Swindon Borough Council

Regulation of Investigatory Powers Act 2000

Policy and Procedure

August 2023

Scope

This Protocol applies to authorisations for surveillance (not involving entry on or interference with property or wireless telegraphy as regulated by the Police Act 1997), the use of covert human intelligence sources and the acquisition of communication data in exercise of available powers set out in the Regulation of Investigatory Powers Act 2000 ("RIPA") by Local Authority Investigation Sections.

Contents

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was enacted to provide a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the Human Rights Acts 1998. The main purpose of the Act is to ensure that individuals' rights are protected whilst allowing law enforcement and security agencies to do their jobs effectively and act proportionately.

1.2 RIPA regulates the carrying out of covert surveillance; the use of covert human intelligence sources (CHIS) (RIPA Part II); and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed (RIPA Part III). The acquisition and disclosure of data relating to communications is now subject to the safeguards contained within the Investigatory Powers Act 2016.

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

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

European Convention on Human Rights

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

1.6 Under Article 8, everyone also has the right to respect for their private and family life, their home and their correspondence. The Article recognises that there may be circumstances in a democratic society where it may be necessary for the State (which includes the Council) to interfere with this right. This can only be done in accordance with the law and for clearly defined purposes. These purposes are:

- In the interest of national security
- In the interest of public safety
- In the interest of the economic well-being of the country
- For the prevention or detection of crime or of preventing disorder
- The protection of health or morals

- For the purposes of assessing or collecting any tax, levy or other imposition, contribution or charge payable to a government department
- For the purpose, in emergency, of preventing death or injury or any damage to a person's physical or mental health, or mitigating the same
- For any other purpose as specified by the Secretary of State

1.7 Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences. These offences must be either punishable, whether on summary conviction or indictment, by a maximum term of at least six months' imprisonment or related to the underage sale of alcohol and tobacco. They can only do so where prior approval from the Magistrates Court has been granted. A local authority is a 'Relevant Public Authority' as listed in schedule 2, Part 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010.

1.8 Local authorities may acquire communications data under the provisions of the Investigatory Powers Act 2016. All such applications must be made on behalf of the local authority by a Single Point of Contact (SPoC) provided by the National Anti-Fraud Network (NAFN). Requests for authorisation are determined by the Office for Communications Data Authorisations (OCDA).

Impact on Investigations

1.9 To be able to justify any interference with the right to respect for an individual's privacy, and comply with the HRA, the Council will need to demonstrate that any intrusion into an individual's privacy is necessary for the purposes of an investigation. Surveillance is often a necessary part of an investigation. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert surveillance, and the Investigatory Powers Act 2016 (IPA) regulates the acquisition of communication data. Where it is considered appropriate, it will be necessary for the exercise of these powers to be authorised before surveillance can commence or communications data acquired. This applies where the surveillance is being undertaken by the Council Officers or by an outside agency acting on the Council's behalf. Authorising officers will need to satisfy themselves that a defensible case can be made for covert surveillance activity.

2. Policy

2.1 To ensure that authorisations and procedures are applied in a consistent way, the Council has adopted a policy covering the authorisation and use of covert surveillance, and the acquisition of communication data.

2.2 The Secretary of State has issued codes of practice on the use of covert surveillance under RIPA. The Investigatory Powers (Code of Practice) Regulations 2018 brought into force a series of codes of practice which include the acquisition of communications data under the IPA. The codes are admissible as evidence in criminal and civil proceedings.

2.3 There are links to the relevant Codes of Practice included within Appendix C of this Policy. In cases of conflict between the Policy and the Codes of Practice, the latter shall prevail.

2.4 This Policy will be reviewed annually to reflect any changes in legislation and best practice.

Investigatory Powers Commissioner's Office (IPCO)

2.5 IPCO provides independent oversight and authorisation of the use of investigatory powers as outlined in the Investigatory Powers Act 2016 by intelligence agencies, police forces and other public authorities.

2.6 IPCO's purpose is to oversee how these powers are used, taking account of the public. This oversight includes the inspection and authorisation of the use of these powers by over 600 public authorities.

2.7 The acquisition of Communications Data by local authority officers is no longer subject to judicial approval by a Magistrate. Authorisation of applications for the acquisition of communications data are considered by the Office for Communications Data Authorisations (OCDA) on behalf of the IPCO. The OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards and challenging where required.

Statement of Policy

2.8 The Council and officers, as well as those acting on its behalf undertaking investigations into criminal offences and breaches of the civil law will endeavour to comply with the following statement of policy at all times:

In carrying out investigations into criminal offences and breaches of the civil law, the Council will seek to ensure that any interference with the rights of any person is in accordance with the law and is justified by reason of it being undertaken for a legitimate purpose. The use of the covert surveillance or the acquisition of communication data will be conducted in accordance with the statutory codes of practice then in force. The means to be employed in any investigation will be proportionate.

Proportionality is an essential element of the Human Rights Act; to be proportionate any surveillance must not be arbitrary, unfair or excessive. The extent of the surveillance must be balanced against the individual's human rights. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair".

This requires the officer to justify the need for the surveillance and the methods used and balance those with the impact on the privacy of the subject. The Department of Constitutional Affairs ("DCA") guide on Human Rights (page 55) states:

"When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim."

3. Procedures and the Codes of Practice

3.1 This guide seeks to set out the Council's procedures for the authorisation of surveillance operations and acquisition of communications data, and to provide a brief summary of the main points in the Statutory Codes of Practice on Covert Surveillance. The Statutory Codes of Practice are set out at Appendix C. In addition to this Policy and the Statutory Codes of Practice, individual teams within the Council may adopt practices and procedures to assist with compliance within their service areas, provided they are in keeping with this Policy and the relevant Codes. For example, the Council's Trading Standards Team and CCTV Team. This function specific guidance is an aide for clarification and is not a substitute for the Policy or Codes themselves.

Surveillance

3.2 Surveillance includes monitoring, observation or listening to persons, their movements, their conversations or their other activities or communications. If surveillance is carried out without the person's knowledge, it will be covert and require prior authorisation. RIPA applies to Directed Surveillance, Intrusive Surveillance and the use of Covert Human Intelligence Sources. Surveillance includes 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.

Directed Surveillance

3.3 Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) 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.

Intrusive Surveillance

3.4 Surveillance becomes intrusive if the covert surveillance:

- Is carried out in relation to anything taking place on any residential premises or in any private vehicle involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device, or
- Is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

3.5 The Council is not permitted to carry out intrusive surveillance.

Identifying directed surveillance

3.6 Is the surveillance covert?

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.
If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

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

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

3.7 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

3.8 Is the surveillance undertaken in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

3.9 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol. However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

3.10 Investigating Officers may need to identify whether a location is suitable for surveillance, for example, by 'drive-by'. This is not prevented under the Codes of Practice. However if officers make more than one 'drive-by' then authorisation may be required, unless, for example, where the officer's observation was interrupted or blocked in some way and the 'drive by' is repeated.

3.11 General observation forms part of the duties of many law enforcement officers and other public authorities and Authorisations are not usually required. For example, officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

3.12 When Authorisation of Surveillance in or into a Public Place is Not Required

Where the use of CCTV surveillance systems (fixed or mobile) is overt, usually by way of a notice, authorisation is not required. However if the camera is used to observe the actions of a particular individual then the surveillance becomes directed and covert, therefore an authorisation would be required.

Where a person suspected of having committed an offence has been notified that his activities are being monitored, no authorisation will be required. For example, where the Council receives a noise complaint, or it is alleged that goods are being displayed on the highway verge, if a letter is sent to the person responsible for the alleged nuisance or display, notifying him that the level of noise from his premises or activities are being monitored, any surveillance will not be covert. However any recording of conversations, rather than just the level of noise is intrusive surveillance and must not be done. The investigating officer must consider whether there is likely to be any collateral intrusion as a result of his surveillance. If there is any likelihood of any collateral intrusion where private information is acquired, an authorisation will be required.

3.13 Use of the Council's CCTV system

The use of Council's CCTV system is detailed in the CCTV manual located in the CCTV control room. This manual covers the use of the CCTV for surveillance purposes and must be followed at all times when conducting surveillance activities. The Home Office Surveillance Camera Code of Practice can be found here: https://www.gov.uk/government/publications/update-to-surveillance-camera-code

3.14 Non RIPA

Due to the changes brought about by the Protection of Freedoms Act 2012, there may be circumstances whereby it is necessary and proportionate, to carry out covert surveillance for activities which do not meet the crime threshold set out above.

3.15 In such circumstances, staff must complete a non-RIPA form (adapt a standard application form for these purposes), setting out why such activity is necessary and proportionate and giving due consideration to any potential collateral intrusion.

3.16 Non RIPA forms must be authorised by a Head of Service. However, if the activity relates to an investigation against a member of staff, authorisation must be provided by the Senior Responsible Officer, the Head of Internal Audit or one of the Council's Corporate Directors.

Covert Human Intelligence Sources (CHIS)

3.17 A person is a Covert Human Intelligence Source if:

- The source establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (a) and (b) below.

    a) The source covertly uses such a relationship to obtain information or provide access to any information to another person; or
    b) The source covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

It is important to remember a relationship can be formed from a single encounter.

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

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship 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, it is used or 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.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence.

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

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, or if an adult is observing a juvenile test purchase, this will require authorisation as directed surveillance. In all cases, a prior risk assessment is essential in relation to any young person used for a test purchase.

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

It should be noted, however, that if the information provided is recorded as potentially useful or actionable, there is potential duty of care to the individual and the onus is on the public authority to manage human sources properly. Authorising Officers should be alive to the possibility of 'status drift'. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

An authorisation under RIPA will provide lawful authority for the use of a source.

3.19 Examples of Covert Human Intelligence Sources

- Purchases from a person selling goods from home should be covered by a CHIS Authorisation, both because the nature of discussion generally might go further than an 'across-the-counter' exchange and to avoid intrusive surveillance.
- Trading Standards Officers may use residential and business premises, rented specifically for the purpose, to invite suspected rogue traders to quote for business. A CHIS Authorisation should be used. However if the premises is being used as a residential dwelling then the surveillance is considered to be intrusive surveillance and cannot take place.
- An officer working under cover, gathering information by concealing his or her identity will usually require the activity to be authorised, using the forms in Appendix B. The authorisation would also cover the use of any body worn covert recording device. Other directed surveillance of a covert human intelligence source would require separate authorisation.
- Routine test purchases where the officer acts as a member of the public and purchases goods for sale will not require authorisation. If the officer extends this situation in any significant way, by for example,
    - Engaging the seller in conversation to elicit information;
    - Developing a relationship with the seller to gain access to goods not on display.

Then authorisation will be required for the use of a covert human intelligence source.

3.20 If officers are considering the use of a CHIS they must seek advice and guidance from the Legal Services Team, prior to completing the RIPA application.

3.21 Where the authority uses a CHIS, that CHIS should be assigned a Handler. The Handler will keep regular contact with the CHIS, or daily where the Authority uses one of its own officers as the CHIS. The Handler will ensure that the CHIS's identify has not been compromised. The Handler will record information of the identity of the source on a log and will destroy all records which identify the CHIS once the investigation has been completed.

3.22 The authority shall also appoint a Controller who will have general oversight of the use made of the source.

3.23 Before a CHIS is used a risk assessment must be completed and kept with the application (see Appendix B). This risk assessment should be reviewed at least monthly.

3.24 The use of a juvenile (those under 18 years old), or other vulnerable person as a CHIS should generally be avoided and must only be used in exceptional circumstances. The Chief Executive is the only officer who can authorise an application to use such persons as a CHIS, or in his/her genuine absence, the Chief Operating Officer.

3.25 Any decision to use a juvenile or other vulnerable person as a CHIS will be based on full consideration of the justification for doing so, the risks posed to that individual and the protection able to be afforded to the CHIS.

3.26 The duration for authorisation of a juvenile is four months, rather than 12, and the authorisation is subject to monthly review.

3.27 Public authorities must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age.

Covert surveillance of social networking sites (SNS)

3.28 Even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available. The author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission.

3.29 Providing there is no warrant authorising interception, if it is necessary and proportionate for a public authority to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf, i.e. the activity is more than mere reading of the site's content

3.30 Officers must not:

- Set up a false identity for a covert purpose without authorisation
- Adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation and without the consent of the person of the person whose identity is used, and without considering the protection of that person. The consent must be explicit.
- Use their personal social network login details to view individuals under investigation

3.31 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place, this can be regarded as overt and a directed surveillance authorisation will not normally be necessary.

3.32 As set out in paragraph 3.33 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.33 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.34 Whether the Council interferes with a person's private life includes a consideration of the nature of the Council's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where the Council is systematically collecting and recording information about a particular person or group, a directed

surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

Communications data

3.35 Definition

Communications data covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating 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.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc. As technology advances and more services become 'online', there is a higher likelihood that associated data becomes communications data rather than data that would have traditionally been accessible under the Data Protection regime. For example, mandatory information provided by a user whilst accessing a telecommunications service (including a website) such as eBay subscriber information (name and email address) would be obtained under IPA, but transaction details and advert history would be obtained under the Data Protection Act.

The Investigatory Powers Act 2016 (IPA) created new Communications Data terminology. Communications Data now comprises 'Entity Data' and 'Events Data'. Entity Data broadly replaces 'Subscriber Data' under RIPA, s21(4)(c), e,g name of subscriber, address for billing, contact telephone number, subscriber account information etc. Events Data identifies or describes events which consist of one or more entities engaging in an activity at a specific time or times. It includes call histories and activity, including itemized records of telephone calls, internet connections, dates and times/duration of calls etc.

Event data refers to both 'Traffic Data' (S21(4)(a)) and 'Service Use Information' (S21(4)(b)) under RIPA. 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.

3.36 Serious Crime threshold

From 1 November 2018, a serious crime threshold must be met for the acquisition of service or traffic data. This means that where an application is for the crime statutory purpose (S60A(7)(b)) IPA to acquire event data, the crime must be a serious crime.

3.37 Definition of Serious Crime

- 12 months (or more) imprisonment

  - an offence that is capable of attracting a prison sentence of 12 months or more

- Corporate Body

  - an offence by a person who is not an individual

- S81 Offence

- an offence falling within the definition of serious crime in S81(3)(b) of the IPA where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose

- Communication Offence

  - an offence which involves, as an integral part of it, the sending of a communication

- Breach of Privacy

  - an offence which involves, as an integral part of it, a breach of a person's privacy

Encryption

3.38 Encryption is the conversion of data into a form that renders the contents unintelligible to anyone not authorized to read it. Decryption is the process of converting the encrypted data back into its original form, so it can be understood. Many people use easily-accessible programmes to encrypt their email, files, folders, documents and pictures. However, these technologies are also used by terrorists, criminals and paedophiles to conceal their activities.

3.39 Part III of RIPA deals with the 'Investigation of Electronic Data Protected by Encryption etc.' It provides any public authority the power to require that data they have obtained or expect to obtain lawfully should be put into an intelligible form or to require disclosure of the means to make it intelligible.

3.40 When using encryption powers refer to the 'Code of practice for investigation of protected electronic information'.

4. Authorisations

4.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons.

4.2 All applications for authorisation of directed surveillance or for the conduct and use of any source must be referred to the RIPA Senior Responsible Officer (SRO) before submission to an Authorising Officer for consideration.

If the authorisation is provisionally approved by the Authorising Officer, each provisional authorisation then needs to receive judicial approval before being acted upon. Once approved, the original authorisation and accompanying paperwork must be forwarded to the SRO to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the central register.

4.3 Any officer wishing to engage in conduct in relation to a system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure of which differs slightly and is outlined in paragraph 4.17.

4.4 Who can give Provisional Authorisations?

The Council's appointed Authorising Officers are set out in Appendix A. An Authorising Officer may grant a provisional authorisation, but this authorisation will not take effect until it receives judicial approval (See paragraph 4.14). Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can only be granted by the Chief Executive, or, in his/her genuine absence, the Chief Operating Officer.

4.5 It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

4.6 Training will be given, or approved by the SRO, before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training or a one-to-one meeting with the SRO on such matters will be kept by the SRO.

4.7 Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document. Authorising Officers must also ensure that, when sending copies of authorisations and associated documentation to the SRO, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'.
Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

4.8 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance. An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance, or for the use of a source unless he/she believes:

a) that a provisional authorisation is necessary and

b) the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe.

4.9 The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion at 4.12 below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or

alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and schools admissions/suspected false addresses will not be deemed a proportionate activity.

4.10 Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities.

4.11 Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

4.12 Collateral Intrusion

Where a request for surveillance is made, the Authorising Officer will have to be satisfied that the risks of collateral intrusion have been properly considered. Collateral intrusion is where a third party's privacy is being infringed. For example, where an officer takes still or video photographs, or observes one or more innocent third parties, this could be considered as being collateral intrusion. If in the course of investigating a case, a third party's privacy has been inadvertently invaded, the action should be defensible from a legal viewpoint, provided that the grounds for investigation are sound, i.e. the investigation has been undertaken to detect and/or prevent fraud or some other offence for which the Council is the enforcing authority and the actions are reasonable.

People who may be the subject of collateral intrusion include:

- Customers or workers at a business premises
- Visitors to a property
- Friends or relatives of the suspect

4.13 Firstly, identify here who else may be caught by the surveillance.

Secondly, state why it is unavoidable. This could be because of the nature of the premises (e.g. restaurant) or because of what the person is doing (e.g. visiting other subject/target premises) that there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.
Thirdly set out what steps you have taken to minimise collateral intrusion. This may include:

- Using a still camera as opposed to a video camera
- If installing hidden cameras, only switching them on at specific times rather than all the time
- Narrowing the field of vision or the place where the cameras are cited
- Reducing the amount of surveillance done at busy times e.g. shops or places of worship

If you cannot minimise collateral intrusion you still need to show you have considered it. You may wish to add that you cannot do anything to minimise it but you will not be making any decisions on the information gathered about third parties unless it shows them committing a criminal offence.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

4.14 Judicial Approval of Provisional Authorisations and Renewals

The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. All provisional authorisations and renewals must be approved by the Magistrates Court before surveillance commences.

The Council must apply to the local Magistrates Court for an Order approving the grant or renewal of an authorisation. A template application form and draft Order are included at Appendix B to this policy. In order to obtain judicial approval, the first page of the template form must be completed and submitted along with a copy of the provisional authorisation and any other relevant supporting documents. Also within Appendix B is a flow chart setting out the Magistrates Court authorisation process.

The Council does not need to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuse to approve the application, they may also make an order quashing the provisional authorisation.

4.15 The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves that:

a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;

b) That the person who granted provisional authorisation was an appropriately designated person;

c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and

d) Any other conditions provided for by an order made by the Secretary of State were satisfied.

4.16 A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and

- the tasks given to the source during that period, and the information obtained from the conduct or use of the source.

and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Council service area dealing with the investigation will generally make applications for judicial approval to the Magistrates Court on behalf of the Council. Any particularly complex authorisations or authorisations arising from other areas of the Council that require legal input or representation may be dealt with by the Council's Legal Services Team if necessary in the circumstances.

Judicial approval is necessary for all applications/authorisations and renewals. There is no requirement for judicial consideration of cancellations or internal reviews.

Oral Authorisations for urgent surveillance are no longer available for use by Local Authorities.

Special Procedure for Authorisation of Communications Data

4.17 The introduction of the Office for Communications Data Authorisations (OCDA) means the acquisition of Communications Data by local authority officers is no longer subject to judicial approval by a Magistrate. OCDA assesses Communications Data applications from public authorities and makes decisions about those applications that strike a fine balance between the protection of privacy and the risk to public safety. OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards and challenging where required.

Applications for the obtaining and disclosure of communications data may only be made by officers of the Council.

4.18 Applications for communications data must be channelled through single points of contact ("SPoCs"). The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

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. All applicants must be registered with NAFN via the NAFN website at www.nafn.gov.uk . Any initial internal queries can be directed to the SRO .

The SPoC is required to:

- 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

4.19 S60A of IPA provides for independent authorisation of communications data requests by the Investigatory Powers Commissioner (IPC). OCDA performs this function on behalf of the IPC. An authorising officer in OCDA can authorise any lawful request, for any of the specified purposes from any listed authority. For the Council, the sole purpose is the 'applicable crime purpose'.

The IPA provides a new requirement for a local authority making an application to ensure someone of at least the rank of Senior Responsible Officer is aware.

4.20 OCDA will only retain, for a limited period of time, the Communications Data applications which are sent to them and the decision document they issue back to public authorities. Public Authorities are therefore required to keep records of both the Communications Data applications that they issue as well as the decisions received from OCDA. Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data

Protection Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

4.21 Where the purpose of a Communications Data application is to identify a journalistic source, these must first be authorized by an Authorising Individual (OCDA AO or DSO) but must also be approved by an IPCO Judicial Commissioner (JC). The Applicant and SPOC should pay special consideration to these applications and inform their Senior Responsible Officer. The IPA does not alter the existing processes for Communications Data applications that may feature sensitive professions including medical doctors, lawyers, journalists, parliamentarians or ministers of religion. If the Communications Data could contain information relating to any of these professions, this must be noted in the application.

4.22 Urgency

Urgent authorisations are no longer available in relation to directed surveillance or covert human intelligence sources.

4.23 Surveillance where it is likely that Confidential Material will be obtained

If, exceptionally, an Investigating Officer thinks that in the course of conducting surveillance s/he may obtain confidential information, the Investigating Officer will have to obtain authorisation from the Chief Executive. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

Legal privilege includes:

- Communications between a professional legal adviser and his client or any person representing his client, which are made in connection with the giving of legal advice to the client; or
- Between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person, which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings. It does not include communications and items in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose
- Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.
- Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.24 Standard Forms

All authorisations must be in writing. Standard forms for seeking provisional directed surveillance and source authorisations, as well as a standard form for obtaining judicial approval, are provided at Appendix B. All authorisations shall be sought using the standard forms as amended from time to time.

5 Activities by other public authorities

The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

5.1 Joint investigations

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

5.2 When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record and / or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

b) wish to use the Council's premises for their own RIPA action, the officer should normally co-operate, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

6 Duration, renewals and cancellation of authorisations

6.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed. Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source (4 months for juvenile CHIS authorisations)
b) three months from the date of judicial approval for directed surveillance

c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

6.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews. Standard review forms for directed surveillance and CHIS are available at Appendix B.

6.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations. Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired.

The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source.

and for the purposes of making an Order, the Magistrates have considered the results of that review. The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are available at Appendix B**.**

6.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the authorising officer who issued it.

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

Standard cancellation forms for directed surveillance and CHIS are available at Appendix B.

7. Records

7.1 The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Senior Responsible Officer. In relation to communications data, the designated SpoC (NAFN) will retain the forms and the Senior Responsible Officer will have retain copies of such forms as required.

7.2 Central record of all Authorisations

The Senior Responsible Officer, shall hold and monitor a centrally retrievable record of all provisional and judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Senior Responsible Officer to ensure that the records are regularly updated.

7.3 The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

7.4 The Senior Responsible Officer will monitor the submission of provisional and judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Senior Responsible Officer shall contain the following information:

a) the type of authorisation or notice
b) the date the provisional authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;
e) the unique reference number (URN) of the investigation or operation;
f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) review dates
j) the date the authorisation or notice was cancelled.

7.5 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;
b) a record of the period over which the surveillance has taken place;

c) the frequency of reviews prescribed by the Authorising Officer;
d) a record of the result of each review of the authorisation or notice;
e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;
f) the date and time when any instruction was given by the Authorising Officer.
g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

7.6 Other Record of Covert Human Intelligence Sources

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless s/he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

7.7 The records shall contain the following information:

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant investigating authority other than the Council;
d) the means by which the source is referred to within each relevant investigating authority;
e) any other significant information connected with the security and welfare of the source;
f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g) the date when, and the circumstances in which, the source was recruited;
h) the identities of the persons who, in relation to the source;
    I. hold day-to-day responsibility for dealing with the source and for the source's security and welfare
    II. have a general oversight of the use made of the source (not to be the person identified in (h)(i))
    III. have responsibility for maintaining a record of the use made of the source

i) the periods during which those persons have discharged those responsibilities;
j) the tasks given to the source and the demands made of him in relation to his activities as a source;
k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l) the information obtained by the conduct or use of the source;
m) any dissemination of information obtained in that way; and
n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

7.8 Retention and destruction

Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data.

Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

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.

8. Consequences of ignoring RIPA

8.1 RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be lawful for all purposes.

8.2 Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

8.3 Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

9. Scrutiny of investigatory bodies

9.1 The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioner will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.ipco.org.uk

9.2 There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from IPCO.

The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

10. RIPA Roles and Responsibilities

10.1 Senior Responsible Officer – is responsible for having daily over sight of the RIPA process by ensuring:

- The integrity of the process in place within the public authority to authorise directed and intrusive surveillance;
- Compliance with Part II of the 2000 Act, Part III of the 1997 Act and with the codes;
- Engagement with the Commissioners and inspectors when they conduct their inspections,
- That all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners Investigatory Powers Commissioner's Office. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed
- To review the quality of the applications and authorisations
- To authorize surveillance activities but only in exceptional circumstances.

10.2 Senior Responsible Officer will oversee the process for acquiring communications data under IPA, and will be consulted in relation to the submission of applications to NAFN for consideration by the OCDA.

10.3 Coordinating Officer - is responsible for ensuring all authorising officers and investigating officers are properly trained and to raise awareness of RIPA within the Authority.

10.4 CHIS handler - is responsible for the safety and security of the CHIS and their identity. The handler is also responsible for directing the day to day activities of the source and recording the information supplied by the source. The handler will ensure that the CHIS' identify has not been compromised and will destroy all records which identify the 'CHIS' once the investigation has been completed.

10.6 CHIS Controller - is responsible for the general oversight of the use of the source.

10.7 Authorising Officer is responsible for ensuring that the application for surveillance is permitted to be undertaken by the local authority, to ensure that the proposed surveillance is necessary and proportionate and that any collateral intrusion is limited as far as is practical. The authorising officer is responsible for determining the surveillance that can take place.

Note: The Authorising Officer must be independent from any operation/investigation they are asked to consider. If this requirement cannot be shown to have been met OR if there is any uncertainty, then a different Authorising Officer who is independent must consider the application.

10.8 Elected members - a report will be issued to elected members reviewing the authority's use of the 2000 Act and set the policy at least once a year to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

10.9 Coordinating Officers Group is responsible for ensuring that the procedures are being applied across the Authority. To ensure consistency of approach and application of RIPA.

10.10 The Senior Responsible Officer is responsible for:

- Keeping the central register of RIPA authorisation
- Providing a URN for each RIPA application and
- Maintaining the records of applications, authorisations, reviews, renewals and cancellations.

Training

10.11 No officer shall undertake any surveillance activity unless they have received training for RIPA at a level and to an extent considered appropriate to the officer's role in the opinion of the Senior Responsible Officer. Every applying officer should undertake refresher training every two years.

Authorising officers should be regularly trained and if they do not authorise surveillance activities on a regular basis they should refresh their knowledge of RIPA before they authorise a request.

Appendix A – Authorising Officers

The Council has designated the following officers to authorise surveillance:-

***Notes:**

i. The Authorising Officer must be 'Operationally Independent' from any investigation they are asked to consider for approval. If this requirement cannot be shown to have been met OR if there is any uncertainty, then a different Authorising Officer who is independent, must consider the application.

ii. For guidance, areas of investigation presumed to compromise respective Approving Officers operational independence are shown in the table below.

iii. Ultimately it is for Approving Officers to make this judgment in each case i.e. to ensure their Operational Independence AND their ability to demonstrate this if required.

Designation	**Officer**	**Scope**	**Exclusions**
Chief Executive	Sam Mowbray	All purposes (including where there is a likelihood of acquiring confidential information); the use of a juvenile or other vulnerable person as a CHIS although this should generally be avoided and must only be used in exceptional circumstances). In the absence of the Chief Legal Officer, the duties of Senior Responsible Officer for the purposes of the Investigatory Powers Act 2016	Where there is insufficient Operational Independence
Chief Legal Officer	Lisa Hall	Senior Responsible Officer for RIPA Duties of Senior Responsible Officer for the purposes of the Investigatory Powers Act 2016	**Precluded except in exceptional circumstances*.
Chief Operating Officer	Mick Bowden	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive) In the absence of the Chief Legal Officer, the duties of Senior Responsible Officer for the purposes of the Investigatory Powers Act 2016	Where there is insufficient Operational Independence.

Designation	Officer	Scope	Exclusions
Head of Regulatory Services	Kate Bishop	RIPA Co-ordinating officer. Any appropriate investigations.	Where there is insufficient Operational Independence.
Director of Strategic Development and Growth	Richard Bell	Any appropriate investigation.	Investigations Involving: Planning Trees Licensing Taxis Animal welfare and related offences.
Director of Housing	Michael Ash	Any appropriate investigation.	Housing (tenant related) Anti-Social Behaviour investigations.
Corporate Director Adult Services, Health & Housing	Alison Barker	Any appropriate investigation.	Safeguarding of Adults and other related issues where there is insufficient operational independence.
Corporate Director Children Services (DCS)	Lisa Arthey	Any appropriate Investigation	Truancy, Youth Offending, Safeguarding of Children or young persons and other related issues where there is insufficient operational independence.