North Northamptonshire Council

Guidance on the use of RIPA and IPA powers

June 2022

www.northnorthants.gov.uk

Document Version Control

Author (Post holder title):	Director of Governance & HR
Type of document:	Policy
Version Number:	1.0
Document File Name:	
Issue date:	May 2022
Approval date and by who (CMT / committee):	
Document held by (name/section):	
For internal publication only or external also?:	Internal
Document stored on Council website or Intranet?:	
Next review date:	June 2023

Change History

Issue	Date	Comments

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)

Distribution List

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)

Links to other documents

Document	Link

Contents

Purpose of document

1. The purpose of this document is to explain the scope of RIPA and IPA and provide guidance on approval / authorisation procedures. It should be read in conjunction with the North Northamptonshire Council ('NNC') Policy on RIPA.

2. Advice from the Senior Responsible Officer (i.e. the Director of Governance & HR), Assistant Director of Regulatory Services or the Trading Standards Manager should be sought at first instance in the event of any query as to the application of the policy or the interpretation of these guidance documents. Legal advice must be sought in advance of any use of the techniques regulated by RIPA.

RIPA in a nutshell

3. RIPA provides a **lawful means** for public authorities to breach the so-called right to privacy which is contained in the European Convention on Human Rights.

4. Two forms of covert surveillance activities

    - the use of '**directed surveillance**' - such as watching, following or listening to people;
    - the use and conduct of '**covert human intelligence sources**' (CHIS) - such as obtaining information about people covertly through informants, infiltrators;

    can be authorised under RIPA by a senior, competent officer of a local authority for the purpose of preventing or detecting crime or of preventing disorder, where it is necessary and proportionate to do so.

5. Also, the **obtaining of communications data** (such as telephone subscriber information – but not the contents of calls or messages) can be similarly authorised under IPA.

6. The authorisation level, when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a CHIS, is the Head of Paid Service (i.e. the Chief Executive) or (in their absence) the person acting as the Head of Paid Service. These instances are extremely rare.

7. Elected members of a local authority have certain responsibilities relating to policy.

8. A senior responsible officer, who should be a member of the authority's corporate leadership team, has specified operational oversight responsibilities.

9. RIPA / IPA authorisation by local authorities require:

- additional judicial (magistrate's) approval for all local authority RIPA authorisations; and
- directed surveillance to be confined to cases where the offence under investigation carries a maximum custodial sentence of 6 months or more (unless they relate to investigations into underage sales of alcohol and tobacco – including nicotine inhaling products and proxy purchasing).

10. RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance etc. and lack of authorisation does not necessarily mean that the carrying out of surveillance etc. is unlawful. However, failure to seek a RIPA authorisation where one is available could lead to a civil action against a local authority for acting in a way which is incompatible with a person's human rights. In addition, a court may refuse to allow evidence which has been obtained as a result of unauthorised conduct to be admitted in a criminal case.

11. Unauthorised surveillance etc. by an officer does not lead to the commission of a criminal offence under RIPA. However unlawfully obtaining communications data under IPA can constitute an offence.

12. The fact that particular conduct cannot be authorised under RIPA does not necessarily mean that the actions proposed cannot be lawfully undertaken – providing it is necessary proportionate and has been approved, with a verifiable audit similar to the process and documentation for RIPA.

13. Local authorities are subject to oversight provisions by the Investigatory Powers Commissioner (IPC). The Investigatory Powers Tribunal (IPT) was created to investigate complaints about covert conduct by various public bodies.

14. Guidance on the application of RIPA and IPA is provided by statutory Codes of Practice, the IPC, and Office of Surveillance Commissioners (OSC) Guidance (which is still relevant despite being formally withdrawn upon the IPCO replacing the OSC).

Summary of key guidance points

15. In relation to authorisations for **obtaining communications data** (see flowchart at Appendix 1):

- "Communications Data" (CD) includes the 'who', 'when', 'where', and 'how' of a communication, but not the content i.e. what was said or written. The Council may only acquire less intrusive types of CD; "Entity data" (e.g. the **identity of the person to whom services are provided**) or "Events Data" (e.g. the **date and time sent, duration, frequency of communications**). The l**ocation of the entity or events data** at the time the communication is sent or received may also be obtained in appropriate cases. The Council is prohibited from obtaining "Content Data", the meaning of the

communication, (e.g. what the communication says or contains).

- Requests to obtain communications data must be approved.
- Requests to obtain communications data will only be approved for the purpose of preventing or detecting of crime or of preventing disorder.
- Officers need to avoid the possibility of making, or being a party to, unlawful interceptions of communications data.
- Additional approval by the Office for Communications Data Authorisations (OCDA) is required for all local authority IPA authorisations before they can be given effect.
- The Council uses the National Anti- Fraud Network (NAFN) service to manage all applications for the obtaining of communications data.

16. In relation to s**urveillance and covert human intelligence sources** (see flowchart at Appendix 2):
    - Officers who may be engaged in any form of **covert enforcement activity** must ensure that it is considered for authorisation before carrying it out.
    - Directed surveillance and the use or conduct of covert human intelligence sources must be authorised.
    - Authorisations for directed surveillance and the use or conduct of covert human intelligence sources will only be granted for the **prevention or detection of crime.**
    - Officers must not undertake intrusive surveillance.
    - An authorising officer must consider applications for authorisation having regard to **necessity, proportionality and collateral intrusion**.
    - An authorising officer must grant all authorisations in writing.
    - Additional **judicial (magistrate's) approval** is required for all local authority RIPA authorisations before they can be given effect.
    - An authorising officer will undertake regular **reviews** of authorisations and **cancel** those where the conduct no longer meets the criteria for which they were originally authorised.
    - Any officer who becomes aware of a matter which suggests a complaint being made about a Service activity being responsible for any interference with the privacy of an individual, should draw the matter to the attention an authorising officer without undue delay.
17. Additionally, in relation to **surveillance**:
    - Directed surveillance may only be granted where it complies with the following two conditions:
    - The first condition is that the authorisation is for the purpose of **preventing**

or detecting conduct which:

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

- The second condition is that the criminal offence or one of the criminal offences referred to in the first condition is or would be:

  (a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of **at least 6 months of imprisonment**, or

  (b) an offence under sections 146, 147 or 147A of the Licensing Act 2003 (Sale of alcohol to children, Allowing the sale of alcohol to children & Persistently selling alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco and cigarette papers to children) or sections 91 or 92 of the Children and Families Act 2014 (purchase of tobacco, nicotine products etc. on behalf of persons under 18 & prohibition of sale of nicotine products to persons under 18)."

18. The RIPA Policy cannot be considered in isolation but must be applied in conjunction with other relevant policies relating to enforcement, CCTV, information governance etc.

Roles and Responsibilties

Senior Responsible Officer (SRO):

19. The role of SRO for RIPA and IPA matters will be undertaken by the council's Director of Governance and HR. In accordance with good practice the SRO will be responsible for:

a) The integrity of the process in place within the council for the management of CHIS and Directed Surveillance;

b) Ensuring that all authorising officers are of an appropriate standard;

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

d) 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;

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

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

Authorising Officers

20. The officers named in Appendix 3 shall be the only officers within the council who can authorise applications under RIPA in accordance with the procedures set out in this policy.

21. 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. The officer who authorises a RIPA application should ideally 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.

22. Authorising Officers must have a full understanding of where all relevant data in respect of authorised activities are stored.

RIPA Record Keeping Officer

23. The post holder appointed RIPA Record Keeping Officer is identified in Appendix 3. The RIPA Record Keeping Officer shall:-

    a) have overall responsibility for the management and oversight of requests and authorisations under RIPA;

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

    c) 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;

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

    e) chase failures to submit documents and/or carry out reviews / cancellations;

    f) be responsible for organising a corporate RIPA training programme;

    g) ensure corporate awareness of RIPA and its value as a protection to the council is maintained;

    h) produce a report to the council's Audit and Governance Committee on the council's use of RIPA, as detailed in paragraph 24 below.

Councillors

24. Members of the council's Audit and Governance Committee will approve the RIPA policy on an annual basis and will receive the following information:

Information to be provided	Frequency
No. of RIPA authorisations requested and granted	Annual report, with details of individual authorisations (suitably anonymised) provided to the next available meeting
No. of Joint operations where RIPA authorisation has been sought from, and granted by, another authority	Annual report, with details of individual authorisations (suitably anonymised) provided to the next available meeting
No. of times social networking sites have been viewed in an investigatory capacity	Report to each meeting of the Committee

25. Further, the SRO shall report usage of the investigatory powers to the Executive on a monthly basis.

Authorisations for obtaining communications data

26. The Data Retention and Acquisition Regulations (SI 2018/1123) changed the way in which local authorities access communications data. The Regulations amended both the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 by creating a new authorisation process for public bodies that seek to obtain communications data for a specific criminal investigation. Previously judicial oversight for applications by local authorities to obtain communications data rested with magistrates' courts. This, however, has now been transferred to a new independent body established by the Government, the **Office of Communications Data Authorisations (OCDA)**, which will consider and authorise all future requests.

27. The legislation also requires authorities to enter into a **formal collaboration agreement with the National Anti-Fraud Network (NAFN)** an organisation, hosted by Tameside Metropolitan Borough Council which specialises in providing data and intelligence services to enforcement agencies. NAFN will in future act as the single point of contact between any communications service provider and the Council and prepare on the Council's behalf any applications to the OCDA.

28. An application to obtain communications data must first receive senior internal approval by the delegated designated person before it can be submitted to the OCDA for consideration. An application will therefore only be referred to the OCDA if it first meets the Council's own necessity and proportionality test.

29. Local authorities are permitted to acquire the less intrusive types of communications data, now referred to as '*entity' data* (e.g., the identity of the person to whom services are provided) and '*events' data* (e.g. the date and type of communications, time sent, and duration, frequency of communications). However, it will remain the case that under no circumstances will it be permitted to obtain or intercept the content of any communications.

30. In order to obtain either type of data, in addition to satisfying the necessity / proportionality test, an authority previously had to show the purpose for the application was for the prevention and detection of a crime. This remains the same for *'entity'* data. However, **for *'events'* data, the threshold has been raised and the purpose must now be for the prevention or detection of a *'serious'* crime** (e.g., an offence for which an individual could be sentenced to imprisonment for a term of 12 months or more, or offences which involve, as an integral part, the sending of a communication or a breach of a person's privacy).

Interception of communications

31. With certain exceptions, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be **authorised only by warrant issued by the Secretary of State.**

32. There are no provisions which enable officers of a local authority to lawfully intercept communications.

33. It should be noted that a person who, intentionally and without lawful authority, intercepts any communication in the course of transmission by means of a public postal / telecommunication service or a private telecommunication system, commits an offence.

34. Officers need to avoid the possibility of making, or being a party to, unlawful interceptions.

Recording of telephone conversations

35. An exception to the rule that interception of telephone conversations must be warranted, includes a situation where one party to the communication consents to the interception. In these circumstances, it may be authorised in accordance with section 48(4) RIPA. In such cases, the interception is treated as directed surveillance (see Guidance Note on Surveillance and Covert Human Intelligence Sources).

Authorisation of surveillance and human intelligence sources

36. Some enforcement investigations may require or involve covert techniques i.e. where the gathering of information is carried out in a manner calculated to ensure that the person subject to the activity is unaware that it is taking place,

and it is likely that such operations will come within the scope of Part II of RIPA.

37. Part II of RIPA provides a statutory basis for the authorisation and use by a local authority of **covert surveillance, agents, informants and undercover officers.**

38. Officers who may be engaged and authorised, if appropriate, in any form of covert enforcement activity must ensure that it is considered for authorisation before carrying it out.

39. Whilst the availability of an authorisation under RIPA does not mean that it is unlawful not to seek one, failure to do so could possibly lead to a civil action against the Council for acting in a way which is incompatible with a person's human rights. In addition, a court may refuse to allow evidence, which has been obtained as a result of unauthorised conduct, to be admitted. Unauthorised surveillance does not, however, lead to the commission of a criminal offence.

40. RIPA is supported by C**odes of Practice on Surveillance and The Use and Conduct of Covert Human Intelligence Sources.** These Codes provide guidance on how to ensure operations comply with the Act. These are available on the Home Office website along with the relevant forms to complete:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

41. The Office of Surveillance Commissioners issued Procedures and Guidance in July 2016 that could be considered however this was formally withdrawn in April 2021. No replacement guidance has been issued by the IPCO therefore the OSC guidance may still be a useful point of reference.

https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

Conduct which may be authorised

42. Part II of RIPA applies to three types of conduct - directed surveillance, intrusive surveillance and the conduct and use of covert human intelligence sources.

Definitions

43. The following information explains the meaning of these types of conduct and associated expressions.

Surveillance

44. **“Surveillance”** includes

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device, e.g. any apparatus designed or adapted for use in surveillance.

45. Surveillance does not include the conduct / use of a source (see below) for obtaining or recording any information which is disclosed in the presence of the source.

46. Surveillance is ***“covert”*** if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is and may be taking place. However, case law suggests that the use of bodyworn cameras may amount to surveillance.

47. “**Intrusive surveillance**” is covert surveillance that:

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

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

NOTE: ***An authorisation for intrusive surveillance can only be obtained for the purpose of preventing or detecting serious crime and cannot be issued by officers of a local authority.***

Therefore, officers must not undertake intrusive surveillance.

48. “**Directed surveillance**” is covert surveillance, but not intrusive, and undertaken:

a) for the purposes of a s**pecific investigation or specific operation**;

b) in such a manner as is likely to result in the o**btaining 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 Part II of the 2000 Act to be sought for the carrying out of the surveillance. 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.

49. It can be seen from this that a **wide range of covert enforcement activities potentially fit within the meaning of directed surveillance**, such as

- following a person (e.g. to find out his home address)
- observing a person (e.g. to see if he sells cars from his home premises)
- using a surveillance device to listen to or to photograph or to video a person (e.g. to monitor traders carrying out servicing or repairs or to record a one-day sale)
- the one-sided consensual interception of a telephone conversation (which is regarded as directed surveillance see RIPA section 48(4)) (e.g. recording telephone contacts at tyres / exhaust seller by telephone to price quotations following complaints of misleading price indications being given or ordering a takeaway meal requesting no peanuts)
- monitoring a person's social media pages (e.g. to see if they are selling counterfeit goods)

In practice, virtually any use that is made of covert enforcement techniques should be considered for authorisation.

50. **Test purchasing** - In a number of situations officers or external test purchasers will be tasked with buying goods on behalf of the Service to determine compliance with legislation. In some cases, this activity may be observed by another officer for evidential reasons. Where such activity is conducted in part of a business premise to which the public have access for the purpose of conducting such transactions it is unlikely that any business staff would have an expectation that their conduct, conversations etc. were in private. Therefore, it is unlikely that any private information would be obtained and a directed surveillance authorisation is not likely to be required. However, each situation must be considered on its own merits and advice sought from an authorising officer where any doubt exists and a record kept of the decision making process.

51. **"Private information"**, in relation to a person, includes any **information relating to a person's private or family life**. Decisions of the European Court of Human Rights support the concept of private information being broadly interpreted to include an individual's private or personal relationship with others and activities which take place in the course of their employment and business. Family life should be treated as extending beyond the formal relationships created by marriage.

52. Data which is accessible to the public, such as entries in a telephone directory, an electoral role or from the Driver and Vehicle Licensing Centre, would not be regarded as private information.

Covert human intelligence source

53. A person is a "covert human intelligence source" (described in this guidance note both as a CHIS or a source) if:

    a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c);

b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) they covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

54. If it were ever desirable to use a third party CHIS, then arrangements should be sought for Northamptonshire Police to manage the CHIS. It will only be appropriate to utilise an officer of the Service as a CHIS where their security and welfare can be properly managed.

55. Persons who voluntarily share knowledge / information as part of their own feeling of civic duty are not considered to be a CHIS. Officers **must not ask such persons to do anything on behalf the Service**.

Age-restricted sales

56. A young person who is used by the Service to assess compliance with laws concerning age-restricted goods, by test purchasing, is n**ot regarded as a CHIS** because the person does not establish or maintain any form of relationship with the seller, but particular consideration should be given to the child's safety and welfare before each exercise.

57. It is noted that the procedures under RIPA are not intended that an authorisation should be sought each time a source is tasked – however a separate application should be made for each occasion that a source is deployed to test purchase from persons who are not part of the same operation / investigation.

58. Officers considering the ***use of an informant*** (i.e., not an undercover officer) should first discuss the proposal with an authorising officer before any approach is made to Northamptonshire Police.

Online covert activity

59. The Covert Surveillance and Property Interference Code of Practice gives guidance on this area and it is reproduced below:

> 3.10 The growth of the internet, and the extent of the information that is now available online, presents **new opportunities for public authorities to view or gather information** which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make f**ull and lawful use of this information for their statutory purposes.** Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. W**here online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered,** as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to **engage with others online without disclosing his or her identity, a CHIS authorisation may be needed** (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 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, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 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.

3.14 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.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the **nature of the public authority'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 a public authority 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. See also paragraph 3.6.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to **look at the intended purpose and scope of the online activity it is proposed to undertake**. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 I**nternet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation** (see paragraph 4.32).

Example: *Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

60. The Office of Surveillance Commissioners issued the following guidance in relation to the covert surveillance of social networking sites, which has since been withdrawn due to the OSC being replaced by the Investigatory Powers Commissioners Office, however the principles addressed remain valid:

> 289 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that services provided by a single provider are the same.
>
> 289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data must 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 (instant messages for example). Where privacy settings are available but not applied the

data may be considered open source and authorisation is not usually required. **Repeat viewing of 'open source' sites may constitute directed surveillance** on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly 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).

289.3 It is **not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation** for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not 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 whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e., the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

61. Any officer considering carrying out any covert online activity or covert surveillance of social networking sites who has any concerns about it must speak to the Director Governance & HR or the Assistant Director, Regulatory Services before doing so.

Process for authorisation of directed surveillance and CHIS

62. If a proposed enforcement activity is considered to be the undertaking of directed surveillance or the use of a CHIS, the investigating officer should consult with their Line Manager, before completing the appropriate application. Before submitting an application, the investigating officer should believe that there is definitely a **need for the proposed activity** to be conducted and that there is **not an alternative** way in which the information etc could be obtained without an interference with any person's privacy.

Stage 1: A written application for authorisation is made by the investigating officer to the authorising officer

63. Where an investigation involves a number of officers, the officer in charge must make the application. The authorising officers will not authorise their own conduct. The relevant forms to complete can be found at: https://www.gov.uk/search?q=ripa+forms

64. In completing applications particular regard should be had to the following:

- The consideration of **necessity** requires thought to be given to the reasons why it is necessary to use covert surveillance or a CHIS in the investigation
- **Proportionality** requires consideration of the following elements:
  - 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
  - Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented
- **Collateral intrusion –** measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance / undercover activity. Where such intrusion is unavoidable, the activities may still be authorised, provided the intrusion is considered proportionate to what is sought to be achieved. The same tests above should be applied.
- **Confidential information –** when considering whether confidential information is likely to obtained it is generally considered that it is improbable that local authority officers to acquire such information. In most cases the likelihood of acquiring such information will be 'none'.

65. Covert surveillance that is likely to reveal private information about a person but is carried out by way of an **immediate response to events** such that it is not reasonably practicable to obtain an authorisation under the 2000 Act, would not require a directed surveillance authorisation.

66. The 2000 Act is not intended to prevent law enforcement *officer*s fulfilling their legislative functions. To this end section 26(2)(c) of the 2000 Act provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances the nature of which is such

that it is not reasonably practicable for an *authorisation* to be sought for the carrying out of the surveillance.

67. The use of a CHIS, as stated above, will be restricted to an officer of the local authority acting undercover and is only likely to be appropriate for relatively basic activity such as test purchasing from social media sites where illegal goods are being offered for sale. Remember, the Police have trained undercover officers who may be more appropriate to try to use.

68. There are specific rules relating to the management of a CHIS that must be followed and are detailed in the Code of Practice:

    a) RIPA requires that a 'handler' has **day to day responsibility** for dealing with the CHIS on behalf of the Council, directing the day to day activities of the CHIS, recording the information supplied by the CHIS and monitoring the CHIS's security and welfare.

    b) RIPA also requires that a 'controller' will have responsibility for the **management and supervision of the handler** and general oversight of the CHIS.

    c) A **risk assessment** must be carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset, including the potential to have to disclose information tending to reveal the existence or identity of the CHIS to or in court.

    d) The handler is responsible for **alerting the controller to any concerns** about the personal circumstances of the CHIS insofar as they might affect the validity of the risk assessment, the conduct of the CHIS and the safety and welfare of the CHIS. Where appropriate concerns about such matters must be considered by the authorising officer and a decision taken on whether or not to allow the authorisation to continue.

    e) Detailed records must be kept of the **authorisation and use** made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000 SI No. 2725 details the particulars that must be kept in the records.

69. Normally, the handler will be the immediate line manager of undercover officer with their line manager being the controller.

70. The risk assessment in c) above shall be carried out using the relevant risk assessment paperwork available on the Health & Safety pages of the intranet.

71. It will be usual practice for the handler to also be responsible for maintaining the detailed records referred to in e) above.

Stage 2: The authorising officer considers the application, having regard to necessity, proportionality and collateral intrusion

72. The authorising officer must consider the application against the criteria set out under RIPA. Following inspections from the Office of Surveillance Commissioners it has been agreed that all applications will be forwarded for legal advice and the application will not be approved by the authorising officer until it has been received.

73. The Authorising Officers within the Council are set out in Appendix 3.

74. ***Necessity.*** An authorisation may be granted by an authorising officer where he firstly believes that the authorisation is ***necessary*** in the circumstances of the particular case **for the purpose of preventing and detecting crime or preventing disorder**.

    Note that RIPA authorisations for local authority conduct may NOT be given for other purposes e.g., in the interests of public safety; or for the purpose of protecting public health.

75. ***Proportionality.*** If the conduct is necessary, the authorising officer must believe that it is ***proportionate*** to what is sought to be achieved by it. This involves balancing the intrusiveness of the conduct against the need for the conduct to be used in operational terms. **The conduct will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.** The conduct should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way. The proportionality test is defined as follows:

    > Even if a particular policy or action which interferes with a Convention right pursues a legitimate aim (such as the prevention of crime) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Public authorities must not use a sledgehammer to crack a nut. Even taking all these considerations into account, interference in a particular case may still not be justified because the impact on the individual or group is just too severe.

76. ***Collateral intrusion*****.** Before authorising directed surveillance or the use or conduct of a source, 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 operation or investigation (***collateral intrusion***). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

77. An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the directed surveillance or the use and conduct of a source.

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

79. An officer granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the directed surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of directed surveillance.

80. There is no additional authorisation requirement where the proposed use or conduct of a CHIS involves the ***use of a surveillance device.***

81. Particular information should be given in any application for authorisation in cases where the subject of the investigation or operation might reasonably assume a high degree of privacy or ***confidential information*** (matters subject to legal privilege, confidential personal information or confidential journalistic material) is involved. No special protection is provided under RIPA for such cases, but a higher level authorisation is prescribed in the Codes where it is likely that confidential information will be acquired – for local authorities it is "The Head of Paid Service or (in his absence) a Chief Officer".

Stage 3: The authorising officer grants/does not grant the authorisation.

82. All authorisations will be granted in writing. The Council will not permit exceptions to this principle, even where, it is accepted, that, in urgent cases, authorisations may be given orally. Officers need to ensure, therefore, that, in planning enforcement programmes and investigative activities, they consider whether authorisations may be required.

Stage 4: Judicial approval

83. Details of the judicial approval process can be found at: http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/?view=Standard&pubID=1079688

    Officers shall follow this guidance in seeking the relevant judicial approval. It is Council policy that both the applicant and authorising officer should attend the hearing where judicial approval is sought.

84. ***Records***: All RIPA documentation must be provided to the Assistant Director, Legal and Democratic Services for inclusion in the Central Record of Authorisations.

Stage 5 - Reviews

85. The authorising officer will undertake regular reviews of authorisations to assess the need for the conduct to continue in accordance with the required timescale. The results of reviews will be recorded.

Stage 6 - Renewals

86. Unless renewed or cancelled, authorisations are valid for a period of 3 months (for directed surveillance) and 12 months for a CHIS (one-month if the person

is a juvenile). **Renewals are not automatic** and must be applied for with the same rigour as the original application.

87. A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An **application for renewal** should not be made until shortly before the authorisation period is drawing to an end. If at any time before an authorisation would cease to have effect, an authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period.

88. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

Stage 7 - Cancellations

89. Authorisations must **never be allowed to simply lapse**. An applying officer is expected to apply for the cancellation of an authorisation once the need for the authorisation has finished.

90. An authorising officer must cancel the authorisation if satisfied that the authorisation is no longer appropriate and proportionate to the circumstances.

Ceasing of surveillance activity

91. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded.

92. The requirements of the Regulation of Investigatory Powers (Source Records) Regulations 2000 should be noted in relation to records which are kept for the conduct or use of a covert human intelligence source.

Records

Central Record

93. There are requirements under the relevant codes of practice to keep a central record of authorisations and to maintain a central retrieval system for all authorisations for a period of at least 5 years from the ending of the authorisation. These records are maintained by the Senior Responsible Officer, who shall ensure compliance with the requirements of the Codes and authorise disposal of records having regard to whether such records may need to be retained under other legislative requirements such as the Criminal Procedures and Investigation Act 1996.

Data Retention

94. In addition, consideration must be given to the retention of data obtained under a directed surveillance authorisation. This must be retained in

accordance with the Council's retention policy. Care must be taken that data stored on all pathways is appropriately disposed of:

> For example, data may be obtained (e.g. CCTV) and stored onto a CD which would be stored in a secure cabinet. A copy of this data is then e-mailed to a colleague and their manager who both store it in Outlook. The manager then e-mails it to a legal colleague so that it may be assessed and they also save it in Outlook.

The data held on all of these different pathways must be managed as part of the disposal process.

Non-RIPA activity

95. Councils can undertake surveillance without the benefit of a RIPA authorisation – usually because an authorisation is unavailable under the Act due to the matter being civil in nature, or for an offence without the required sentencing powers. This could include, for example when the police, by consent, seek to deploy a camera within the house of a vulnerable person in order to investigate allegations of doorstep 'scams'.

96. As much care should be taken in these cases as when a RIPA authority is available in order to ensure that the activity is subject to appropriate oversight. The Council has therefore decided to implement a non-statutory authorisation process that runs in parallel to any RIPA approvals. We will review the adequacy of these arrangements throughout 2018. The IPC does not seek in any way to discourage 'non-RIPA' surveillance but instead public authorities should usually follow a RIPA-style approach in these circumstances.

Complaints procedure

97. RIPA establishes an independent Investigatory Powers Tribunal which can deal with a number of issues - including any complaint by a person who believes that they have been subject to the use of investigatory powers under RIPA in challengeable circumstances (which are set out in RIPA).

98. Any officer who receives or becomes aware of a matter which suggests a complaint being made about any interference with the privacy of an individual, in addition to recording the matter as a customer complaint and following internal council procedures, should draw the matter to the attention of the authorising officer without undue delay so that appropriate information and advice can be given about contacting the Tribunal etc. Contact details for the Investigatory Powers Tribunal are as follows:

> The Investigatory Powers Tribunal,
> PO Box 33220
> London
> SW1H 9ZQ
>
> Tel: 0207 035 3711

Authorising Officer Contact Details

Assistant Director, Regulatory Services
Iain Smith – 01536, @northnorthants.gov.uk etc.

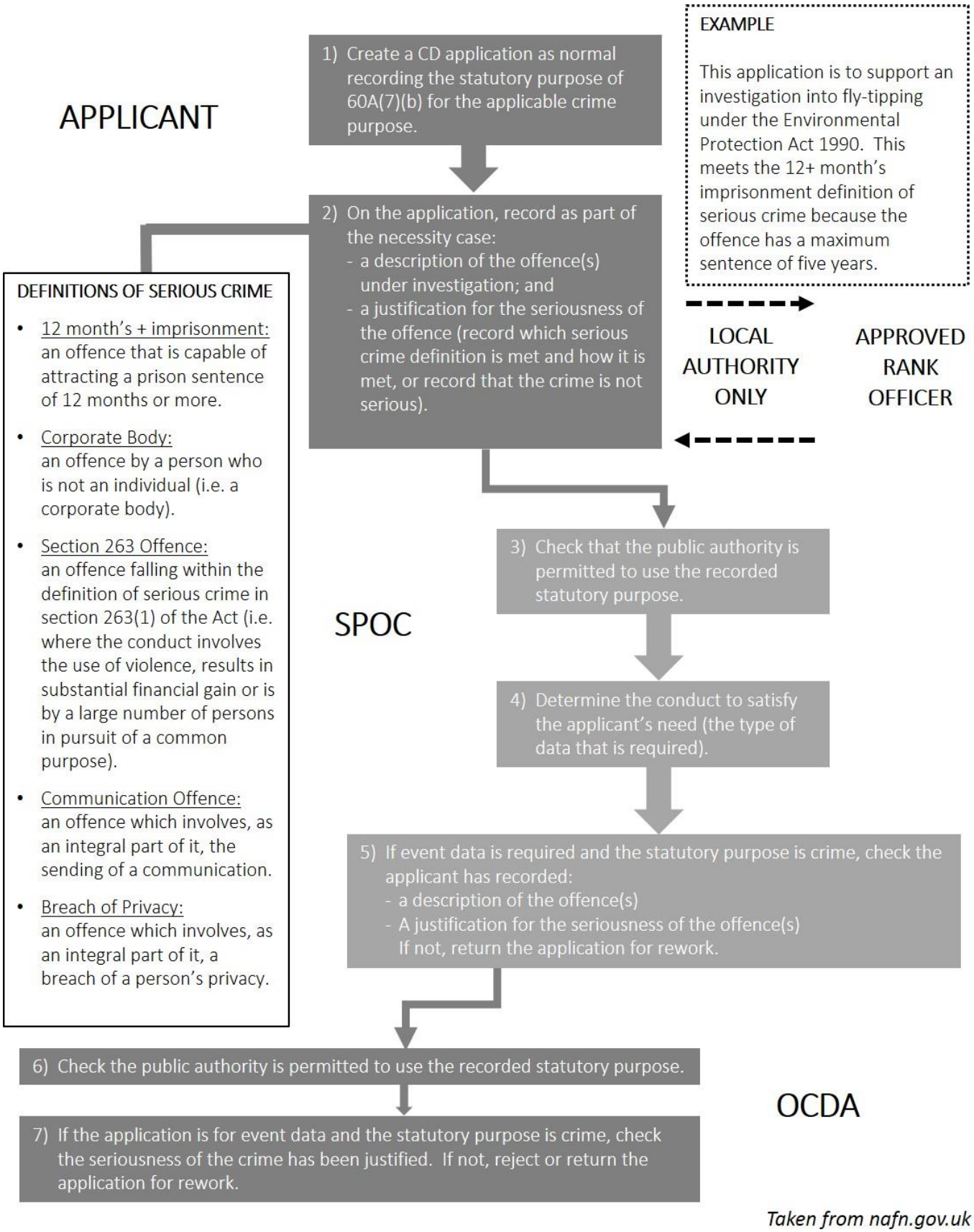
Executive Director, Place and Economy
George Candler….

Director, Governance & HR (Senior Responsible Officer)
Adele Wylie…

Chief Executive (Head of Paid Service)
Rob Bridge…

Executive Director, Adults, Community & Well-being
David Watts

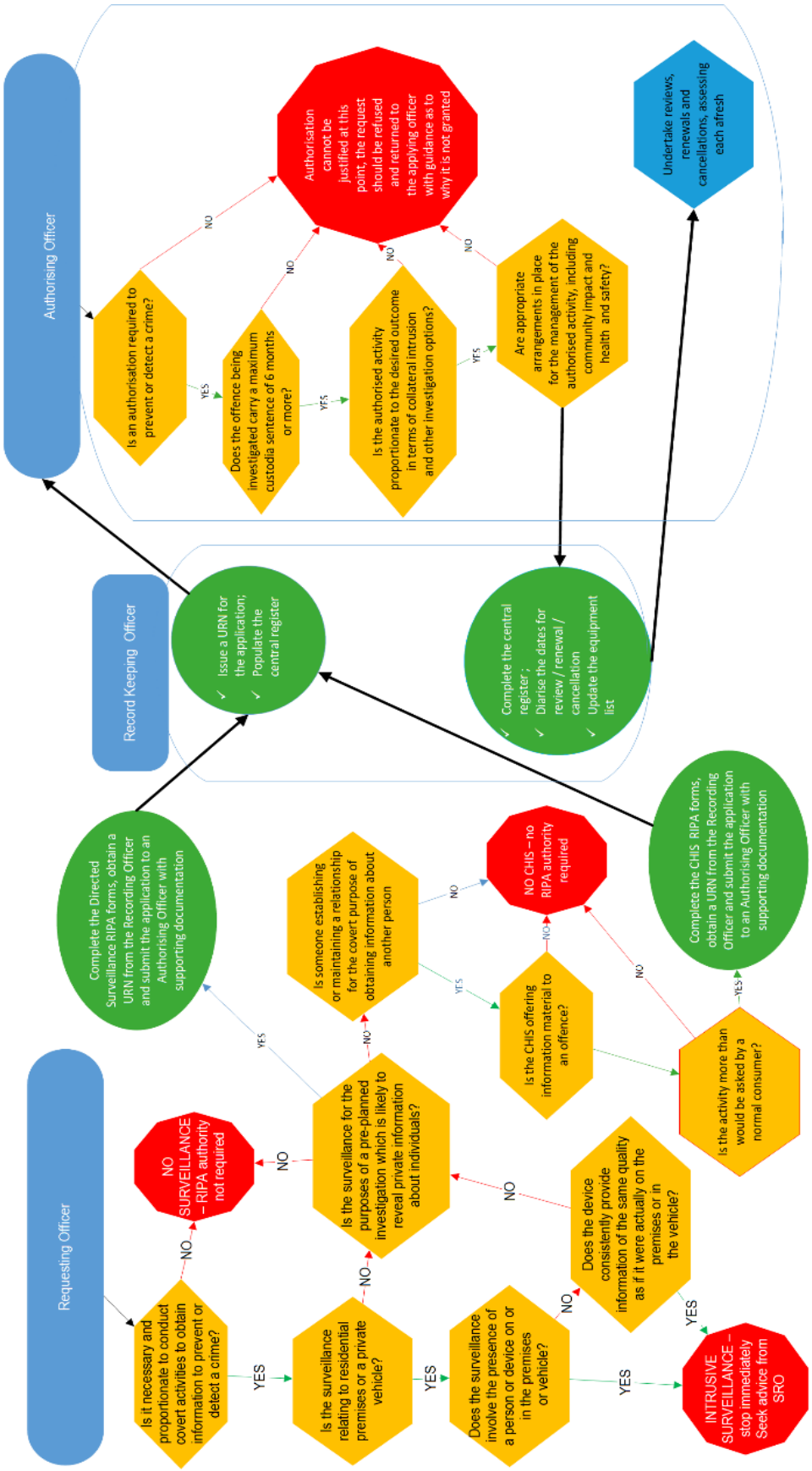
APPENDIX 1 – COMMUNICATIONS DATA APPLICATION PROCESS via NAFN



Taken from nafn.gov.uk

APPENDIX 2 – CHIS or Directed Surveillance Process

IMPORTANT NOTE: For obtaining communications data, see Appendix 1



Appendix 3 – Authorising Officers

Only the following officers are authorised by the Council to approve activities regulated under RIPA for North Northamptonshire Council:

- Chief Executive (Head of Paid Service);
- Executive Director of Adult, Communities & Wellbeing;
- Executive Director of Place & Economy;
- Assistant Director, Regulatory Services.

Appendix 4 – Judicial Approval Process