for more detail and information on what permitted

Duration, reviews, renewals and cancellation of authorisations

Duration

Authorisations last for:

- Three months from date of grant or latest renewal for Directed Surveillance
- Twelve months from date of written grant for the conduct or use of a source (NB: Juvenile Sources (CHIS) 1 Month)
- One month from date of written notice or authorisation for Communications Data, or earlier if cancelled

Officers should note that the authorised period starts from the date authorisation is granted, not from the date the surveillance begins.

Authorisations must not expire. They must be kept under review, and then renewed or cancelled if no longer required.

Reviews

AOs must review the operation by the date he/she has entered on the authorisation form (or latest renewal, if applicable). The review's purpose is to assess the need for the surveillance to continue, considering the specific circumstances and sensitivities of the investigation. They must cancel the authorisation if no longer needed.

AOs should record review results on the standard review form and add a copy to the central authorisations record held by the RIPA Coordinating Officer.

Where the Surveillance provides access to Confidential or sensitive Information or involves Collateral Intrusion the officer should conduct reviews more frequently.

Cancellations

An AO must cancel an authorisation as soon as it is no longer Necessary, or no longer Proportionate to the objective. The duty to cancel a notice falls on the AO who issued it.

This applies to both original applications and renewals.

Authorisations must also be cancelled if the Surveillance has been carried out and the original aim has been achieved.

A copy of the original cancellation form must also be sent to the RIPA Coordinating Officer. The standard Home Office cancellation forms should be used and is available here:

RIPA forms - GOV.UK (www.gov.uk)

Renewals

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

Authorisations can be renewed shortly before the maximum period has expired. The renewal will begin on the day the authorisation would have expired. Where renewals are timetabled to fall outside of court hours, it is the AO's responsibility to ensure the renewal is completed ahead of the deadline. (Not more than 7 working days before)

An AO must still consider all of the issues that are required for a first application before a renewal can be granted. Each renewal will need the approval of a Magistrate.

If the reason for requiring authorisation has changed from its original purpose it will not be appropriate to treat the application as a renewal. The original authorisation should be cancelled, and a new authorisation should be granted.

The AO and applicant should retain a copy of the renewal and the judicial application/order form. A copy of the original renewal form and the judicial

application/order form must also be sent to the RIPA Coordinating Officer for the central register.

An authorisation cannot be renewed after the authorised period has expired. In this case the AO must cancel the authorisation and consider the matter afresh.

Renewal forms are available here: RIPA forms - GOV.UK (www.gov.uk)

Judicial Approval

Judicial Approval is required for Directed Surveillance and the use of a CHIS.

The AO should contact HM Courts & Tribunals Service at the Magistrates' court to arrange a hearing and may delegate this to the IO or Legal Services.

The hearing is a legal proceeding, so officers must be formally designated to attend, be sworn in and present evidence or information as required. It is envisaged that the AO will usually attend as they will have the detailed knowledge of why the application was deemed Necessary and Proportionate, but it is understood that sometimes the IO will attend. However, it is important to note that the forms and supporting papers must, by themselves, make the case for authorisation. Legal Services are happy to assist if necessary.

The Magistrate should have sight of the authorisation form and the supporting documents setting out the case – including all information the authorisation relied on. The Council must retain the original documentation.

The Magistrate must be sent a partially completed judicial application form and will complete the form's order section, which will then be the official record of the Magistrate's decision.

The hearing will take in private (closed to public) and can be conducted by one Magistrate

Reporting Errors

There is a requirement to conduct regular reviews and report all covert activity that was not properly authorised to the (IPCO) in writing as soon as the error is recognised. An "error" includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the AO. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply and the notification should be made as soon as practicable.

This will require a report detailing any remedial action taken, including details of the cause, material obtained, unintended Collateral Intrusion, whether material destroyed or retained, and summary of steps taken to prevent recurrence. The Council also has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is

to confirm that any direction provided by the IPCO has been followed. This will also assist with the oversight provisions of the Council's RIPA Legislation activity.

'The Reporting Errors Form' in Appendix D should be used for this purpose.

This does not apply to Covert activity which is deliberately not authorised because an AO considers that it does not meet the legislative criteria but allows it to continue. This would be surveillance outside of RIPA Legislation and should be recorded by the AO on a Sub-RIPA form.

The central record

The RIPA Coordinating Officer will maintain a central register of Covert Surveillance and use of sources in order to comply with legal requirements and for quality assurance.

AOs must ensure that copies of the following are included in the Council's central record:

- Authorisation Forms (whether or not the authorisation is granted or refused)
- Review forms/Renewal forms
- Cancellation forms

The central record shall contain the following information for each case:

- The type of authorisation or notice
- The date the authorisation or notice was given
- Name and rank/grade of the AO
- The unique reference number (URN) of the investigation or operation
- Title of operation, including brief description and names of subjects, if known
- If the authorisation or notice is renewed, when it was renewed and who authorised renewal, including name and rank/grade of the AO
- Whether the operation is likely to result in obtaining confidential information
- The date the authorisation or notice was cancelled
- Where and when a Justice of the Peace or Magistrate has granted authorisation

These records will be retained for at least six years from the ending of the cancellation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

AOs must provide the relevant forms to the RIPA Coordinating Officer within one week of the authorisation, review, renewal, cancellation or rejection.

AOs must ensure that any forms, sent through internal post, are in sealed envelopes using the security measures required for documents classified as “Official-Sensitive”.

This record will be monitored, and appropriate advice given from time to time. It will also be made available to the relevant Commissioner or an Inspector from the IPCO.

IOs must retain the original form with the investigation’s working file.

Records retention and destruction

Retention of material obtained through surveillance

Arrangements must be in place for handling, storage and destruction of material obtained using Directed Surveillance, a CHIS or Communications Data. The AO must make the following arrangements to protect the material:

- A named officer responsible for retaining the data and disposing of it securely.
- Physical, technical/organisational measures must be in place to prevent unauthorised access to, and use of the data obtained by the surveillance.
- Physical, technical/organisational measures must be in place to prevent accidental/unauthorised loss of data obtained by the surveillance exercise.
- AOs must ensure compliance with data protection and local documented working procedures relating to the handling and storage of material.
- Material obtained from properly authorised surveillance, or a source may be used in other investigations. Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.
- This applies to material which points towards or away from the suspect and the fact that the subject of the investigation may see the documents on later date should be borne in mind in the drafting of applications/findings
- Communications Data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose. When it is no longer Necessary or Proportionate to hold such data, all copies of relevant data held by the public authority must be destroyed. Data must be deleted such that it is impossible to access at the end of the period for which it is required.
- Information obtained through Directed Surveillance or a CHIS, 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 an

authorised purpose (as outlined in relevant code of practise). 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.

- The AO must review whether the information should be disposed of or kept for a further length of time.
- The AO should take into consideration the status of any legal proceedings connected to the operation and the likelihood of any future legal action (including action taken by the subject(s) of the surveillance).
- The justification for any decision to keep the information must be documented and kept with the file.

The following documents must be kept, but need not form part of the central record:

- Supplementary documentation and notification of AO's approval
- Supporting documentation submitted when a renewal is requested
- Date and time when any instruction is given by the AO

Covert Human Intelligence Source Records (CHIS)

IOs must keep proper records of the authorisation and use of a source. Please see the Code of Practise for more details: Covert Human Intelligence Sources code of practice 2022 - GOV.UK (www.gov.uk)

The records must contain information as to identity, security and welfare, risk assessments, recruitment information, handlers and controllers, tasks allocated, communications and all information given to or obtained from the source.

If any officer is unsure about the provisions of the Legislation or have questions about the use of Covert Surveillance techniques, please contact Legal Services

Part 3 - Appendices

Appendix A: Authorising officers

Please check with the Legal Department for the most up to date list of AOs.

Table 1: Names of SRO and Authorising Officers (subject to training being completed)

Designation	Name
Joint Chief Executive	Must authorise any operations using juveniles and any operations where confidential information is likely to be obtained
Senior Responsible Officer (SRO)	Joint Executive Head of Legal & Democratic Services (Monitoring Officer)
Authorising Officer 1	Joint Strategic Director, Community Wellbeing
Authorising Officer 2	Joint Strategic Director, Place
Authorising Officer 3	Joint Strategic Director, Transformation & Governance
Authorising Officer 4	Joint Executive Head Community Services
Authorising Officer 5	Joint Executive Head, Housing Services
Authorising Officer 6	Joint Executive Head, Planning Development
Authorising Officer 7	Joint Executive Head, Regulatory Services
RIPA Coordinating Officer	Legal Services – Litigation Lawyer

Appendix B:

Use of Social Media in Investigations - Procedure and guidance note

A guide to the Council's approach to the use of social media in relation to Regulation of Investigatory Powers Act 2000 investigations.

Social Media guidance

This guidance sets the framework on which the Council may utilise Social Media when conducting investigations into alleged offences. Whilst the use of Social Media to investigate is not automatically considered Covert Surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of Covert and/or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the provisions of the RIPA 2000, as it relates to Directed Surveillance and use of a CHIS, are followed at all times when using Social Media information in investigations. Otherwise, any evidence obtained may become inadmissible

It is recognised that the use of the internet and, in particular, social networking sites such as Facebook, can provide useful information for council staff carrying out investigations or gathering evidence when dealing with service users. However, accessing an individual's or company's internet and social networking sites may potentially fall within the definition of Covert Directed Surveillance, which would require authorisation to be sought from a Magistrates Court.

Failure to seek authorisation, when necessary, could result in the Council breaching Article 8 Rights. It is therefore important that officers adhere to the Council's policy and this guidance when considering accessing internet and social networking sites as part of an investigation or to gather evidence.

Process to be followed when considering using Social Media or Social Networking Sites in Investigations

Where an officer considers it necessary to view a social networking site to investigate an allegation or an individual, the process to be followed is:

1. Before viewing any social networking site, the officer must seek the approval of their direct line manager.
2. Officers must not use their own personal or private account when accessing social networking sites for investigations/evidence gathering, only Council accounts should be used.
3. Officers may access the main page of an individual's profile to take an initial view as to whether there is any substance to the allegation of the matter being investigated. The initial viewing must be reasonable, for example, it would not be reasonable to spend any significant amount of time searching through various pages of an individual's profile or to print out several pages just in case they may reveal something useful.

4. The DPO maintains a log recording when social networking sites are viewed for investigations/evidence gathering. Each single viewing of a company or individual's social networking site must be recorded on the log This is to enable the Council to monitor the use of these sites for investigations/evidence gathering and use this information to review policies and guidance.
5. If it is considered that there is a need to monitor a company's or individual's social networking site, then the officer must refer the matter back to their line manager for consideration as to whether the activity constitutes Covert Surveillance. If officers are in any doubt as to whether an authorisation is required, they should seek advice from Legal Services before continuing to access a social networking site.
6. If the offence being investigated falls under RIPA Legislation, a formal Covert Surveillance application must be completed, authorised by one of the Council's AOs and then approved by a Magistrate.
7. If the offence being investigated falls outside of RIPA Legislation, a 'Sub-RIPA form must be completed and forwarded to the RIPA Coordinating Officer to be added to the log.

What is meant by 'Social Media' for the purposes of this guidance note:

Social Media, sometimes also referred to as a Social Network, can take many forms. Therefore, it can be difficult to provide a definitive list of sites.

Social Media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, Social Media can be diverse, but will often have some, or all, of the following characteristics:

- An ability to show a list of other users with whom they share a connection; often termed "friends" or "followers".
- An ability to view and browse their list of connections and those made by others within the system.
- Host capabilities allowing users to post audio, photographs and/or video content that is
- viewable by others.
- Social Media can include community-based web sites, online discussions forums, chatrooms and other social spaces online.

Current examples of the popular forms of Social Media include (this list is not exhaustive and new forms can be created and others may vary or wain in popularity):

- Facebook
- Twitter
- Instagram
- LinkedIn
- Pinterest
- Tumblr

- Reddit
- Flickr
- Instagram
- Tiktok
- Snapchat
- Online dating websites

The definition of 'private information' under RIPA 2000 includes:
"any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships."

Privacy settings
The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy, or otherwise indifferent about who is able to view their information, others prefer to maintain a level of privacy.

Depending on their intentions, many users will purposely use Social Media with no privacy setting applied whatsoever. This could be due to the fact that they are actively promoting something, such as a business or event, and therefore require as many people as possible to be able to view their Social Media profile at all times; others may do so for reasons of self-promotion.

The information publicly available is known as an individual's public profile and the information is "open source".

Persons who operate public profiles on Social Media without any, or only limited, forms of privacy settings do so at their own risk.

Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain.

A private profile is one set up on Social Media where an individual sets privacy settings to limit their content, information or interactions according to their requirements.

By setting their profile to private, a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act.

What activity is permitted under this policy
For individuals who do have a presence on Social Media, a lot of what is permitted under this policy for use in investigations will depend on whether they have a public or private profile.

In practice, this means that photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any Social Media platform can be viewed, recorded and ultimately used as evidence in legal proceedings, subject to the usual rules of evidence.

When considering what is available on an individual's public Social Media profile, those investigating an offence, or potential offence, should always keep in mind what relevance it has to that investigation. Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, should be gathered. If there is any doubt as to whether something is relevant, then advice should be sought from Legal Services.

What is not permitted under this policy

When it is discovered that an individual under investigation has set their Social Media account to private, Officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to:

- sending "friend" or "follow" requests to the individual
- setting up or using bogus Social Media profiles in an attempt to gain access to the individual's private profile
- contacting the individual through any form of instant messaging or chat function requesting access or information
- asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the Social Media accounts of such people to gain access, or
- any other method which relies on the use of subterfuge or deception

Officers must not use their own personal or private account when accessing social media sites for investigation and evidence gathering purposes. Only Council accounts should be used. Interaction and conversations of any kind should be avoided.

Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be traced through tracking of IP Addresses, and other electronic identifying markers.

One off visits or infrequent visits to an individual's Social Media profile spread over time cannot be considered "Directed Surveillance" for the purposes of RIPA Legislation. Repeated or frequent visits may cross over into "Directed Surveillance" requiring RIPA Legislation authorisation.

A person's Social Media profile should not, be routinely monitored on a daily or weekly basis, as this will require RIPA Legislation authorisation. If an officer requires more advice on this, they should contact Legal Services for advice.

Each viewing of a company or individual's social media profile for the purpose of

investigation or evidence gathering must be recorded on the case log.

Capturing evidence

Once content available from an individual's Social Media profile has been identified as relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution.

Where evidence takes the form of readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way.

Where evidence takes the form of audio or video content, then efforts should be made to download onto a hard drive or some other storage device such as a CD or DVD. Those should then be exhibited to a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of the Council's IT Team.

When capturing evidence from an individual's public Social Media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's Social Media profile, the Council Officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, in relation to a specific status update or post published on the individual's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.

When capturing evidence from a Social Media profile, steps should be taken to minimise Collateral Intrusion of inadvertently capturing third party information - either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on Social Media profiles promoting certain events, where users interact with each other by posting messages or photographs where they may make comments.

Retention and destruction of information

Where recorded material (in any form or media) 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 the Data Protection Legislation, the Freedom of Information Act 2000, CPIA and any other legal requirements, including those of confidentiality, and the Council's policies and procedures on document retention. Advice should be sought from the Data Protection Officer or Legal Services.

Personal data gathered by the Council is subject to the Data Protection Legislation. When considering whether to retain the data, the Council should:

- review the length of time it keeps personal data;
- consider the purpose(s) it holds the information for in deciding whether (and for how long) to retain it;
- securely delete information no longer needed for these purposes; and
- update, archive or securely delete information if it goes out of date

Due to the nature of Social Media, it is important to remember that when information produced as a hard copy is destroyed in line with this paragraph, that all digital copies of that evidence is likewise destroyed.

Appendix C: Examples to help you decide whether your activities are covered by this policy

Firstly, consider:

- Is it necessary for the operation to be Covert? Could you obtain the evidence without Covert Surveillance? AOs should consider this very seriously because, if found that there was no need for Covert surveillance, the invasion of privacy may be deemed disproportionate to the investigation.
- Overt investigations (i.e., not done in a way calculated to ensure the subject is unaware of the operation) is not subject to the authorisation procedures in this policy. Overt activity includes (but is not limited to) routine patrols, observation at trouble spots, immediate response to events and overt use of CCTV.

Examples:

Does the investigation involve the collection of private information?

Example 1:

Two people talking on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation even though they are associating in public. The conversation should be considered as private information.

The offence under investigation would need to meet the minimum penalty criteria and a Directed Surveillance authorisation would be necessary to listen in to or record the conversation as part of a specific investigation or authorisation. (Source: *Covert Surveillance & Property Interference Revised Code of Practice 2018*)

Example 2:

A surveillance officer intends to record a specific person giving their name and phone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation.

Although the person has disclosed these details in a public place, there is reasonable expectation that the details are not being recorded separately for another purpose. Before proceeding, the IO should make sure the alleged offence meets the minimum penalty criteria and seek a Directed Surveillance authorisation. (Source: *Covert Surveillance and Property Interference Revised Code of Practice 2018*).

Planning Enforcement

Example 3:

Routine activities such as Enforcement Officers looking at new building work, which has not been granted planning permission.

This is not Directed Surveillance but falls under normal enforcement duties. RIPA 2000, section 80 provides a general saving for collecting information by lawful means such as this. However, such routine activities should not develop into Directed Surveillance.

Example 4:

Officers wish to drive past a café to obtain a photo of the exterior.

This is unlikely to require a Directed Surveillance authorisation. However, if the exercise was to establish a pattern of occupancy of the premises by someone, the accumulation of information is likely to result in private information. In the latter case, a Directed Surveillance authorisation would be required, and the offence would need to meet the minimum penalty requirements. (*Covert Surveillance Revised Code of Practice 2018*).

Example 5:

You are conducting a site visit in response to a report from a member of the public who suspects a change of use of land, which is likely to involve criminal activity. The circumstances suggest you will need to monitor the site covertly and are likely to obtain private information about the owner and/or collateral information about other users of the site such as workers.

This activity appears to fall within the Directed Surveillance. However, it is not legal to use Covert Surveillance to investigate crimes that would attract a custodial sentence with a minimum term of under six months (unless related to underage sale of alcohol or tobacco). You must therefore find an overt method of dealing with the offence.

Example 6:

You are unable to gather conclusive evidence that illegal activity is taking place on site, but you still suspect that it is. Therefore, you decide to observe the site by driving past it periodically over the next fortnight. If you see unauthorised work taking place you will take a photo – but not covertly.

This does not appear to fall within the definition of either Directed or Covert Human Intelligence Sources. This low-level activity is not subject to the authorisation procedures set out in this policy.

Benefit Fraud

Example 7:

You are investigating an allegation that Mr X is claiming housing and council tax benefit even though he has been working full time for some years. Mr X did not declare on his benefit application that he had been working. You therefore intend to covertly observe him at his alleged employer's address in order to establish if he is working there. The observation will be from a vehicle and will cover a number of days.

This appears to involve systematic surveillance of an individual and falls within the definition of Directed Surveillance, as set out in Appendix B, for the following reasons:

- The surveillance is being carried out for the purposes of a specific investigation into Mr X's alleged benefit fraud.
- The surveillance is of Mr X's personal activities and is therefore likely to produce private information about him.
- The exercise is not an immediate response to events but has been planned in respect of timing and the way in which the surveillance is to be carried out.
- It is likely that collateral material will be gathered

Employer Responsibilities

Example 8:

Recurrent thefts from staff are taking place and after considering the options, it has been suggested that the only recourse is to set up a secret camera covering the work area to catch the culprit "in the act".

Normal business practice (i.e., the responsibilities that all employers would have in relation to staff) are outside of the RIPA Legislation controls. Therefore, the operation would need to be conducted in accordance with the Data Protection Legislation and the Privacy Impact Assessment (PIA) provisions. Use the PIA template available on the Intranet.

You must consider all of the circumstances of the case. But where the aim is to stop the offending behaviour, overt measures (e.g., overt CCTV) may be more Proportionate.

Please note that if a crime on Council premises were being investigated by the police and they are conducting the surveillance, they would be required to authorise the surveillance, not the Council.

Example 9:

A manager has received a report from employee A that employee B is spending hours surfing the internet. The manager requests a printout of employee B's websites visited and times spent on the internet to check whether the allegations are true.

As with the scenario above, this investigation would fall outside RIPA Legislation provisions. The Council has arrangements to ensure any staff investigations involving ICT equipment are necessary and Proportionate. Please use the Council's Privacy Impact Assessment form.

Please note that automatic, untargeted central monitoring of internet/email use carried out by ICT software, which would highlight infringements of the Council's Acceptable Use Policy is allowed under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Housing Management

Example 10:

A member of the public reports that their neighbour's garden is a health hazard. You visit the site, which contains excessive rubbish and materials clearly likely to be an environmental hazard to the community. As the tenant is not at home, you

photograph the view of the garden from the road. You have not deliberately planned the photo to be taken without the tenant's knowledge and any future surveillance of the site will not be carried out in a manner calculated to ensure that the tenant is unaware of it.

This does not appear to fall within the definition of either Directed Surveillance or Covert Human Intelligence Sources as set out in Appendix A and is therefore not subject to the authorisation procedures in this policy. However, care will be required if photos are taken whilst on the premises as this may in some cases become "Intrusive Surveillance", which the Council does not have the authority to carry out.

If you gather personal data (i.e., that can be used to identify someone), this will be subject to the Data Protection Legislation and would be subject to a Privacy Impact Assessment.

Example 11:

You have received an application for housing by someone claiming to be homeless. However, you have grounds to believe that the claim is fraudulent, so you wish to carry out surveillance of the claimant's suspected residence to establish the truth.

This appears to fall within the definition of Directed Surveillance, as set out in Appendix B, for the following reasons:

- The surveillance is for the purposes of a specific investigation into a fraudulent application.
- The surveillance is likely to produce private information on the applicant as well as collateral information about third parties.
- The exercise is not an immediate response to circumstances but has been planned in respect of timing and the way the surveillance is to be carried out.

However, you would need to consider whether the offence is listed on the statute book as attracting a minimum custodial sentence of six months or more before proceeding with the covert elements of the investigation and applying for authorisation.

Use of CCTV

Example 12:

An officer receives information that an individual suspected of Benefit Fraud will be going to their workplace, in the High Street and within an area monitored by CCTV. The officer wishes to use the CCTV to obtain evidence that the suspect is working.

This is targeted use of the town centre's overt CCTV system, to conduct surveillance against that individual without his knowledge. The IO would need to apply for an authorisation for Directed Surveillance.

If you are investigating a serious criminal matter and you are unsure if your surveillance activity falls under RIPA Legislation, you should apply for authorisation in order to avoid any claim that the Council has infringed anyone's Human Rights, which could disqualify the evidence from being permitted in court.

Appendix D: Forms

Please check you are using the correct forms. The latest versions of the forms listed below should be downloaded from the Home Office.

RIPA forms: RIPA forms - GOV.UK (www.gov.uk)

Application for use of Directed Surveillance - application-directed-surveillanc.doc (live.com)
Review of use of Directed Surveillance - review-directed-surveillance.doc (live.com)
Renewal form for Directed Surveillance - renewal-directed-surveillance.doc (live.com)
Cancellation of use of Directed Surveillance - cancellation-directed-surveillan.doc (live.com)
Application for the use of covert human intelligence sources (CHIS) - chis-application.doc (live.com)
Reviewing the use of covert human intelligence sources (CHIS) - chis-review.doc (live.com)
Renewal of authorisation to use covert human intelligence sources (CHIS) - chis-renewal.doc (live.com)
Cancellation of covert human intelligence sources (CHIS) - chis-cancellation.doc (live.com)

Application to Magistrates: approval-order-form.doc (live.com)

Coded of Practice can be accessed here :RIPA codes - GOV.UK (www.gov.uk)

Error reporting form can be accessed through IPCO or here :IPCO Error Report Form.pdf

NAFN website can be accessed here: NAFN - National Anti-Fraud Network

Agents Agreement Form - Please see Page 39

REGULATION OF INVESTIGATORY POWERS ACT 2000

AGENT'S AGREEMENT FORM

I ……..(insert Agent's name)

of

……..(address)

confirm that in relation to

……

……..

……..

……..

……

……

……(name or description of the surveillance)

I agree to comply with the Regulation of Investigatory Powers Act 2000, with all statutory provisions, statutory Codes of Practice and with Waverley and Guildford Borough Council's Policy and Social Media Guidance when undertaking any and all surveillance authorised by Waverley or Guildford Borough Council under the Regulation of Investigatory Powers Act 2000.

I acknowledge receipt of a copy of the Council's Authorisation Form reference number ……..dated the…….

and I agree not to carry out any surveillance that is contrary to this authorisation.

Signed……Dated……
……..

Covert Surveillance and Investigative Powers Policy and Procedure agreed and signed by:

Executive Head of Legal & Democratic Services Guildford and Waverley Borough Councils