Norfolk County Council

Appendix B

Regulation of Investigatory Powers Act 2000

Policy and Guidance Notes

nplaw
Norfolk Public Law

Last Updated October 2017

CONTENTS

1. INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations and that privacy is only interfered with where the law permits and there is a clear public interest justification.

1.2 The essence of these provisions is to give effect to the provisions in the Human Rights Act which are designed to protect the privacy of members of the public but subject to the right of public authorities to infringe that human right where necessary in a democratic society for the prevention of crime. If applied correctly, the Act also protects the County Council and its officers.

1.3 This Policy and Guidance is intended as a practical reference guide for Council Officers/investigators who may be involved in covert operations. Officers involved in covert operations must familiarise themselves with the Home Office Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data, together with the Home Office guidance on the judicial approval process and crime threshold for directed surveillance, in order to ensure that they fully understand their responsibilities. The Home Office Codes and guidance are available from https://www.gov.uk/government/collections/ripa-codes. In addition, it is suggested that officers may wish to look at the latest policy and guidance issued by the Office of Surveillance Commissioners (OSC)

1.4 The right to respect for one's private and family life is enshrined in Article 8 of the ECHR, as adopted in the Human Rights Act 1998 (HRA) which renders it unlawful for a public authority to act in a way which is incompatible with any of the Convention rights. As with many of the rights in the HRA, the right to privacy is not an absolute right and is subject to certain qualifications. RIPA and regulations provide an exemption from the right to privacy in certain circumstances, and allow public bodies to interfere with the individual's right to privacy in circumstances which amount to covert surveillance.

1.5 The Council is committed to implementing the provisions of RIPA to ensure that any covert surveillance carried out during the course of investigations is undertaken properly and that the surveillance is necessary and proportionate to the alleged offence/s. The Council seeks to ensure that this Policy Statement remains consistent with the Council's objectives.

1.6 This Policy and Guidance ensures that:

- proper procedures are in place in order to carry out covert surveillance;
- an individual's right to privacy is not breached without justification;
- the potential invasion of privacy caused by using techniques regulated by RIPA, are properly justified in a clear, concise paper/electronic trail;
- proper authorisation and judicial approval is obtained for covert surveillance;

- covert surveillance is considered as a last resort, having exhausted all other avenues;
- the seriousness of the offence is considered, in addition to the requirement to weigh up the benefits to the investigation, when considering whether to authorise covert techniques under RIPA;
- an officer is designated as the Senior Responsible Officer (SRO) for ensuring that all authorising officers meet the standards required by the Investigatory Powers Commissioner's Office ; and
- the Communities Committee has a strategic oversight role in/of the Council's RIPA process.

1.7 **Definitions**

a "Covert"

Concealed, done secretly

b "Surveillance"

This includes, monitoring, observing or listening to persons, their movements, their conversations or their activities or communication. It also includes the recording of anything monitored, observed or listened to. Surveillance can be done with or without the assistance of a surveillance device.

c "Covert surveillance"

Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. If activities are not hidden from the subjects of the investigation, it is not covert

d "Directed Surveillance"

Directed surveillance is defined in the Act as surveillance which is covert, but not intrusive and undertaken for the purposes of a specific investigation or operation;

Directed surveillance is conducted where it involves the observation of a person or persons with the likelihood of gathering private information to produce a detailed picture of a person's life, activities and associations.

For the purposes of the definition, private information in relation to a person can include information relating to their business and professional activities as well as their private or family life.

Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" which the County Council cannot carry out.

Any covert surveillance which is likely to intrude upon anyone's privacy to more than a marginal extent should be treated as directed surveillance. This may include covert CCTV surveillance. If any department is unsure, advice should be taken from Nplaw.

Directed surveillance **must** be properly authorised and judicially approved in accordance with the procedure set out in section 6 of these guidance notes.

e "Covert human intelligence source" (CHIS)

Use of a covert human intelligence source means establishing or maintaining a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council officer to strike up a relationship with someone as part of an investigation to obtain information "under cover". Recent examples have involved investigations using social media.

Someone who volunteers information to the Council, either as a complainant or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount by itself to use of a covert human intelligence source, because they will not have obtained the information in the course of, or as a consequence of, the existence of a personal or other relationship.

However, if the Council is relying on an individual to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source. The test to apply is not whether there is a task to perform but whether it is to be done by the use of a personal or "other" relationship (which could include commercial, professional, managerial or employment contracts). If and when it becomes apparent that a repeat informant is obtaining his information in this way, then he is, in reality a CHIS to whom a potential duty of care is owed if the information is acted upon.

Advice should be sought from nplaw before acting on information supplied by such a source.

f "Intrusive Surveillance"

Covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. If a device is not on premises or in vehicle but provides consistent information of the same quality and detail as if it were on the premises or in vehicle, then this will be considered "intrusive". Surveillance devices designed or adopted principally for the purpose of providing information about the location of a vehicle are not considered intrusive. Residential premises includes hotel or prison accommodation if being used for living accommodation plus houses, boats, barracks etc BUT not any common area to which a person is allowed access in connection with his or her

occupation of any accommodation. Private vehicles include those for domestic, family and leisure use. It includes any vessel, aircraft or hovercraft.

g "Communications Data"

The term communications data embraces the "who" "when" and "where" of a communication but not the content and not what was said or written. It includes the manner in which and by what method a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within that communication.

Communications data is generated, held or obtained in the provision, delivery or maintenance communication services, both being postal services or telecommunication services. A postal service consists of any service which is involved in the collection, sorting, conveyance, distribution and delivery of postal items and is offered or provided as a service, the main purpose of which is to transmit postal items from place to place. Any service which consists in the provision of access to and for making use of any telecommunication system (whether or not provided by the person providing the service) the purpose of which is to transmit communications using electric or electro magnetic energy.

h "Definition of Traffic Data"

This is data that is comprised in or attached to communication for the purpose of transmitting the communication and in relation to the communication which:

(a) identifies or appears to identify any person, equipment or location to or from which a communication is or may be received;

(b) identifies or selects transmission equipment;

(c) comprises signals activate equipment used for transmission of communication;

(d) identifies data as data comprised in or attached to a communication;

(e) identify a computer file or a computer programme to which access has been obtained or which has been run by means of a communication but only to the extent that the file or programme is identified by reference to the apparatus in which the final programme is stored (i.e. traffic data may identify a server but not a website or page).

i "Service Use Information"

This is data relating to the use made by any person of a postal or telecommunication service or any part of it and falls within Section 21(4)(b) of RIPA.

Examples of data within this definition include:

(a) itemised telephone call records (numbers called);

(b) itemised records of connections to internet services;

(c) itemised timing and duration of service usage (calls and all connections);

(d) information about amount of data downloaded and/or uploaded;

(e) information about the connection, disconnection and re-connection of services;

(f) information about provision and use of forwarding/re-direction services by postal and telecommunications service providers;

(g) information about provision of conference calling, call messaging, call waiting and call barring telecommunications services;

(h) information about selection of preferential numbers or discount calls;

(i) records of postal items such as records of registered, recorded or special delivery postal items;

(j) records of parcel confinement, delivery and collection.

j. "Subscriber Information"

This relates to information held or obtained by a communication service provider about persons to whom the communication service provider has provided or provides a communication service. Those persons would include people who are subscribers to a communication service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

Examples of this include:

(a) subscriber checks, such as who is the subscriber of phone number, 123456789 or who is the account holder of e-mail account xyz at xyz.co.uk;

(b) subscribers' or account holders' information including payment methods and any services to which the subscriber or account holder is allocated or has subscribed;

(c) addresses for installation and billing;

(d) information provided by a subscriber or account holder to a communication service provider such as demographic information or sign up data (to the extent that the information such as a password giving access to the content of the communication is not disclosed).

2. WHAT DOES RIPA DO?

2.1 RIPA places controls on the use of certain methods of investigation. In particular, it regulates the use of surveillance, “covert human intelligence sources” and the acquisition and disclosure of Communications Data. This guidance covers these aspects of the Act.

2.2 RIPA’s main implications for the Council are in respect of covert surveillance by Council officers and the use of “covert human intelligence sources”. It also covers the Council’s limited dealings with the acquisition and disclosure of Communications Data.

2.3 Surveillance is covered in sections 5 to 6 of this guidance. The use of “covert human intelligence services” is covered in Section 7. Communications Data is dealt with in Section 8.

3. JUDICIAL APPROVAL AND THE SERIOUS CRIME THRESHOLD

3.1 From 1 November 2012 local authorities have been required to obtain judicial approval prior to using covert techniques. Local authority authorisations and notices under RIPA will only be given effect once an order has been granted by a Justice of the Peace (JP).

3.2 Additionally, local authority use of **directed surveillance** under RIPA is now limited to the investigation of crimes which attract a six month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco. This threshold does **not** apply to the use of CHIS or to the acquisition and disclosure of communications data.

3.3 The Home Office has published guidance for local authorities and magistrates, which is available at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

3.4 Local authority officers will need to be formally designated to appear before the court for the purpose of seeking judicial approval.

4. PRINCIPAL RESPONSIBILITIES

The Senior Responsible Officer

4.1 The Codes of Practice on Covert Surveillance, CHIS and Communications Data set out the responsibilities of the Senior Responsible Officer, which are broadly the same. The following is a composite list.

4.2 The senior responsible officer (SRO) is responsible for:

(a) the integrity of the process in place within the local authority to authorise directed surveillance, for the management of CHIS and the acquisition of communications data;

(b) compliance with Part 1 and II of the Act and with the Codes;

(c) oversight of the reporting of errors to the Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

(d) engagement with the Commissioner/inspectors when they conduct their inspections and;

(e) where necessary, oversight of the implementation of post-inspection action plans recommended or approved by the Commissioner;

4.3 Also, in relation to covert surveillance and CHIS, the SRO is responsible for:

(f) ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the IPCO; and

(g) where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

4.4 The Chief Legal Officer has been nominated as the SRO for the Council for directed surveillance and CHIS and also for communications data.

Communities Committee responsibilities

4.5 Following on from the role undertaken previously by Cabinet, the Communities Committee now reviews this Policy and Guidance, on an annual basis, to ensure fitness for purpose. This higher level review provides an additional safeguard against inappropriate or disproportionate use of the RIPA powers.

4.6 The Communities Committee receives reports on the use of RIPA, to ensure that RIPA is being used consistently and in accordance with this Policy Statement. Reports are presented in such a way, that individuals and/or organisations who have been/are the subject of an authorisation, are not identifiable.

4.7 The Committee is not involved in making decisions on specific authorisations.

External oversight of the Council's RIPA processes: The Office of Surveillance Commissioner and the Interception of Communications Commissioner's Office – superceded by the Investigatory Powers Commissioner's Office wef 8 September 2017.

4.8 There were two separate national bodies which carried out audits to ascertain standards within those enforcement bodies which carry out covert surveillance and access communications data. These were respectively the Office of the Surveillance Commissioner (OSC) and the Interception of Communications Commissioner's Office (IOCCO).

4.9 The last inspection by the IOCCO was 6 March 2012. As the Council is a member of the National Anti-Fraud Network (NAFN), subsequent inspections have been (and are likely to continue to be) conducted of NAFN and not the Council directly.

4.10 The last inspection by the OSC was carried out on 31 October 2016.

4.11 These two bodies have been replaced, with effect from 8 September 2017, by one oversight body: the Investigatory Powers Commissioner's Office, established under the Investigatory Powers Act 2016.

5. COVERT SURVEILLANCE

Introduction

5.1 The Act is designed to regulate the use of "covert" surveillance, which is surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. If activities are not hidden from the subjects of the investigation, it is not covert.

5.2 Two types are regulated by RIPA - “directed" and "intrusive" surveillance. These terms are defined in paragraph 1.7 and also below:

- **Directed Surveillance** is defined in the Act as surveillance which is covert, but not intrusive and undertaken for the purposes of a specific investigation or operation. It involves the observation of a person or persons with the likelihood of gathering private information to produce a detailed picture of a person’s life, activities and associations. Private information about a person can include information relating to their business and professional activities as well as their private or family life. Any covert surveillance which is likely to intrude upon anyone’s privacy to more than a marginal extent should be treated as directed surveillance. This may include <u>covert</u> CCTV surveillance.

- Intrusive Surveillance is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. If a device is not on premises or in a vehicle but provides information of the same quality and detail as if it were, this will be considered “intrusive”. Surveillance devices designed or adopted principally for the purpose of providing information about the location of a vehicle are not considered intrusive. Residential premises includes hotel or prison accommodation if being used for living accommodation plus houses, boats, barracks, etc BUT not any common area to which a person is allowed access in connection with his or her occupation of any accommodation. Private vehicles include those for domestic, family and leisure use. It includes any vessel, aircraft or hovercraft.

RIPA provides for the authorisation of covert surveillance provided it is necessary and proportionate.

5.3 General observation forms part of the duties of some Council Officers. Where an incident occurs during officers normal duties, which is unforeseen and an officer has to respond immediately to the situation, what the officer does will not require an authority. This "unforeseen" activity where an officer was merely reacting to events does not need to be covered by the procedures in these Guidance Notes.

5.4 Generally, the provisions of the Act do not include the use of <u>overt</u> CCTV surveillance systems. Members of the public are aware that such systems are

in use, for their own protection and to prevent crime. However, where CCTV systems are used for covert surveillance the Act will apply.

Application to the County Council

5.5 The County Council cannot carry out Intrusive Surveillance. These powers are reserved to bodies such as the Police and HM Revenue and Customs. If a County Council officer is asked by another agency to co-operate with Intrusive Surveillance, advice should immediately be obtained from nplaw, who will give advice as to possible risks to and concerns for officers and equipment. Similarly, the County Council cannot conduct entry on, or interference with, property or with wireless telegraphy (known as "property interference").

5.6 The County Council may however authorise Directed Surveillance.

5.7 The County Council may be asked to carry out directed surveillance for another agency, or may ask others to carry out surveillance on its behalf. It is for the lead agency to apply for an authorisation. When acting with another body, the operation can be covered by that authority's authorisation. However, all involved must ensure they are familiar with the terms of the authorisation.

Authorising Directed Surveillance and obtaining judicial approval: The Rules

5.8 It is crucial that all directed surveillance is properly authorised and judicially approved. No officer may commence any form of directed surveillance operation unless it is authorised and approved in accordance with this guidance. Failure to secure proper authorisation/approval and to comply with this procedure could lead to evidence being excluded by the courts and to complaints against the Council. The Council is subject to audit and inspection by the Investigatory Powers Commissioner's Office and it is important that we can demonstrate compliance with RIPA.

Who can authorise directed surveillance?

5.9 Regulations made under the Act say that the most junior level at which authorisations can be given is by what it refers to as Director, Head of Service, Service Manager or equivalent. However, authorisations should be given by those officers set out in Appendix A. Officers named on this designated list should have full training in respect of RIPA and the considerations that must be made before granting authorisation.

5.10 If anyone authorised is not available, anyone holding a senior position can be delegated to authorise. Advice can also be sought from anyone senior to an authorising officer in difficult or sensitive cases, and also from nplaw.

5.11 Where practicable, the authorising officer should not be directly involved in the case giving rise to the request for authorisation. Where it is not practicable for authorisation to be given by an officer who is not directly involved, this should be noted with reasons on the authorisation form.

On what grounds can directed surveillance be authorised?

5.12 In the case of local authorities, directed surveillance can only be authorised if it is necessary for the purpose of preventing or detecting crime and the offence(s) under investigation attracts a maximum custodial sentence of six months or more or relate to the underage sale of alcohol or tobacco.

5.13 It is very important to consider whether the surveillance is necessary. If the objective can be achieved by less intrusive means, which do not involve directed surveillance, then these should be used.

5.14 If there are no other means then this should be stated on the authorisation form.

5.15 The crime under investigation should be fully detailed.

Is the proposed surveillance proportionate?

5.16 Authority should not be given unless the person authorising the request is satisfied that the surveillance is proportionate.

5.17 The authorising officer should make sure that any interference with the privacy of an individual is justified by the end being sought. If the benefit to be obtained from surveillance is marginal, the person authorising should think very carefully about whether the use of surveillance is proportionate. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. Suggested areas to consider include, prevalence of offence and other means by which the information can be obtained.

5.18 In addition, the activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

5.19 The authorisation must detail all methods that have been considered and why they have not been implemented, in order to demonstrate that full attention has been given to the proportionality of the proposed surveillance.

5.20 Further guidance on proportionality can be found in part 9 of Appendix B.

Is the proposed surveillance discriminatory?

5.21 The County Council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. Departments 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.

Will the surveillance involve "collateral intrusion"?

5.22 In other words, will the surveillance intrude upon the privacy of people other than those who are the subject of the investigation? Those authorising the surveillance should be sensitive to the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefits of undertaking the surveillance. If there is considered to be a risk of collateral intrusion, consideration must be given to minimising this risk.

What is legally privileged information, personal confidential information or confidential journalistic material?

5.23 Confidential material' is described by RIPA as being:

(a) matters subject to legal privilege;

(b) confidential constituent information between the MP and a constituent in respect of constituency matters;

(c) confidential personal information; or

(d) confidential journalistic material.

5.24 Authorisations in respect of confidential material can only be granted by the Head of Paid Service (the Managing Director) and in her absence, by his/her substitute.

5.25 A substantial proportion of communications between a lawyer and client may be subject to legal privilege. Matters subject to legal privilege must be kept separate from enforcement investigations or criminal prosecutions, as they will not be admissible in court. In the very rare circumstances where legally privileged information may be acquired and retained, the matter must be reported to the Authorising Officer by means of a review. The Authorising Officer will decide whether the authorisation should continue. The attention of the Commissioner should be drawn to legally privileged information, during the IPCO inspection and the material made available to the inspector, if requested.

5.25 Oral and written communications are held in confidence if subject to an express or implied undertaking to hold the communications in confidence or where such communications are subject to a restriction on disclosure or an obligation of confidentiality contained in legislation e.g. consultations between a health professional and a patient, information from a patient's records or information relating to the spiritual counselling of a person.

5.26 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to an undertaking. The attention of the Commissioner should be drawn to confidential journalistic material during the IPCO inspection and the material made available to the inspector, if requested.

5.27 Acquiring material in the manner referred to above, is likely to be rare for the Council.

Activities/operations involving directed surveillance

5.28 It is safest to assume that any operation that involves planned covert surveillance of a specific person or persons (including Council employees) likely to obtain private information, of however short a duration, falls within the definition of directed surveillance and will, therefore, be subject to authorisation under RIPA.

5.29 The consequence of not obtaining an authorisation may render the surveillance action unlawful under the HRA, or any evidence obtained may be inadmissible in Court proceedings.

5.30 It is strongly recommended that Council Officers seek an authorisation, where the surveillance is likely to interfere with a person's Article 8 rights to privacy. Obtaining an authorisation will ensure that the surveillance action is carried out in accordance with the law and is subject to stringent safeguards against abuse.

5.31 Proper authorisation of directed surveillance should also ensure the admissibility of evidence under the common law, PACE and the Human Rights Act.

5.32 Directed surveillance might be used, for example:

- For fraud or similar offences, where there is a need to observe premises in order to establish who the owner/occupier is, to find out who the occupier has associations with, or to establish whether or to what extent they are being used as business premises.

- Where the Council directs another person/organisation to act as its ‘agent’ for the purposes of obtaining private information e.g. where Council Officers specifically ask residents to maintain diary notes of the incidence of sales of alcohol to young persons.

- By placing a stationary mobile or video camera outside a building or the use by officers of covert recording equipment to record suspected illegal trading activity, such as the sale of counterfeit goods or ‘mock’ auctions.

5.33 It will not be necessary to obtain authorisation for directed surveillance when using surveillance devices such as standard video cameras, still cameras, or binoculars, which are utilised on an overt basis.

Activities/operations not involving directed surveillance

5.34 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person’s life, activities and associations.

Private information includes any information relating to the person's private or family life.

5.35 However, it does not include general observation which is part of an Enforcement Officer's normal work.

5.36 General observation duties of the Council's Enforcement Officers whether overt or covert, frequently form part of their day to day activities and the Council's legislative core functions – such activities will not normally require a directed surveillance authorisation as the obtaining of private information is highly unlikely.

5.37 Examples of activities/operations which are unlikely to involve directed surveillance are:

- Enforcement officer's attendance at a car boot sale where it is suspected that counterfeit goods are being sold. In such a case, the officer is not carrying out surveillance of particular individuals - the intention is, through reactive enforcement, to identify and tackle offenders;

- A one-off identification/confirmation of the existence of a premises address by officer observation;

- Anything which constitutes an immediate response e.g. a council officer with regulatory responsibilities may by chance be present when an individual is potentially infringing the law and it is necessary to observe, follow, or engage in other surveillance tactics as an instant response to the situation to gather further information or evidence. Once this immediacy has passed, however, any further directed surveillance of the individual, must be subject to a RIPA authorisation.

5.38 In circumstances where such activities/operations are considered to fall outside the scope of RIPA, it is good practice to record the reasons for this decision.

Test Purchasing of Age Restricted Products

5.39 It is the view of the Office of Surveillance Commissioners (OSC) that the use of young persons, pursuant to an arrangement with an officer of a public authority, to conduct test purchasing exercises attracts the desirability to obtain RIPA authorisation for directed surveillance.

5.40 The Better Regulation Delivery Office (BRDO) Code of Practice for Age Restricted Products repeats and supports the OSC guidance, stating that if covert recording equipment is worn by the test purchaser, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance.

5.41 Local authority use of directed surveillance under RIPA is now limited to the investigation of crimes which attract a six month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and

tobacco. The majority of other age restricted products already attract a six month or more imprisonment penalty, for example gas lighter refills, fireworks, knives and solvents all attract those penalties and so RIPA would be triggered. This means that in most cases a directed surveillance application would be required for test purchasing of age-restricted products. However there may be circumstances where different age restricted products are under consideration for which a test purchasing operation is being considered. In these circumstances it is good practice to record the reasons for the decision on - a 'non-RIPA' form which has been devised to cover this eventuality at Appx F.

5.42 It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have already been attempted and failed, or that they would not be appropriate given the circumstances. This may include where advice visits to establishments have taken place and subsequent intelligence of sale to minors is being received.

5.43 Premises identified for a test purchase may be combined within a single directed surveillance application on a 'per operation' basis, provided that each premises is clearly identified at the outset and the intelligence sufficient to prevent "fishing trips".

5.44 It is important that those individuals involved in the planning and conduct of test purchasing exercises avoid inciting, instigating, persuading or pressurising a person into committing an offence that, otherwise, would not have been committed. This includes giving due consideration to the impact of instructing an underage test purchaser to lie about their age if challenged by the seller of an age restricted product. The application for directed surveillance or the CHIS application must fully consider the impacts this might present together with the mitigation measures of any additional risks that may emerge as a result of the change in approach.
The individual making the test purchase is not classed as a CHIS for single transaction operations. This is because he/she does not establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the obtaining of information. The one-time act of making a purchase in a shop open to the public, where there may even be no verbal exchange, cannot reasonably constitute establishing a relationship, personal or otherwise – other than a momentarily fleeting one in which no information is obtained, which could reasonably constitute an interference with the privacy of the retailer/proprietor.

5.45 These assumptions are equally valid in circumstances where it is appropriate to evidence systematic breach of legislation at any given premises by using a number of different test purchasers, each making a one-off purchase. There are, however, some important qualifications to this advice. Firstly, different considerations would apply where the test purchaser has made previous visits to the premises, or is to make repeated visits, and in doing so, has established or is seeking to establish a relationship with the retailer/occupier prior to the attempted test purchase. In this case the juvenile would be revisiting in a way that encourages familiarity and as such they would be deemed a CHIS. Secondly, different considerations would apply, if the attempted test purchase

is made other than from business premises open to the public, for example from a person's home including parts of their home adjacent to retail premises.

5.46 In circumstances where the test purchaser is not deemed to be a CHIS, it is nevertheless considered good practice to follow the requirements to ensure that:

- The safety and welfare of the test purchaser has been fully considered;
- Any risk has been properly explained to, and understood by the test purchaser; and
- A risk assessment has been undertaken, covering the physical dangers including any moral and psychological aspects of the test purchaser's deployment.

5.47 In the vast majority of test purchase operations, it is likely that there will be minimal risk to the test purchaser involved. Where an operation differs in the standard approach, for example where the test purchaser of an age restricted product may be asked to lie about their age, a directed surveillance or CHIS application must fully consider the mitigation of any additional risks that may emerge as a result of the change in approach.

Online covert activity, including covert surveillance of Social Networking Sites (SNS)

5.48 Wherever possible officers should continue to adopt overt methods in seeking to achieve business compliance. However as a result of the scale of online trading the need to make online test purchases and investigation checks is inevitably increasing. It is therefore recognised that from time to time covert methods will need to be employed. Whenever it is intended to carry out covert activity online, officers must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. 'General' test purchases from an open internet site or marketplace (such as Ebay) is unlikely to require RIPA authorisation. However any covert activity likely to interfere with an individual's Article 8 rights should only be carried out when it is necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, a directed surveillance authorisation must always be sought, as set out elsewhere in this guidance.

Social Networking Sites (SNS)

5.49 A directed surveillance application will often be required where an investigator wishes to communicate covertly online via SNS. Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, 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 an 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.

5.50 An authorisation for the use and conduct of a CHIS will also be necessary if a relationship is established or maintained by an officer or by a person acting on their behalf (i.e. where the activity is more than mere reading of the site's content).

5.51 It is not unlawful for officers to utilise a false identity as part of online investigations, but it is inadvisable to do so for a covert purpose without RIPA authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws. Officers must also 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).

Authorising Directed Surveillance: The Procedure

Applying for authorisation.

5.52 Applications for authorisation must be made in writing on the correct form. The form to seek authorisation can be found on the nplaw pages of the intranet. A written authorisation is normally completed as far as possible by the investigating officer before being submitted to the Authorising Officer for approval.

5.53 A written application for authorisation for directed surveillance should describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and the grounds (i.e. for the purpose of preventing or detecting crime) stated in Section 28(3) of the 2000 Act; The offence under investigation should be fully detailed.
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance; (although there is no requirement to know the identity of those who are to be the subject of the surveillance);
- the approximate cost of the surveillance;
- the results of consultation with other enforcement agencies or community leaders
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date. If the authorising officer has not granted the authorisation in full and has amended the terms of the application, this must be recorded on the application form and reasons given for the decision.

5.54 Each application must be given a Unique Reference Number, which will then be used to locate the application on the Central Register.

5.55 Guidance on completing an application for authority for directed surveillance can be found in Appendix B.

5.56 When an authorisation has been granted, the terms of the authorisation must be followed exactly. Any deviation might lead to the authorisation being considered invalid. If as a result of initial observations, the investigating officer wishes to deviate from the terms of the authorisation, then either a fresh authorisation or renewal requesting revised authority must be made.

5.57 If the surveillance involves juveniles or vulnerable adults then special consideration should be given to the following:

- If possible authorisation should be at the highest level. (If considering use of a juvenile or vulnerable adult as a CHIS – Authorisation should not be granted unless a risk assessment has been considered covering physical dangers and psychological aspects. Use of an appropriate adult should be considered.

- No authorisation can be granted to use a source under age 16 years to give information against his/her parents).

The judicial approval process

5.58 Once an application has been authorised by an authorising officer, it will not take effect until it has been approved by a Justice of the Peace (JP).

5.59 The process for seeking judicial approval is as follows:-

- The local authority must contact HMCTS to arrange a hearing.

- The JP should be provided with a copy of the authorisation/notice, all supporting documentation and a partially completed judicial approval/order form. (The original authorisation/notice should be shown to the JP at the hearing.)

- A hearing will take place in private, usually attended by the case investigator, who will be best placed to answer the JP's questions about the investigation. However, in some cases, for example where there are sensitive issues, it may be appropriate for the Authorising Officer to attend to answer questions.

- The JP will consider the application and record his/her decision on the order section of the application/order form.

5.60 The JP may decide to:-

- Approve the grant or renewal of the authorisation/notice;

- Refuse to approve the grant or renewal of the authorisation/notice;

- Refuse to approve the grant or renewal and quash the authorisation/notice.

5.61 The form for seeking judicial approval is incorporated into the application forms available on the nplaw pages of the intranet.

Duration of authorisations

5.62 A written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect. An authorisation cannot be granted for a period of less than three months. However, it should be noted that all authorisations **must** be cancelled as soon as the decision is taken that directed surveillance should be discontinued.

Reviews

5.63 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion. If a minor change has occurred in the investigation, then these can be dealt with by way of review. If the scope of the investigation has changed then a fresh authorisation is required.

5.64 In each case authorising officers within the Council should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but at no longer than monthly intervals. The Review form available on the intranet should be completed on review.

Renewals

5.65 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, s/he may renew it in writing for a further period of **three months**. Renewals must also be judicially approved, following the process outlined in paragraph 5.59 above.

5.66 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, but taking into consideration that time must be allowed for obtaining judicial approval. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

5.67 All applications for the renewal of an authorisation for directed surveillance should be made on the renewal form available on the intranet and should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information given in the original application for authorisation;

- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.68 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraphs 5.74 to 5.75).

Cancellations

5.69 The authorising officer who granted or last renewed the authorisation **must** cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer. If in doubt about who may cancel an authorisation, please consult nplaw. Cancellations are to be effected by completion of the cancellation form available on the intranet.

5.70 It is essential that there is a completed cancellation for each authorisation once surveillance has been completed. An authorisation cannot simply be left to expire.

5.71 As soon as any decision is taken to discontinue surveillance, instruction must be given to those involved to stop all surveillance. The date and time of such an instruction must be included in the Notification of Cancellation form.

5.72 It is also good practice to retain a record of the product obtained from the surveillance and whether or not objectives were achieved. The Authorising Officer should give directions on the handling, storage or destruction of the product of surveillance.

Record Keeping and Central Record of Authorisations

5.73 In all cases in which authorisation of directed surveillance is given the individual department is responsible for ensuring that the following documentation is kept securely for a period of at least five years from the date of authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of the judicial approval application form/order;
- 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.

- a copy of the cancellation document

5.74 In addition, the following must be sent to nplaw immediately upon completion:

- all completed forms authorising and approving directed surveillance;

- all completed forms authorising and approving renewal of directed surveillance;

- all judicial approval application forms/orders;

- all completed forms cancelling directed surveillance.

5.75 These will be held securely by nplaw and form part of a Central Record of Authorisations. Each application will be accessible by virtue of its Unique Reference Number. The Senior Responsible Officer, assisted by nplaw will review the Central Record on a bi-monthly basis and complete a central record of authorisations in accordance with paragraph 8.1 of the Code of Practice on Covert Surveillance. The Central Record should be available for inspection by the Investigatory Powers Commissioner's Office upon request.

6 SURVEILLANCE OPERATIONS NOT REGULATED BY RIPA:

6.1 The Regulation of Investigatory Powers Act 2000 (RIPA) aims to ensure that covert surveillance carried out for the purposes of a specific investigation or operation is undertaken in a manner which is human rights compliant. This is achieved through a system of self authorisation by senior officers, who have to be satisfied that the surveillance is necessary and proportionate to what is sought to be achieved, followed by judicial approval.

6.2 Local authorities are only required to seek authorisations under RIPA for covert surveillance carried out for the purposes of preventing or detecting crime. No RIPA authorisations can be sought for covert surveillance being undertaken for other purposes. Nor should they be sought for crime prevention or detection purposes, if that purpose is not linked to one of the authority's regulatory functions. This was stated by the Investigatory Powers Tribunal in the case of C v The Police and the Secretary of State for the Home Department (14/11/2006, No: IPT/03/32/H), who held that surveillance of employees is unlikely to be for a regulatory function of the authority.

6.3 This means that there may be circumstances when the Local Authority wishes to carry out surveillance and will not be able to rely on a RIPA authorisation (eg surveillance of employees). Not being able to seek an authorisation under RIPA means there is a greater risk of a human rights challenge, as privacy rights under Article 8 are likely to be interfered with. This can be reduced by following a similar self- authorisation process, which can be achieved by using the non-RIPA authorisation form available on the nplaw pages of the intranet and which should be completed by the officer and authorised by a person identified in Appendix A.

6.4 The Authorising Officer should consider the same issues as if he were responding to a request under RIPA, particularly the necessity of the operation, whether it is proportionate and whether there are any other methods of obtaining the information. If there is any doubt as to the issue of a Local Authority regulatory role and its ordinary functions, then advice should be sought from nplaw.

6.5 When considering surveillance of employees, it is also important to ensure compliance with the Data Protection Act 1998 and in particular Part 3 of the Data Protection Act Employment Practices Code.

7 COVERT HUMAN INTELLIGENCE SOURCES:

Authorising Use of Covert Human Intelligence Sources (CHIS)

7.1 Similar principles and procedures apply to authorising the use of covert human intelligence sources. The use of CHIS is also subject to judicial approval and the process outlined at paragraph 5.47 should be followed.

7.2 Officers' attention is drawn to the explanation of the nature of a covert human intelligence source in paragraph 1.7. If necessary, Forms 5, 6, 7 and 8 available on the nplaw pages of the intranet can be utilised to authorise the use of a CHIS.

7.3 The considerations for authorising a CHIS are broadly similar to those of directed surveillance, but there are some additional matters which must be considered.

7.4 There are rules about the use of vulnerable adults or juveniles as sources and there are also special requirements with regard to the management, security and welfare of sources. Refer to the Covert Human Intelligence Sources Code of Practice for detailed guidance.

7.5 In summary:

- when deploying a source, the Council should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, including the foreseeable consequences to others, of that tasking.
- before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences, should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.
- the person responsible for the day to day management of the source's welfare and security e.g. departmental manager, will bring to the attention of the Authorising Officer, any concerns about the personal circumstances of the source, insofar as they might affect:

  i. the validity of the risk assessment;
  ii. the conduct of the source, and
  iii. the safety and welfare of the source.

7.6 Where deemed appropriate, the concerns about such matters should be considered by the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

7.7 In addition to the appointment of the required roles of handler and controller as part of a CHIS operation, a separate person within the organisation should be

appointed to oversee the use made of CHIS. The Senior Responsible Officer, has assumed this role .

7.8 The records kept by the authority should be maintained so as to protect the confidentiality of the source and the authorising officer must ensure there is a satisfactory risk assessment in place.

Activities/operations involving CHIS

7.9 If a department is considering the use of a CHIS, advice must be sought from nplaw.

7.10 **Activities/operations not involving CHIS**

7.11 The following situations will not normally require a relationship to be established for the covert purpose of obtaining information and therefore do not involve a CHIS:

- One-off test purchase transactions carried out in the normal course of business, where Enforcement Officers are operating as would a member of the public and do not establish a personal or other relationship. For example, the purchase of a music CD for subsequent expert examination would not require authorisation, but where the intention is to ascertain whether a trader is taking delivery of suspected fakes and a relationship is established between the trader and the Officer, then authorisation should be sought beforehand. Please refer to paragraphs 5.39 to 5.51 of this Policy Statement for additional guidance regarding Test Purchasing and Online covert activity.

- The task of ascertaining purely factual information e.g. the location of cigarette vending machines in licensed premises;

- Where members of the public volunteer information to an Officer as part of their normal duties;

- Where the public call telephone numbers set up by the Council to receive information; and

- Where members of the public are asked to keep diaries of incidents in relation to anti-social behaviour – however such activity will be regarded as directed surveillance, requiring an authorisation.

7.12 In circumstances where such activities/operations are considered to fall outside the scope of RIPA, it is good practice to record the reasons for this decision.

8. ACCESSING COMMUNICATIONS DATA

Introduction

8.1 Since 5 January 2005, RIPA has regulated access to Communications Data. This is defined in paragraph 1.7. These guidance notes should be read in conjunction with the current Code of Practice issued under Section 71 of RIPA. Copies of the Code are held by nplaw and/or are available via https://www.gov.uk/government/collections/ripa-codes

Application to the County Council

8.2 The County Council are only entitled to seek the acquisition of communications data defined as service user information and subscriber information (see paragraph 1.7 for definition). The County Council is not authorised to acquire what is defined as traffic data (see paragraph 1.7).

Acquisition of communications data: The interception of postal, telephone, email and other electronic communications

8.3 It is an offence to intercept communications sent by public postal services and public telecommunications systems except in very specific circumstances. It can be an offence to intercept communications sent by private telecommunications systems.

8.4 It is unlikely that the Council would wish to intercept communications of this nature, even if it could do so legally. In the very unlikely event that you are considering intercepting communications, you should take no steps to do so before seeking advice from nplaw.

8.5 There may be circumstances in which it is appropriate and legitimate to intercept communications sent and received by employees. However, once more, great care needs to be taken, not only in respect of RIPA, but in respect of employment law and human rights issues. You should not intercept communications sent by or received by employees without first seeking advice from the Head of Human Resources and/or nplaw.

Authorising the acquisition and disclosure of communications data and obtaining judicial approval

8.6 It is crucial that the acquisition of communications data is properly authorised and judicially approved. No officer may seek the acquisition of any form of communication data unless he is authorised and the application approved in accordance with this guidance. Failure to secure proper authorisation and approval and to comply with this procedure could lead to evidence being excluded by Courts and complaints against the Council. The Council is subject to audit and inspection by the Investigatory Powers Commissioner's Office and it is important that we demonstrate compliance with RIPA.

8.7 Acquisition of communications data under the Act involves four roles:

(a) the applicant;

(b) the designated person;

(c) the single point of contact (SPoC);

(d) the senior responsible officer

8.8 The Act provides two alternative means for acquiring communications data by way of:

(a) an authorisation under Section 22(3); or

(b) a Notice under Section 22(4)

The Applicant

8.9 The Applicant is a person involved in conducting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data. The Applicant should complete an application form setting out for consideration by the designated person the necessity and proportionality of the specific requirement for acquiring communications data.

The Designated Person

8.10 The designated person is a person holding a prescribed office in the same public authority as the Applicant. Authorisations and Notices to acquire communications data should ordinarily be given only by those officers set out in Appendix A who are specifically designated to approve applications for the acquisition of communications data.

8.11 The designated person must consider the application and record his considerations at the time in writing or electronically. If the designated person believes it is appropriate in the specific circumstances of the case, an authorisation may be granted or a notice given. Designated persons should assure that they grant authorisations or give notice only for purposes and only in respect of types of communications data that a Designated Person of their office, rank or position and the relevant public authority may give or grant. Designated persons shall assess the necessity for any conduct to acquire or obtain communications data, taking account of any advice provided by the Single Point of Contact (SPoC).

8.12 Designated persons must not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved. If it appears unavoidable or it is necessary to act urgently or for security reasons then a designated person may grant an authorisation or notice in relation to an investigation in which they are directly involved but the reason why such person was required to authorise that particular case, should be noted on the application form and this must be notified to the Commissioner.

8.13 Designated persons should have undertaken some training in relation to human rights principles and have current working knowledge of the rules and requirements of RIPA and the use of this guidance.

The Single Point of Contact

8.14 The Single Point of Contact (SPoC) is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and a communications service provider. To become accredited an individual must complete a course of training appropriate for the role of a SPoC. An accredited SPoC promotes efficiency and good practice in ensuring any practical and lawful requirements for communications data are undertaken. The SPoC provides objective judgment and advice to both the Applicant and the Designated Person, in this way the SPoC provides a guardian and gatekeeper function ensuring that public authorities act in an informed and lawful manner.

8.15 Norfolk County Council is a member of the National Anti-Fraud Network (NAFN). NAFN is a 'One Stop' data and intelligence provider for all public bodies. As part of their portfolio they offer a comprehensive SPoC service. Norfolk County Council now has no in house SPoCs and NAFN should be used for this service.

The Senior Responsible Officer

8.16 The senior responsible officer role is set out at paragraphs 4.1 to 4.4 above.

On what grounds can the acquisition of communications data be authorised. Is the proposed request for the acquisition of communications data necessary?

8.17 In the case of Local Authorities, acquisition and disclosure of communications data can only be authorised if it is **necessary** for the purpose of preventing or detecting crime or preventing disorder. It is extremely important to consider whether the acquisition of the particular communications data is necessary. If an investigation can be carried out by means which do not involve such acquisition then these should be used. If there are no other means then this should be stated on the authorisation form.

Is the proposed request for the acquisition of communications data proportionate?

8.18 Authority to acquire communications data should not be given unless the person authorising the request is satisfied that the application is **proportionate**. The designated person should make sure that any interference with the privacy of an individual is justified by the end being sought. If the benefit to be obtained from acquiring communications data is marginal, the person authorising should think very carefully about the use of such an investigation technique. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

8.19 Suggested areas to consider include the seriousness of the offence, the expense of the operation and other means by which the information could be obtained. In addition the activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Might the acquisition of communications data involve collateral intrusion?

8.20 The designated person needs to consider whether the application might intrude upon the privacy of people, other than those who are the subject of the investigation. The designated person should be sensitive to the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefit of the investigation. If there is considered to be a risk of collateral intrusion, consideration must be given to minimising this risk during the authorisation process.

The procedure - Applying for authority to acquire communications data

8.21 Applicants and Designated Persons (DP) must submit, approve and track applications through the central NAFN website, using the NAFN online forms. An allocated SPoC will then check for legal compliance and, where necessary, provide feedback before submitting for final authorisation from the DP.

8.21.1 Once an application is authorised by the DP it must be subject to judicial approval as per paragraph 5.47 above. NAFN will provide the applicant with a 'Court Pack' containing:

- Final case application
- Judicial application/order form
- Relevant Assurance(s), Authorisation(s) and/or Notice(s)

8.22 These documents will enable the applicant to present their application at court.

8.22.1 If the application is approved all documentation must be returned to NAFN for subsequent processing via the secure online system. The NAFN SPoC administers all requests promptly to obtain the data required. Results are uploaded to the secure website for retrieval, with all aspects of administration covered by NAFN, including the tracking of reportable/recordable errors, cancellations, and withdrawals.

8.25 The application should describe in detail the communications data to be acquired and the purpose of the investigation operation. The application should also include:

(1) the name

(2) the office, rank or position held by the person making the application

(3) the operation name to which the application relates

(4) a unique reference number

(5) the specific purpose for which the data is required

(6) a description of the communications required specifying where relevant any historic or future date and where appropriate time periods

(7) an explanation as to why the acquisition of that data is considered necessary and proportionate and what is thought to be achieved by acquiring it

(8) Consideration of any meaningful collateral intrusion and why that intrusion is justified in the circumstances.

(9) an identification and explanation of the timescale within which the data is required.

(10) an assessment by the SPOC

(11) the application should record whether it was approved or not by a Designated Person by whom and when the decision was made.

8.26 An authorisation provides for persons within a public authority to engage in specific conduct relating to a postal service or telecommunications system to obtain communications data. An authorisation may be appropriate where a communications service provider is not capable of obtaining or disclosing communications data or a designated person believes the investigation or operation may be prejudiced if the communications service provider is required to obtain or disclose the data or there is an agreement in place between the public authority and a communication service provider relating to appropriate mechanisms for disclosure of communications data or a designated person considers there is a requirement to conduct a telephone subscriber check but the communications service provider as yet to be conclusively determined as the holder of the communications data. The authorisation is not served upon a communications service provider, although there may be circumstances where the provider may require or may be given assurance that conduct being undertaken is lawful. That assurance may be given by disclosing details of the authorisation itself.

Notices

8.27 The giving of a notice is appropriate where a communications service provider is able to retrieve or obtain specific data and to disclose that data unless the grant of an authorisation is more appropriate. A notice may require a communications service provider to obtain any communications data if that data is not already in their possession. The decision of a Designated Person whether to give a notice shall be based upon information presented to them in an application. The notice should contain enough information to allow the communications service provider to comply with the requirements of the notice. A notice must:

(a) be given in writing or if not in the manner that produces a record of its having been granted;

(b) specify the purpose for which the notice has been given;

(c) describe the communications data to be obtained or disclosed under the notice specifying where relevant, any historic or future date and where appropriate time periods;

(d) include an explanation that complies with the notices as a requirement of the Act;

(e) specify the office, rank or position held by the designated person and the designated person's name should also be recorded;

(f) specify the manner in which the data should be disclosed, the notice should contain sufficient information to enable a communications service provider to confirm the notice is authentic and lawful;

(g) record the date and when appropriate to do so at the time when the notice was given by the designated person;

(h) where appropriate the notice should provide an indication of any urgency or time within which the communications service provider is requested to comply with the requirements of the notice. In giving notice a designated person may only require a communications service provider to disclose the communications data to the designated person or a specified person working within the same public authority.

Duration of authorisations and notices

8.28 Relevant to all authorisations and notices is the date upon which the authorisation or notice takes effect, which is the date on which judicial approval is given. From that date when the authorisation or notice becomes valid it has a validity of a maximum of one month, this means that the conduct authorised should have been commenced or the notice served within that month. All authorisations and notices must relate to the acquisition or disclosure of data for a specified date or period. Any periods should clearly be indicated in the authorisation or notice. A start date and end date should be given and where a precise start and end time are relevant, these must be specified. Where an authorisation or notice relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month.

Renewal of authorisations and notices.

8.29 Any valid authorisation or a notice may be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice and again judicial approval must be obtained before the renewal can take effect. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing. The reasoning for seeking renewal

should be set up by an Applicant in an addendum to the application upon which the authorisation or notice being renewed was granted or given. The Designated Person should give careful consideration to renewal of an authorisation or notice and should:

(a) consider the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and

(b) record the date and when appropriate to do so the time when the authorisation or notice is renewed.

8.30 The designated person should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise would impact on the proportionality of the authorisation or notice and impose unnecessary burden on a communications service provider.

Cancellations and Withdrawals

8.31 A designated person who has given notice to a communications service provider shall cancel the notice if at any time after giving the notice, it is no longer necessary for the communications service provider to comply with the notice or the conduct required by the notice is no longer proportionate to what is sought to be achieved. Equally where a designated person considers an authorisation shall cease to have effect because the conduct authorised becomes unnecessary or no longer proportionate to what is sought to be achieved, the authorisation shall be withdrawn. The communications service provider should be advised of the withdrawal of an authorisation.

8.32 Cancellation of a notice must be:

(a) undertaken in writing;

(b) identified by reference to its unique reference number, the notice being cancelled;

(c) record the date and when appropriate to do so, the time when the notice was cancelled and

(d) specify the office rank or position held by the designated person cancelling the notice.

8.33 Withdrawal of an authorisation should be:

(a) undertaken in writing;

(b) identified by reference to its unique reference number, the authorisation being withdrawn;

(c) record the date and when appropriate to do so the time when the authorisation was cancelled;

(d) record the name, the office, rank or position held by the designated person withdrawing the authorisation.

Keeping of records

8.34 Completed original documents must be retained centrally by the SPOC, in written or electronic form, for a period of at least three years from the date of authorisation. The documents should be classified and stored securely in accordance with the Government protected marking scheme. In addition, a record should be kept of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. These records should be available for inspection by the Investigatory Powers Commissioner's Office upon request. (The retention of documents is a service provided by NAFN.)

8.35 On an annual basis nplaw must send to the Investigatory Powers Commissioner's Office, information as to the number of applications submitted to the designated person, the number of notices issued, number of authorisations issued and the number of times an urgent notice is given orally.

Errors

8.36 Proper application of the contents of this guidance should reduce the scope for making errors but if an error occurs in the grant of an authorisation or the giving of a notice or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept and a report made to the Commissioner. (The recording and reporting of errors is a service provided by NAFN.)

Investigatory Powers Act 2016

8.37 The provisions in RIPA relating to the acquisition of communications data are expected to be replaced (and largely replicated) by similar provisions contained in the Investigatory Powers Act 2016. This guidance will be updated to reflect the position when the relevant provisions of the 2016 Act have been brought into force.

9. COMPLAINTS

9.1 Where any person expresses their dissatisfaction with a surveillance operation carried out by the Council or with a communications data issue and they are either unwilling to accept an explanation or are dissatisfied with the explanation offered or they wish to complain about any other aspect of the Council's operations under RIPA, they must be informed of the existence of the Investigatory Powers Tribunal.

9.2 Every assistance shall be given to the person to complain to the Council's Corporate Complaints Officer or to make contact with the Tribunal and make their dissatisfaction known to it.

9.3 The address for the Investigatory Powers Tribunal is
PO Box 33220
London
SW1H 9ZQ.
Tel: 0207 035 3711
Website address: www.ipt-uk.com

9.4 These procedures are mutually exclusive.

10. FURTHER INFORMATION

10.1 There is helpful information on the Gov.uk web site about RIPA. See https://www.gov.uk/guidance/surveillance-and-counter-terrorism

10.2 Advice can be provided by nplaw on issues connected with RIPA. In this respect please contact Louise Hartley – Lawyer, nplaw (ext. 222974) in the first instance.

10.3 Departments also need to consider what their training needs are in this area and nplaw is also willing to discuss what help can be offered with this.

10.4 Please also contact Louise Hartley for copies of the relevant forms, if difficulties are encountered accessing them via the intranet.

Appendix A

NORFOLK COUNTY COUNCIL

Senior Responsible Officer; Officers Authorised to Approve Applications For Directed Surveillance and CHIS;Designated Persons for Communications Data Applications

Officer	Name	Telephone Number
Managing Director	Wendy Thomson (Authorising Officer for confidential material	01603 222609
Chief Legal Officer	Victoria McNeill Senior Responsible Officer (SRO)	01603 223415
Trading Standards – Authorising Officers	Sophie Leney (also authorised Designated Person for Communications Data)	01603 224275
	Shaun Norris (also authorised Designated Person for Communications Data)	01553 669256
	Alice Barnes (also authorised Designated Person for Communications Data)	01603 222749
	Brian Chatten (also authorised Designated Person for Communications Data)	01603 638075
	Jon Peddle (also authorised Designated Person for Communications Data)	01603 224380
	Nick Johnson (also authorised Designated Person for Communications Data)	01603 228940

SPoC Service provided by NAFN

Appendix B

Guidance on Completing Application for Authority for
Directed Surveillance

Read this guide in conjunction with the Model RIPA form. The level of detail officers need to complete the form is crucial. It is important to include as much information as is known, otherwise the application may not be authorised. Applicants must be familiar with the contents of the full Guidance Notes.

Applicant is officer applying for authority to carry out directed surveillance.

Unit/Team: team where applicant works

Full address: The applicants base either county hall or other

Contact Details: Contact details of the applicant including telephone and email

Operation name: only if one has been assigned

Unique Reference Number: to be included on every form

Details of application

Part 1 - Level of authority

See Appendix A of Procedure Guide. In case of urgency, and a person detailed in Appendix A not being available, then seek guidance or seek advice from nplaw.

Part 2 - Give an account of the investigation or operation

Details of the investigation to date. Brief clear specifics. Full details of the crime being investigated must be included.

Part 3 - The action to be authorised, including any premises or vehicles involved

What form is the surveillance to take and why? For example will it be mobile surveillance or from an observation point or van? Description of activities planned needed. Full details of dates, times, officer numbers involved and equipment to be used must be noted as far as is possible.

Part 4 - The identities, where known, of those to be subject of the directed surveillance

Sometimes not known and identifying those involved in an activity can be the reason for surveillance. If identities are not known then it should be so stated. The premises and/or vehicles to be targeted should be identified here in detail.

Part 5 - Explanation of the information which it is desired to obtain as a result of the authorisation

What is the key objective(s) of the surveillance?

Parts 6&7 - Grounds on which action is necessary

The application must show that the directed covert surveillance is considered necessary in the proposed operation. All other methods of investigation not requiring covert surveillance must be detailed and reasons given for why they are not to be used.

The officer must detail why covert surveillance is the only method by which the information required can be obtained.

Part 8 - Collateral Intrusion

Having identified who, what and where you want to carry out surveillance, you should also consider who else might be affected. Will the private life of others be affected in some way? You must show that you have considered this and have planned how to minimise the intrusion.

Part 9 - Explain why directed surveillance is proportionate to what it seeks to achieve

The application should only be authorised if it demonstrates that the activity to be carried out is proportionate to what it seeks to achieve. Full reasons must be given as to why the methods to be employed are not disproportionate (ie not a “sledgehammer to crack a nut”). This includes detailing not only why covert surveillance must be used rather than any other method of investigation, but also stating that the method to be used is the least intrusive way of obtaining the information. It is not enough to rely on the seriousness of the offence or the cost of employing other methods.

All forms MUST address the following points:

1. The size and scope of the investigation must be weighed against the gravity and extent of the crime under investigation

2. An explanation of how and why the methods to be adopted will cause the least possible intrusion on the target and others

3. It must be shown that the activity planned is the only reasonable way, having considered all others, of obtaining the necessary information

4. Details of all other method considered and why they were not implemented.

Part 10 - Confidential Material

Are you likely to come across material relating to communications between a lawyer and client, or personal information relating to physical or mental health or spiritual counselling (communication between an individual and minister of religion), or confidential journalistic material?

This should be considered and highlighted. If such material is likely then the level of authorisation required rises. If there is any doubt, advice must be sought from nplaw.

Authorisation

Parts 12 & 13 - Authorising Officer's Statement

The authorising officer must give the information requested and state in writing that he is satisfied, or why he believes that the activities to take place are necessary and proportionate (see previous explanations of these matters).

The proportionality of the activity must take into account any possibility of collateral intrusion.

All such activity subject to the authorisation must not be considered arbitrary or unfair.

The authorising officer must record that they have considered these matters, and are satisfied the surveillance should still be authorised. If the authorising officer is not satisfied that enough detail has been provided he should refuse the application. If the authorising officer disagrees with certain aspects of the proposed activity he should mark this clearly on the form as unauthorised.