Surveillance Policy

1.1 Policy Statement

1.1.1 This policy is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources (CHIS) and access to communications data.

1.2 Background

1.2.1 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Amongst the qualified rights is a person's right to respect for their private and family life, home, and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of surveillance.

1.2.2 Part II of the Regulation of Investigatory Powers 2000 Act provides a statutory framework under which covert surveillance activity undertaken by the Council can be authorised and conducted compatibly with Article 8 and the Data Protection Act 2018. It seeks to ensure that any interference with an individual's right under Article 8 of the ECHR is in accordance with the law and is necessary and proportionate, and that both the public interest and the human rights of individuals are suitably balanced.

1.2.3 Surveillance, for the purpose of the Regulation of Investigatory Powers Act 2000, includes monitoring, observing, or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

1.2.4 In assessing and understanding whether and in what circumstances it is appropriate to use covert techniques, officers must consider the RIPA Codes of Practice issued by the Home Office**.** The codes of practice can be read in full at the following link. https://www.gov.uk/government/collections/ripa-codes

1.2.5 The Employment Practices Code provides a framework under which surveillance activity of employees can be authorised and conducted compatibly with Article 8 and the Data Protection Act 2018.

1.3 Scope

1.3.1 Gravesham Borough Council is committed to being open and transparent in the way that it works and delivers its services, including the use of surveillance. Where possible the council will always seek to use overt (non-secret) investigation techniques but recognises that the use of covert methods may be necessary in certain circumstances.

1.3.2 Each officer of the council with responsibility for the conduct of investigations, shall, before carrying out any investigation involving surveillance under RIPA or the Employment Practices Code, consult this policy and its associated internal procedures to ensure that any investigations and operations carried out are to be conducted lawfully. To support officers in making such assessments training will be provided.

1.3.3 Officers referring to this policy will need to be aware that it will interact with other council policies including, but not limited to, e-mail and internet policies and guidance, the Data Protection Policy and HR policies. As needed, advice on policy implementation should be sought from the relevant service areas and/or Legal Services.

1.3.4 If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. It is essential, therefore, that all involved with surveillance

activity comply with this document and any further guidance that may be issued, from time to time, by the Director (Corporate Services).

1.4 Senior Responsible Officer (SRO)

1.4.1 The Director (Corporate Services) is appointed as the senior responsible officer for establishing the framework for surveillance activity with council, including:

a) Ensuring integrity with the associated processes set in place within the Council;
b) Maintaining the central record of surveillance requests;
c) Acting as the key point of contact with the Investigatory Powers Commissioner's Office;
d) Maintaining oversight of any inspection process and the implementation of any post-inspection action plan.
e) Providing information to management and Members on the council's use of RIPA and surveillance activity.
f) Provision of training opportunities for officers that may become involved in surveillance activity.

1.5 Definitions

1.5.1 **Surveillance** includes:

a) the monitoring, observing, or listening to persons, their movements, their conversations or other activities or communications.
b) recording anything monitored, observed, or listened to in the course of surveillance
c) surveillance by or with the assistance of a surveillance device
d) the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

1.5.2 **Directed Covert Surveillance** involves specifically focusing attention on an individual for the purposes of a specific investigation or specific operation and is calculated to ensure that the person subject to the surveillance is unaware that the activity is taking place. It is undertaken:

a) in a manner which is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation); and
b) otherwise, than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

1.5.3 **Intrusive Surveillance** involves the presence of an individual at residential premises or in any private vehicle or using a surveillance device at residential premises or in any private vehicle. The Office of the Surveillance Commissioner's guidelines say that gardens and driveways are not included within the definition of 'residential premises'. Intrusive Surveillance can also be considered as taking place when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations. **Local authorities are not permitted to authorise this form of surveillance.**

1.5.4 A **Covert Human Intelligence Source (CHIS)** involves a source (a person such as a council employee or member of the public) who provides information to the council by establishing or maintaining a relationship with a person to obtain information or gain access to information. The relationship is conducted in a manner to ensure that the subject of the investigation is unaware of relationship between the other person and the council.

1.5.5 **Covert monitoring** means monitoring deliberately carried out in secret, without the knowledge of the person being monitored and should be considered in the same way as

surveillance activity. The activity involves the obtaining of access to restricted information either overtly or covertly. For example, an employer monitoring the email activity of an individual or group of employees in order to prevent or detect criminal activity.

1.5.6 **Communications data** is information relating to the use of a communications service, e.g., postal service or telecommunications system. Communications Data does not include the contents of the communication itself, content of emails or interaction with websites. The Investigatory Powers Act 2016 (IPA) created new Communications Data terminology. Communications Data now comprises 'Entity Data' and 'Events Data'.

a) **Entity Data** refers to data relating to entities or links between them e.g., name of subscriber, address for billing, contact telephone number, subscriber account information etc.
b) **Events Data** identifies or describes events which one or more entities engage in at a specific time or times. It could include call histories and activity, including itemized records of telephone calls, internet connections, dates, and times/duration of calls etc. Where the purpose of the acquisition is to prevent or detect crime and the data required is Events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

1.5.7 **Private information** is information relating to a person's private or family life. It can include any aspect of a person's relationship with others including professional and business relationships. A person may have a reduced expectation of privacy in a public place, but covert surveillance of their activities in public may still result in the obtaining of private information. This principle applies equally to the online world including social media sites. A determining factor in considering whether information is private is the use of privacy controls provided by the social networking site. Viewing open source information does not amount to obtaining private information because it is publicly available. Unrestricted open source information, such as social networking accounts which have no privacy settings applied are unlikely to fall within the definition of private information.

1.5.8 **Confidential Material** is defined by Sections 98-100 of the Police Act 1997 as;

c) Matters subject to legal privilege – this can include a situation where there is litigation taking place involving legal advice and also simply where a solicitor-client relationship exists for the purpose of obtaining advice or assistance in relation to rights and liabilities,
d) Confidential personal information – this will include physical and mental health information held by healthcare professionals and spiritual counselling information held by ministers of religion,
e) Confidential journalistic material – this is information obtained for journalistic purposes subject to an undertaking that it will be held in confidence.
f) communications between an MP and a constituent.

1.5.9 **Collateral Intrusion** is the invasion into the privacy of a third party who is not the intended subject of the surveillance. This may be unavoidable in certain circumstances, for example observing members of the public in the course of their daily life while conducting surveillance in a public area. The likelihood of collateral intrusion, and how this can be avoided or minimised, forms part of the proportionality criteria that is considered as part of applications.

1.5.10 **Open source information** is publicly available information (i.e., any member of the public could lawfully obtain the information by request of observation). It includes books, maps, journals, internet WWW and newsgroups, photographs etc.

1.5.11 **Open source research** is the collection, evaluation, and analysis of materials from sources available to the public whether on payment or otherwise, to use as intelligence or evidence within criminal investigations.

1.6 Applications for Directed Surveillance Authorisation

1.6.1 Authorisation is required for the use of directed surveillance when the council is carrying out any activity involving the covert monitoring of what somebody is doing in the discharge of one of its core functions to prevent or detect crime or to prevent disorder. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by six months imprisonment or more or relates to the sale or alcohol or tobacco to underage persons.

1.6.2 Any officer proposing to undertake any such activity must first make an application in writing for authorisation. This application will be in a standard form determined by the SRO.

1.6.3 In certain circumstances RIPA authorisation may not be necessary, for example, general observation that forms part of officers' everyday duties. An Environmental Health Officer, for instance, might covertly observe and then visit a shop as part of their enforcement function to verify the storage conditions of food. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, but this does not involve systematic surveillance of an individual. Such low level activity will not usually be regulated under the provisions of RIPA, which refers to Covert Surveillance only.

1.6.4 RIPA also does not cater for the use of overt CCTV surveillance systems, as members of the public are aware that such systems exist. General use of CCTV does not require authorisation. However, if CCTV is utilised for a covert pre-planned operation to follow an individual already identified, then an authority will be sought for directed surveillance.

1.6.5 Open Source research does not require surveillance authorisation as it involves the collation of publicly available information. However, it is likely that the systematic trawling and analysis of recorded data, if focused on an individual or group of individuals, would amount to surveillance. For example, daily checking of a social media account such as Facebook for updates and additional evidence. If such activity was proposed, written authorisation would be sought under RIPA and only carried out upon relevant approval.

1.7 Necessity and Proportionality

1.7.1 Those seeking authority and the Authorising Officer must consider whether the proposed surveillance, source activity or acquisition of communications data is both necessary for the particular operation or enquiry and whether it is proportionate to what is sought to be achieved by carrying them out.

1.7.2 Surveillance may be considered necessary on the following grounds,

a) Directed Surveillance – preventing and detecting conduct, which constitutes one or more criminal offences punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment, or an offence under;

- section 146 of the Licensing Act 2003 (sale of alcohol to children),
- section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children),
- section 147A of the Licensing Act 2003 (persistently selling alcohol to children), or
- section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

b) CHIS – preventing and detecting crime or preventing disorder.
c) Access to communications data – preventing and detecting crime or preventing disorder.

1.7.3 Any surveillance, CHIS activity or acquisition of communications data must also balance the seriousness of the intrusion into the privacy of the subject of the operation, or any other third party who may be affected, against the need for the activity in investigative and operational terms.

1.7.4 As such, when considering necessity and proportionality, officers will also look at what alternative courses of action are available that are less intrusive and whether they are more appropriate.

1.7.5 An officer seeking authorisation will evidence, as far as is reasonably practicable,

a) why the proposed surveillance activity is necessary and on what grounds,
b) what alternative means of obtaining the information that is to be sought through the use of the surveillance activity have been considered, e.g., by obtaining statements from witnesses (if available), and why they were not implemented.
c) how the size and scope of the activity is balanced against the gravity and extent of the perceived offence,
d) how the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result,
e) how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
f) detail the risks of any potential for collateral intrusion and what steps are to be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion into the lives of those not directly connected with the investigation or operation.
g) That the purpose of the surveillance is the prevention or detection of crime(s) punishable by six months imprisonment or more or relates to the sale or alcohol or tobacco to underage persons.

1.7.6 Authorising Officers will satisfy themselves that the points in paragraph 1.7.5 have been suitably considered and evidenced, as far as is reasonably practicable, before authorisation is granted.

1.7.7 Actions that are not considered necessary under the grounds listed in paragraph 1.7.2, or not considered proportionate because the proposed action is excessive in the overall circumstances of the case, cannot be authorised.

1.8 Provisional Approval of Applications for Covert Surveillance

1.8.1 The use of covert directed surveillance or CHIS for a particular investigation must be subject to prior provisional authorisation by an officer of an appropriate senior level. These officers will be known as Authorising Officers. A record of Authorising Officers currently appointed by the council can be found in the Surveillance Authorisation Guidance & Procedures.

1.8.2 Only the Chief Executive or, in his absence, the Deputy Chief Executive, is able to authorise the use of CHIS when this involves vulnerable individuals and juvenile sources.

1.8.3 The Authorising Officer will consider whether the proposed activity is an appropriate and reasonable use of the legislation, having considered all reasonable alternatives for obtaining the necessary result. In the case of a CHIS authorisation, the Authorising Officer will also consider the proposed arrangements for safeguarding the wellbeing of the source.

1.8.4 The Authorising Officer will record their assessment of the application and outline in detail:
   a) why the activity is considered proportionate; and
   b) how and why the methods to be adopted will cause the least possible intrusion on the target and others.

1.8.5 Applications will not be authorised by an Authorised Officer directly involved in the investigation so that there is an independent review of whether the activity is necessary and proportionate.

1.9 Judicial Approval of Applications for Covert Surveillance

1.9.1 Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval in accordance with the Protection of Freedoms Act 2012.

1.9.2 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until that authorisation has received the approval of the Magistrates Court.

1.9.3 Only the Senior Responsible Officer, through Legal Services, may apply for an appointment with the Magistrates Court to ensure judicial approval is obtained. The Investigating Officer is authorised by the adoption of this policy to attend the Magistrates" Court in order to make or support the application. The Authorising Officer may also be required to attend.

1.9.4 The Authority will make an application, without giving notice, to the Magistrates Court. The Magistrates will give approval if, at the date of the grant of authorisation or renewal of an existing authorisation, they are satisfied that:
   a) there were reasonable grounds for believing that obtaining the covert surveillance, use of a human covert intelligence source or acquisition of communications data was reasonable and proportionate and that these grounds still remain;
   b) the "relevant conditions" were satisfied in relation to the authorisation. Relevant conditions include that:
      - the relevant person was an Authorising Officer;
      - it was reasonable and proportionate to believe that using covert surveillance, a covert human intelligence source or acquiring communications data was necessary and that the relevant conditions have been complied with;
      - the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA;
      - any other conditions provided for by an order made by the Secretary of State were satisfied.

1.9.5 If the Magistrates" Court refuses to approve the grant of the authorisation, then it may make an order to quash the provisional authorisation granted by the Authorising Officer.

1.9.6 Once approved, the original authorisation and accompanying paperwork must be forwarded to the PA to Corporate Services to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the Central Register.

1.10 Procedure for Authorisation in respect of Communications Data

1.10.1 The acquisition of communications data for an investigation must also be subject to prior provisional authorisation by an Authorising Officer.

1.10.2 The introduction of the Office for Communications Data Authorisations (OCDA) means that an application to obtain Communications Data by local authority officers is not subject to judicial approval by a Magistrate but is instead assessed by the OCDA. The OCDA will consider the balance of protection of privacy and the risk to public safety and acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards, and challenging where required.

1.10.3 Applications for the obtaining and disclosing communications data must be channelled through a Single Point of Contact (SPoC) and notified to an Authorising Officer within the council.

1.11 Single Point of Contact (SPOC)

1.11.1 The Council use the services of the National Anti-Fraud Network (NAFN) for all Communications Data enquiries and as such NAFN performs the role of a SPoC through their qualified SPoC officers. Any initial internal enquiries should be directed to James Larkin Head of Internal Audit and Counter Fraud Shared Service (james.larkin@medway.gov.uk).

1.11.2 The SPOC will be in a position to;

- provide quality assurance checks to ensure that applications consistently comply with Investigatory Powers Act standards and are prepared 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.

1.12 Review, Renewal and Cancellation

1.12.1 All authorisations will have fixed duration periods. These time periods are dependent upon the type of activity authorised but in all cases the period of authorisation commences on the date either judicial approval or OCDA authorisation is given.

- Directed Surveillance authorisations - three months.
- CHIS authorisations - twelve months. In the case of a juvenile, a CHIS authorisation will only be valid for a period of four months and should be reviewed at least monthly)
- Authorisation for the acquisition of communications data – one month

Review

1.12.2 All authorisations will be subject to regular review to assess the need for the surveillance activity to continue and ensure that activity does not run on unnecessarily. The frequency of these reviews will be dependent upon the circumstances of the operation but will take place at suitable times, particularly where authorisations are anticipated to be short lived. Reviews

will also take place in response to changing circumstances to ensure that authorisations are still proportionate and lawful.

1.12.3 The outcome of a review should be recorded on the central record of authorisations.

Renewal

1.12.4 Where an authorisation is needed for a period exceeding that granted under the original authorisation, an application to renew the authorisation must be submitted in writing to an Authorising Officer before the expiry of the original authorisation. Authorisations can be renewed more than once, if necessary. An authorisation cannot be renewed after it has expired.

1.12.5 The Authorising Officer will review the renewal application to ensure that the criteria for necessity and proportionality are still met before renewing the authorisation, taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

1.12.6 In the case of a CHIS renewal, the authorising officer will also conduct a review of the use made of the source during the period authorised, the tasks given to the source and the information obtained from the use or conduct of the source. Any decision to renew the authorisation will consider the risks involved in the operation to the source.

1.12.7 In all cases the renewal of the authorisation will require judicial approval from the Magistrates or OCDA authorisation in the case of communications data. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval or OCDA authorisation has been obtained.

1.12.8 All renewals should be kept and recorded on the central record of authorisations.

Cancellation

1.12.9 It is a statutory requirement that all authorisations are cancelled as soon as they are no longer required. The Authorising Officer who granted or last renewed the authorisation will cancel the authorisation if they are satisfied that the authorisation is no longer needed or that the activity no longer meets the criteria outlined in the authorisation.

1.12.10 Cancellations do not require judicial approval or OCDA authorisation and as soon as the authorisation is cancelled, instruction will be given to those involved, including any CHIS, to stop all surveillance activity.

1.12.11 In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

1.13 Records Retention

1.13.1 The SRO will maintain a centrally retrievable record of all authorisations, reviews, renewals, cancellations and rejections for Directed Surveillance, CHIS, or the acquisition of communications data. This will be made available to the appropriate Commissioner or an Inspector from the Commissioner's Office during any review or inspection. Records will be retained for a period of six years after the authorisation has expired or is cancelled.

1.13.2 Copies of individual surveillance or photographic logs will be retained by the relevant department along with all other evidence or documentation related to their specific investigation or enquiry.

1.13.3 In all cases there is a duty of care to those under surveillance. All details and approvals will be kept strictly confidential. The privacy of individuals must not be put at risk and unnecessary information will not be documented.

1.14 Training

1.14.1 All officers undertaking an investigatory or enforcement role and those acting as Authorising Officers will receive appropriate training in the use and application of RIPA to ensure that investigations and operations are carried out in a lawful manner.

1.15 Responsibilities

1.15.1 All staff who may conduct any form of covert surveillance activity as part of their everyday duties are responsible for adhering to this policy and are accountable for their actions.

1.15.2 Failure to comply with this policy may render officers open to misconduct or criminal proceedings.

1.16 Oversight, Scrutiny, Tribunal and Complaints

1.16.1 The Investigatory Powers Commissioner has responsibility for reviewing the use of investigatory powers by public authorities. The Commissioner has a statutory obligation to inspect the use of investigatory powers as part of its oversight role. Further detail can be found at www.ipco.org.uk. The council will welcome and fully co-operate with any inspection visit from the Investigatory Powers Commissioner's Office.

1.16.2 The Act also establishes an independent Tribunal to investigate any case within its jurisdiction and hear complaints from persons aggrieved by conduct. The Tribunal has power to cancel authorisations and order destruction of information obtained and the council is under a duty to disclose to the Tribunal all relevant documentation.

1.16.3 Details of the relevant complaints' procedure are available via http://ipt-uk.com/

1.17 Review and approval of this Policy

1.17.1 This Policy document is important in providing a framework for the effective and efficient operation of the council's actions with regard to surveillance. This document will, therefore, be kept under annual review by the Director (Corporate Services) with any material amendment subject to approval of the Cabinet.

1.17.2 Authorising Officers and those involved in surveillance activity are responsible for bringing any suggestions for continuous improvement of this document and the processes set out therein to the attention of the Director (Corporate Services) at the earliest possible opportunity.

1.18 Contact

1.18.1 If you do not understand the implications of this policy or how it may apply to you, seek advice from the Director (Corporate Services).