CORPORATE PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Document Control

Document ownership	Senior Responsible Officer
Local of document	Council website and internet
Document review period	Every 12 months
Document approval	Cabinet
Enquiries about this document	Senior Responsible Officer/RIPA Co-ordinating Officer

Document History

V	Description of document or amendment	Date
1	Original document	July 2012
2	Full refresh of Joint Policy and changes to key officers	February 2019

CONTENTS PAGE

A. INTRODUCTION AND KEY MESSAGES

1. This document sets out the policy and procedures adopted by Babergh and Mid Suffolk District Councils based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA'). This policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioners Office (IPCO) (formally the Office of Surveillance Commissioners – OSC).

2. For the purpose of this update, references to the Home Office Codes of Practice relate to the latest versions which were issued in August 2018 in relation to covert surveillance and covert human intelligence sources; and 2016 in relation to the acquisition and disclosure of communications data.

   The Home Office Codes of Practice can be found at:
   https://www.gov.uk/government/organisations/home-office/series/ripa-codes

3. Where reference is made in this document to the Senior Responsible Officer (SRO) this means the Assistant Director – Law & Governance and Monitoring Officer, whose duties are set out in Section B.

4. Similarly, where reference is made in this document to the RIPA Co-ordinating Officer this means the Corporate Manager – Internal Audit, whose duties are set out in Section B.

5. Councillors have a role to play in reviewing the Council's use of RIPA to ensure that it is being used consistently with this procedure document. They will also ensure that the policy is fit for purpose. However, councillors will not be involved in making decisions on individual authorisations.

6. The authoritative position on RIPA is, of course, the Act itself and any officer who is unsure about any aspect of RIPA should, if unsure, **contact, at the earliest possible opportunity the SRO or the RIPA Co-ordinating Officer before any request is formally made.**

7. Appropriate training and development (including refresher training) will be provided or arranged by the RIPA Co-ordinating Officer for Authorising Officers and Investigating Officers.

8. The RIPA Co-ordinating Officer will maintain and check the Central Register of all RIPA Authorisations, Reviews, Renewals, Cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to ensure the RIPA Co-ordinating Officer receives the originals of the relevant Forms within 1 week of authorisation, review, renewal, cancellation or rejection.

9. RIPA and this Policy are important for the effective and efficient operation of the Councils' actions with regard to covert investigations. This Policy will, therefore, be kept under annual review by the SRO. **Authorising Officers must bring any**

suggestions for continuous improvement of this Policy to the attention of the SRO at the earliest possible opportunity. If any of the Home Office Codes of Practice change, this Policy will be amended in light of these changes.

10. In terms of internal monitoring of e-mails and internet usage, it is important to recognise the important interplay and overlaps with the relevant Council's e-mail and internet policies, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, and the General Data Protection Regulations (GDPR) 2018. Under normal circumstances, the Councils' e-mail and internet policies should be used, as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA.

11. This August 2018 update includes the changes to RIPA brought about by the Protection of Freedoms Act 2012. This includes judicial approval of all covert surveillance carried out by local authorities and restricting use of directed surveillance to serious criminal offences.

12. **At no time should the Council undertake any surveillance that interferes with any private property. Placing tracking devices on a subject's vehicle or person is not authorised for local authorities and must not be used.**

13. **The Councils take seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in investigation matters.**

14. **It should be noted that any use of activities under RIPA will be as a last resort and Councils' policy is not to undertake such activities unless absolutely necessary.**

15. **Before any action is contemplated it is strongly advisable that early consultation with the Authorising Officer or Co-ordinating Officer is undertaken to ensure all actions are fully considered.**

B. ROLES AND RESPONSIBILITIES (see also Appendix 1)

Senior Responsible Officer (SRO)

1. The role of SRO will be undertaken by the Councils' Assistant Director for Law & Governance and Monitoring Officer.

2. In accordance with good practice the SRO will be responsible for:

    - The integrity of the process in place within the Councils for the management of Covert Human Intelligence Source (CHIS);

    - Compliance with Part 2 of the Act and with the Home Office Codes of Practice;

- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and

- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Authorising Officers

3. It is essential that Authorising Officers take personal responsibility for the effective and efficient operation of this Policy. Authorising Officers are listed in Appendix 1. They can be added to or substituted by the SRO.

4. The SRO has and will ensure that a sufficient number of Authorising Officers are, after suitable training on RIPA and this Policy, duly authorised to take action under this Policy.

The Authorising Officers must ensure the following:

- That staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Policy.

- Pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorising Officer approve any RIPA form unless, and until they are satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, they should obtain prior guidance on the same from the Council's Health & Safety Manager and/or the SRO.

- Acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and ensure that the original forms are sent to the RIPA Co-ordinating Officer in a **sealed** envelope marked '**Strictly Private & Confidential'**. Forms must be provided to the RIPA Co-ordinating Officer within 1 week of signing by the Authorising Officer. Any failure to comply exposes the Council to unnecessary legal risks and criticism from the IPCO. Any cancellations must be dealt with promptly.

- Proper regard is had to **necessity and proportionality** of the surveillance before any forms are signed. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular

circumstances of any person likely to be the subject of the surveillance. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

5. There are enhanced authorisation levels for directed or intrusive surveillance by public authorities when knowledge of **confidential or privileged information** is likely to be acquired (see the Covert Surveillance Code 2018 Chapters 5 and 9, and Annex A). In such cases the surveillance authorisation **must** be signed by the Councils' Chief Executive as failure to do so may invalidate the admissibility of any evidence obtained.

6. Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorising Officers **may not sub-delegate** their powers in relation to RIPA to other officers.

7. The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

RIPA Co-ordinating Officer

8. The appointed RIPA Co-ordinating Officer shall:-

- Have overall responsibility for the management and oversight of requests and authorisations under RIPA;

- Issue a unique reference number to each authorisation requested under RIPA (this must be before the application has been authorised);

- Retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer.

- Maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice.

- Review and monitor all forms and documents received to ensure compliance with the law and guidance and this policy and procedures document and informing the Authorising Officer of any concerns;

- Chase failures to submit documents and/or carry out reviews/cancellations;
- Be responsible for organising a corporate RIPA training programme;

- Ensure corporate awareness of RIPA and its value as a protection to the Councils is maintained; and

- Produce an annual position statement on the Councils' use of RIPA to the Cabinet.

Councillors

9. Members of the Councils' Cabinet will note the RIPA policy and thereafter following any significant changes to working practices and receive an annual position statement on the Councils' use of RIPA.

C. GENERAL INFORMATION ON RIPA

1. The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-

   (a) **in accordance with the law;**
   (b) **necessary for the prevention and detection of crime or preventing disorder; and**
   (b) **proportionate** (as defined in this Policy).

3. RIPA provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – e.g. undercover agents. However, the Councils are reluctant to use CHIS as an investigatory tool, and if any such application is contemplated prior advice must be sought from the SRO or the RIPA Co-ordinating Officer. RIPA also permits local authorities to compel telecommunications and postal companies to obtain and release communications data to themselves, in certain circumstances. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is **necessary** and **proportionate**. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4. Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Councils' behalf must be properly authorised by one of the Councils' Authorising Officers.

5. If the correct procedures are not followed, evidence may be disallowed by the

courts, a complaint of maladministration could be made to the Local Government Ombudsman, and/or the relevant Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with covert investigations comply with this Policy and any further guidance that may be issued, from time to time, by the SRO.

6. The Councils treat the powers given to it under RIPA very seriously and expects Authorising Officers and the investigating officers to do so. Failure to adhere to this Policy by Authorising Officers or the investigating officers may result in disciplinary action being taken against them by the Council.

7. Social Networking Sites and Internet Sites

Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site (e.g. Facebook, Twitter, Instagram etc. – refer to the OSC's Procedures and Guidance – paragraph 289 refers), and even though the 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. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

The Councils need to give consideration to 3.4 of the new Code of Practice for covert surveillance and property interference which states, *"Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites."*

If it is necessary and proportionate for the Councils 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 the officer (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site.

8. A flowchart of the procedure for Magistrates' approval of surveillance operations is at **Appendix 3**.

D. TYPES OF SURVEILLANCE

1. 'Surveillance' includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.

- recording anything mentioned above in the course of authorised surveillance.

- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

2. <u>Overt Surveillance</u>

Most of the surveillance carried out by the Councils will be done overtly – there will be nothing secretive, clandestine or hidden about it. 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. food and safety inspections).

3. 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 the conditions are being met.

4. <u>Covert Surveillance</u>

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place (Section 26(9) (a) of RIPA). It cannot, however, be "necessary" if there is reasonably available an overt means of finding out the information desired.

5. RIPA regulates three types of covert surveillance: Directed Surveillance, Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

6. Directed Surveillance is surveillance which:-

- is covert;

- is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance or any interference with private property);
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it;

- is pre-planned; and

- is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual whether or not that person is specifically targeted for purposes of an investigation (Section 26(10) of RIPA).

7. **Private information** in relation to a person includes any information relating to their private and family life, their home, their correspondence and their business relationships. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and others that they come into contact, or associate, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera(s) are to be directed for a specific purpose to observe particular individual(s), authorisation will be required. The way a person runs their business may also reveal information about their private life and the private lives of others.

9. The use of CCTV must be accompanied by clear signage in order for any monitoring to be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation, then RIPA authorisation is likely to be required as mentioned above.

   Note 272 of the OSC's 2016 Procedures & Guidance document:

   272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

10. **For the avoidance of doubt, Authorising Officers for the purpose of RIPA can authorise 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this Policy are followed. Authorisation can only be granted if it is necessary for the purposes of investigating serious crimes (as defined in Section G – paragraph 9).**

11. **<u>Intrusive Surveillance</u>**

    This is when the surveillance:-

- is covert;
- relates to residential premises and / or private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Surveillance of a place ordinarily used for legal consultation; at a time when they are being used for such consultations is also a form of intrusive surveillance.

12. Areas of a building that are readily visible and accessible to the public are not residential premises. For example, a communal stairway, canteen, reception area, driveway, front garden and so on.

13. Intrusive Surveillance cannot be carried out or approved by the Councils. Only the police and other law enforcement agencies are permitted to use such powers. Likewise, the Councils have no statutory powers to interfere with private property.

14. When considering directed surveillance the following basic points to consider are**:**

Element type	**Consideration**
Is it surveillance?	Are you monitoring/observing the activities/movements of people etc?
Is it covert?	Are you doing it in a way designed to ensure the person is unaware that surveillance is or may be taking place? Overt CCTV systems in the town centre are usually ok, but even they can be used covertly if targeting a specific person/group to record/monitor their activities etc.
Is it a specific investigation or operation?	Town centre CCTV is not usually used for general prevention/detection of crime purposes rather than for a specific investigation (e.g. in relation to a particular individual/group) or a specific operation (e.g. targeting a hotspot such as an area known for anti-social behaviour or fly-tipping)
Are you likely to obtain private information?	This area is a bit vague but probably quite wide.

	It's not just private information about the suspect but also anyone else. It extends beyond personal relationships and includes professional relationships. Private information can include personal data like names, telephone numbers, addresses etc. Recording people's movements and activities (even in public places) for future analysis or consideration.
Is it preplanned?	If this surveillance was an immediate response to something that was not reasonably foreseeable then you won't fall within the definition of directed surveillance.

15. "Proportionality"

Proportionality involves balancing the intrusiveness of the activity on the target subject and others who might be affected by it against the need for the activity in operational terms. Consider the expected benefit to the investigation of the surveillance. The activity will not be proportionate if it is excessive in the circumstances – each case will be judged and be unique on its merits – or if the information which is sought could be reasonably be obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

When authorising covert surveillance, the following elements of proportionality should therefore be considered:

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

16. Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	Police Officer or Parks Warden on patrol Signposted Town Centre CCTV cameras (in normal use). Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	CCTV cameras providing general traffic, crime or public safety information.
Directed must be RIPA authorised	Covert CCTV cameras at a fly-tipping hotspot. Covert and targeted following of a benefit claimant who is suspected of failing to declare earnings from a job.
Intrusive or interfering with private property – **the Council cannot do this!**	Planting a listening or other electronic device (bug) or camera in a person's home or in / on their private vehicle or on their person. Surveillance of a place used for legal consultations.

17. **Further Information** on different types of surveillance can be found in the Home Office Code of Practice on Covert Surveillance: https://www.gov.uk/government/organisations/home-office/series/ripa-codes

18.Confidential Information

Special safeguards apply with regard to confidential information relating to legal privilege, personal information, journalistic material and confidential constituent information. Only the Chief Executive, or in his absence an appointed deputy,

can authorise surveillance likely to involve confidential information. The investigating officer must understand that such information is confidential and cannot be obtained. Further guidance is available in the Home Office Codes of Practice: https://www.gov.uk/government/organisations/home-office/series/ripacodes

19. Is the proposed surveillance discriminatory?

The Councils are under a legal obligation to avoid either direct or indirect discrimination in carrying out their functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the HRA. The Councils need to be sensitive to this issue and ensure that they apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. They should be alert to any assumptions about people from different backgrounds which may not even be consciously held.

20. Collateral Intrusion

Before authorising surveillance, the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (known as collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

21. Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. If the original authorisation is sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required. Further guidance is available in the Home Office Code of Practice.

22. Retention and destruction of product of surveillance

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate GDPR requirements and any relevant codes of practice produced by the Councils relating to the handling and storage of material.

E. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1. **Who is a CHIS?**

This is someone who establishes or maintains a personal or other relationship for the covert purpose of using that relationship to obtain information. This would include, for example, a situation where a Council officer establishes a relationship with another person through social media, even where there is no physical contact with the CHIS. However, a CHIS does not apply in circumstances where members of the public volunteer information to the Councils as part of their normal civic duties, or to contact numbers set up to receive information (e.g. benefit cheat hotlines).

THE COUNCIL IS RELUCTANT TO USE CHIS, AND IF AN OFFICER IS CONTEMPLATING THE USE OF THIS TYPE OF SURVEILLANCE HE/SHE MUST OBTAIN PRIOR ADVICE FROM THE SRO OR RIPA CO-ORDINATING OFFICER. HOWEVER, THE COUNCIL DOES RECOGNISE THAT CIRCUMSTANCES MAY ARISE THAT MAKE THE USE OF A CHIS NECESSARY AS AN INVESTIGATIVE TOOL.

In order to mitigate the risk of a CHIS arising inadvertently during the course of an investigation the Councils will ensure that Authorising and investigating officers are trained in the identification of a CHIS as part of corporate training on RIPA.

Management of a CHIS

Always seek advice from the SRO or the RIPA Co-ordinating Officer prior to authorising a CHIS. In all cases, prior to authorising a CHIS a risk assessment must be undertaken in relation to the source. A CHIS may only be authorised if there will at all times be an officer (referred to as the handler) within the Councils who will have day to day responsibility for dealing with the source on behalf of the Councils in order to protect both the security of the source. The handler is normally the Investigating Officer. In addition, another officer must be appointed (known as the controller) who will have general oversight of the use made of the source. This person is normally the investigating officer's line manager. Lastly, an officer must be identified to maintain certain prescribed records (as specified in the codes of practice) of the use made of the source.

Special requirements apply to the use of a vulnerable individual or a juvenile as a CHIS. Before considering the authorisation of such a person the Authorising Officer must seek legal advice from the RIPA Co-ordinating Officer or the SRO.

2. **Test Purchases**

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 would require authorisation as a CHIS.

3. **Anti-social behaviour activities (e.g. noise, violence, race etc.)**

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

If the sound recording equipment is so sensitive that it can record conversations as if you were in the room, this would be intrusive surveillance and cannot be authorised under RIPA. The noisemaker shall be warned so that it can be overt surveillance.

F. ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

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

2. RIPA defines communications data in three broad categories: -

(a) **Section 21(4) (c) Information about communications service users.**
This category mainly includes personal records supplied to the Communications Service Provider (CSP) by the customer/subscriber. For example, their name and address, payment method, contact number etc.

(b) **Section 21(4) (b) Information about the use of communications services.**
This category mainly includes everyday data collected related to the customer's use of their communications system. For example, details of the dates and times they have made calls and which telephone numbers they have called.

(c) **Section 21(4) (a) Information about communications data (traffic data).**

This category mainly includes network data generated by the CSP relating to a customer's use of their communications system that the customer may not be aware of. For example, cell site data and routing information.

3. **The Councils only have power to request data under Section 21(4) (b) and Section 21(4) (c) but NOT Section 21(4) (a).**

<u>What types of communications data is available to the Councils?</u>

4. **Section 21(4)(c) - Information about communications service users**

- Name of account holder/subscriber;
- Installation and billing address;
- Method of payment/billing arrangements;
- Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to);
- Other customer information such as any account notes, demographic information or sign up data (not passwords or personalised access information).

5. **Section 21(4)(b) - Information about the use of communications services**

- Outgoing calls on a landline telephone or contract or prepay mobile phone
- Timing and duration of service usage;
- Itemised connection records;
- E-mail logs (sent);
- Information about the connection, disconnection and re-connection of services;
- Information about the provision of conference calling, call messaging, call waiting and call barring;
- Information about the provision and use of forwarding/redirection services (postal and telecom);
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

What Purpose Can Communications Data Be Accessed?

6. The Councils can only access communications data for the **prevention and detection of crime or preventing disorder** (Section 22(2) (b) of RIPA).

Applying for Communications Data

7. The Investigating Officer must complete an application form (https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2) in full with no sections omitted. (The form is subject to inspection by the Interception of Communications Commissioner and the applicant may be asked to justify their application).

8. Two forms of authorisation are possible: -

   (a) An authorisation under Section 22(3) of RIPA. This authorises the applicant to personally extract the data from the CSP's records. (This will rarely be used by the Councils as its intended use is where there may be a security breach at the CSP and asking the CSP to provide the data would forewarn or alert the subject).

   (b) A notice under Section 22(4) of RIPA requiring the CSP to extract the communications data specified from its records and to send that data to the Single Point Of Contact (SPOC) (normal request).

   The applicant must indicate which authorisation they seek.

9. The application form is then submitted to the SPOC for the Council, which is the National Anti-Fraud Network (NAFN).

10. The idea of only having one point of contact for each public authority was agreed between the Home Office and the CSP's to ensure data was only supplied to those entitled to obtain the data. Only the SPOC can acquire communications data on behalf of the Council.

11. The SPOC will then assess whether the form is completed properly, that the request is lawful, the request is one to which the CSP can practically respond and that the cost and resource implications for the CSP / Council are within reason.

12. The SPOC will then submit the form to the Authorising Officer for authorisation. (As previously stated, the application form is subject to inspection by the Interception of Communications Commissioner and therefore the Authorising Officer may be called upon to justify any decisions made).

13. The application must then be approved by a Magistrate. The Investigating Officer should liaise with the RIPA Co-ordinating Officer to obtain this authorisation.

14. The RIPA Co-ordinating Officer will arrange a hearing with the Court to seek the Magistrate's approval. They should provide the Court with the application form and supporting information. The investigating officer will be required to attend Court with the Councils' solicitor to seek the Magistrate's approval.

15. Guidance on the procedure for seeking Magistrate's approval can be found at https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

16. If the application is rejected by either the SPOC or the Magistrates, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection.

17. Once authorised by the Magistrates, the SPOC will forward the application to the CSP.

18. Once the data sought is returned to the SPOC, a copy of the information will be passed to the applicant.

19. All original documents will be retained by the RIPA Co-ordinating Officer.

20. There are a number of other administrative forms that the SPOC's are obliged to complete as the application is progressed, although these will not necessarily involve the Investigating Officer.

21. Authorisations to collect communications data under s22 (3) have a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice. Magistrates would need to approve any renewal.

22. If you are at all unsure about anything to do with acquiring communications data, please contact the SPOC, the SRO or the RIPA Co-ordinating Officer for advice **before** applying.

G. AUTHORISATION PROCEDURES

1. Directed surveillance can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

2. All RIPA surveillance authorisations (i.e. Directed Surveillance and the acquisition of Communications Data) must be approved by a Magistrate before they take effect.

Authorising Officers

3. RIPA Forms can only be signed by Authorising Officers.

4. Authorisations under RIPA are separate from delegated authority to act under the relevant Councils' Scheme of Delegation. All RIPA authorisations are for specific investigations only, and must be reviewed, renewed or cancelled once

the specific surveillance is complete or about to expire. **The authorisations do not lapse with time! The Authorising Officer must ensure that an authorisation is cancelled as soon as it is no longer required.**

Training Records

5. Appropriate training will be given (or approved) by the RIPA Co-ordinating Officer before Authorising Officers are certified to sign any RIPA Forms.

6. If the SRO feels that an Authorising Officer has not complied fully with the requirements of this Policy, or the training provided to them, she is duly authorised to retract that officer's authorisation until they have undertaken further approved training.

Application Forms

7. Only the Home Office approved RIPA forms must be used. Any other forms used, will be rejected by the Authorising Officer and/or the RIPA Co-ordinating Officer. All the RIPA forms can be found at: https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

Grounds for Authorisation

8. Acquisition of communications data can only be authorised by the Councils on the grounds of preventing/detecting crime/disorder. No other grounds are available to local authorities.

9. Directed Surveillance can only be authorised for investigating serious criminal offences. 'Serious' means criminal offences that are punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment. Serious criminal offences would include dangerous waste dumping and serious or serial benefit fraud. We cannot carry out Directed Surveillance for offences that would only result in a fine or less than sixth month's imprisonment, such as littering or dog fouling.

Assessing the Application Form

10. Before an Authorising Officer signs an application form, they must:-

(a) Be mindful of this Policy, the training provided or facilitated by the RIPA Co-ordinating Officer and any other guidance issued, from time to time, by the SRO or the Home Office on such matters.

(b) Satisfy themselves that the RIPA authorisation is:-

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case and on the grounds of preventing or detecting crime or preventing disorder;

(iii) for directed surveillance, it must be necessary for the investigation of a serious criminal offence; **and**

(iv) **proportionate** to what it seeks to achieve (see comments in Section D).

(c) In considering necessity, remember that the surveillance must be necessary for the purpose of preventing or detecting crime or of preventing disorder. There should be details of the crime(s) relied upon in the application form. In addition you need to ensure that the crime attracts a custodial sentence of a maximum of 6 months or more, or involves an offence under section 146, 147 or 147A of the Licensing Act 2003. Authorising Officers also need to demonstrate that there were no other means of obtaining the same information in a less intrusive way.

(d) In assessing whether or not the proposed surveillance is proportionate, an Authorising Officer should consider the following:-

(i) balance the size and scope of the proposed surveillance against the gravity and extent of the perceived crime or offence;

(ii) will the surveillance method to be used cause the least possible intrusion on the target and others?

(iii) is the surveillance an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the evidence? And

(iv) what other methods of evidence gathering have been considered and why were they not used?

(e) Always remember that the **least intrusive method will be considered proportionate by the courts.**

(f) Take into account the risk of intrusion into the privacy of persons other then the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality.

(g) Set a date for review of the authorisation and review on that date using the relevant form. Authorisations for directed surveillance should be reviewed at least once a month.

(h) Ensure that the originals of all RIPA forms (applications, review, renewal and cancellation) are forwarded to the RIPA Co-ordinating Officer, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**.

(i) In the case of notices relating to communications data, these will be kept by the RIPA Co-ordinating Officer.

(j) **If unsure on any matter, obtain advice from the SRO or the RIPA Co-ordinating Officer before signing any forms**.

Magistrate's Approval

11. After the Authorising Officer has signed the RIPA application form, it must be approved by a Magistrate before the operation can commence. The Investigating Officer should liaise with the RIPA Co-ordinating Officer to seek this authorisation.

12. The RIPA Co-ordinating Officer will arrange a hearing with the court to seek the Magistrate's approval. They should provide the court with the RIPA application form (signed by the Authorising Officer) and supporting information. The Investigating Officer and Authorising Officer will be required to attend court with the Council's Solicitor to seek the Magistrate's approval.

13. Guidance on the procedure for seeking Magistrate's approval can be found at: https://www.gov.uk/government/publications/changes-to-local-authority-use-fripa

Duration

14. The RIPA authorisation **must be reviewed or renewed in the time stated or cancelled** once it is no longer needed. Authorisation to carry out Directed Surveillance lasts for a maximum of 3 months from authorisation. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the authorisation is 'spent'. In other words, **the authorisation does not expire!** The authorisation has to be reviewed, renewed and/or cancelled once it is no longer required.

15. Magistrate's approval is required to renew an authorisation. There is no requirement for Magistrates to consider either cancellations or internal reviews.

16. Notices/Authorities issued under s22 compelling disclosure of communications data are only valid for one month but can be renewed for subsequent periods of one month, at any time. Again, Magistrate's approval will be required for a renewal.

17. Authorisations can be renewed in writing before the maximum period in the Authorisation 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. Magistrate's approval will then be required.

18. An Authorisation cannot be renewed after it has expired. In such event, a fresh application will be necessary.

H. WORKING WITH / THROUGH OTHER AGENCIES

1. When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and the Home Office approved application forms must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be explicitly made aware what they are authorised to do.

2. When another agency (e.g. Police, DWP, Trading Standards, etc):-

   (a) wish to use the Councils' resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Councils' resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the Councils' record (a copy of which must be passed to the RIPA Co-ordinating Officer for the Central Register) 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 Councils' premises for their own RIPA action, and is expressly seeking assistance from the Councils, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Councils' premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Councils' cooperation in the agent's RIPA operation. In such cases, the Council does not require its own RIPA form as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a) above, if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, 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.

4. **If in doubt, please consult with the SRO or the RIPA Co-ordinating Officer at the earliest opportunity.**

I. RECORD MANAGEMENT

1. **The Council must keep a detailed record of all Authorisations, Reviews, Renewals, Cancellations and Rejections for each respective service area. A Central Register of all Authorisation Forms will be maintained and monitored by the RIPA Co-ordinating Officer. All original forms (Authorisation, Review, Renewal, Cancellation) must be sent to the RIPA Co-ordinating Officer as soon as practicable.**

2. **Records maintained in the Service Area**

The following documents must be retained by the relevant Assistant Director (or their designated administrator) for such purposes:

- a copy of all RIPA forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer; and
- the Unique Reference Number for the authorisation (URN).

Central Register maintained by the RIPA Co-ordinating Officer

3. Each form will have a unique reference number (URN). The RIPA Co-ordinating Officer will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the forms for audit purposes. Rejected Forms will also have URN's.

4. Authorising Officers must forward a copy of every completed RIPA form to the RIPA Co-ordinating Officer for the Central Register, within 1 week of the Authorisation, Review, Renewal, Cancellation or Rejection. The RIPA Co-ordinating Officer will monitor the same and give appropriate guidance, from time to time, as necessary.

5. The Council's will retain records for a period of at least three years from the ending of the Authorisation. The IPCO can audit/review the Councils' policies and procedures, and individual Authorisations, Reviews, Renewals, Cancellations and rejections.

J. TRAINING

1. Appropriate corporate training will be arranged by the RIPA Co-ordinating Officer for all officers likely to make applications or authorise them.

2. The RIPA Co-ordinating Officer will ensure suitable training is in place for all members of staff who undertake an enforcement role. This may be by way of an

external trainer; briefing to officers or an e-learning module. Managers of enforcement teams must ensure new staff undertake RIPA training within six months of their starting date.

3. Authorising Officers must receive regular training as described above.

4. The cost of such external training should be met from the budget of the individual service areas affected.

5. No officer will be permitted to undertake the role of the Authorising Officer unless they have undergone suitable training approved by the RIPA Co-ordinating Officer.

K. Review of this Policy and the Councils' activities

1. This Policy will be regularly reviewed by the Senior Responsible Officer and the RIPA Co-ordinating Officer in relation both to legal developments and for the purpose of monitoring practice and procedure.

2. Members of the Councils' Cabinet will approve the RIPA Policy on an annual basis or before if there are any significant legal developments impacting on the Councils.

3. Members will also receive the following information:

Information to be provided	Frequency
The number of RIPA authorisations requested and granted	Annual report
The number of joint operations where RIPA authorisation has been sought and granted by another authority	Annual report
The number of times social networking sites have been viewed in an investigatory capacity	Annual report

L. CONCLUDING REMARKS

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Policy, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this Policy will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. **Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to consider a RIPA form. They must never sign or rubber stamp forms without thinking about their own personal and the Council's responsibilities.**

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

5. For further advice and assistance on RIPA, please contact the SRO or the RIPA Co-ordinating Officer.

Appendix 1

Responsible Officers

Senior Responsible Officer	**Post Held**
Emily Yule	Assistant Director – Law & Governance and Monitoring Officer
RIPA Co-ordinating Officer	**Post Held**
John Snell	Corporate Manager – Internal Audit (and Deputy Monitoring Officer)
Authorising Officers	**Post Held**
Arthur Charvonia	Chief Executive
Tom Barker	Assistant Director – Planning for Growth
Gavin Fisk	Assistant Director - Housing

Appendix 2

For the latest forms please go to this link:

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

Magistrate's Court Authorisation Procedure

Appendix 3

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE