MANCHESTER
CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 ("RIPA") CORPORATE POLICY AND PROCEDURES

Document Control

Title	RIPA Corporate Policy and Procedures
Document Type	Policy and Guidance
Author	Ian Mark – Senior Lawyer Democratic Legal Services Team
Owner	Liz Treacy – City Solicitor
Subject	Investigatory Powers
Protective marking	UNCLASSIFIED
Created	22 June 2015
Approved	1 July 2015
Review period	Annually

Revision History

Version Date	**Author**	**Description of Change**
1.0 - 27 July 2016	Ian Mark	Revisions/updating to existing clauses and new clause 8 added
2.0 – March 2019	Ian Mark	Revisions/updating following amendments to Home Office Codes of Practice and the disestablishment of OSC and IOCCO

Contents **Page**

1. Abbreviations

CCTV	Closed Circuit Television
CSP	Communications service provider
Council	Manchester City Council
CHIS	Covert human intelligence sources
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom agreed on 2 November 1950
HRA	Human Rights Act 1998
IPCO	**The Investigatory Powers Commissioner's Office**
NAFN	The National Anti-Fraud Network
PFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPoC's	Single Points of Contact for acquisition and disclosure of communications data

Introduction

This Corporate Policy & Procedures is based upon the requirements of the Regulation of Investigatory Powers Act 2000 and the Home Office's Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

The use of covert surveillance, covert human intelligence sources and the acquisition of service use or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law. However, they should be used only rarely and in exceptional circumstances. RIPA requires that public authorities follow a clear authorisation process prior to using these powers. Authorisations granted under Part II of RIPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the ECHR.

Consequences of Failing to Comply with this Policy

Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this Policy may result in the Council's actions being deemed unlawful by the Courts under Section 6 of the HRA or by the Investigatory Powers Tribunal, opening up the Council to claims for compensation and loss of reputation. Additionally, any information obtained that could be of help in a prosecution will be inadmissible.

All uses of RIPA should be referred to the Democratic Services Legal Team for preliminary advice at the earliest possible opportunity.

2. Background

On 2 October 2000 the Human Rights Act 1998 ("HRA") made it unlawful for a local authority to breach any article of the ECHR. An allegation that the Council or someone acting on behalf of the Council has infringed the ECHR is dealt with by the domestic courts rather than the European Court of Justice.

The ECHR states:

(a) individuals have the right to respect for their private and family life, home and correspondence (Article 8 ECHR); and

(b) there shall be no interference by a public authority with the exercise of this right unless that interference is:
- **in accordance with the law;**
- **necessary; and**
- **proportionate**

RIPA, which came into force on 25 September 2000, provides a lawful basis for 3 types of investigatory activity to be carried out by local authorities which might otherwise breach the ECHR. The activities are:

- covert directed surveillance;
- covert human intelligence sources ("CHIS"); and
- acquisition and disclosure of communications data.

RIPA sets out procedures that must be followed to ensure the RIPA activity is lawful. Where properly authorised under RIPA the activity will be a justifiable interference with an individual's rights under the ECHR; if the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government Ombudsman or a complaint made to the Investigatory Powers Tribunal. In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA seeks to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

What RIPA Does and Does Not Do

RIPA does:
- Require prior authorisation of directed surveillance.
- Prohibit the council from carrying out intrusive surveillance.
- Compel disclosure of communications data from telecom and postal service providers.
- Permit the Council to obtain communications records from communications service providers.
- Require authorisation of the conduct and use of CHIS.
- Require safeguards for the conduct of the use of a CHIS.

RIPA does not:

- Make unlawful conduct which is otherwise lawful.
- Prejudice any existing power to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property.
- Apply to activities outside the scope of Part II of RIPA, which may nevertheless be governed by other legislation, including the HRA. A public authority will only engage RIPA when in performance of its 'core functions' – i.e. the functions specific to that authority as distinct from all public authorities.

Under no circumstances can local authorities be authorised to obtain communications traffic data under RIPA. Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

3. Policy Statement

The Council is determined to act responsibly and in accordance with the law. To ensure that the Council's RIPA activity is carried out lawfully and subject to the appropriate safeguards against abuse, the Council adopted a corporate code of practice for surveillance ("the Code") on 10 July 2002 which has subsequently been reviewed, amended and renamed the Corporate Policy and Procedures as detailed below.

All staff who are considering undertaking RIPA activity should be aware that where that activity may involve handling confidential information or the use of vulnerable or juvenile persons as sources of information, a higher level of authorisation is required. Please see 4.6 (in respect of handling confidential information) and 5.2 (in respect of using information sources who are vulnerable or juvenile persons) below.

The Code was revised on:

- 1 August 2003 (following the introduction of the codes of practice issued under section 71 of RIPA on covert surveillance and CHIS);
- 5 January 2004 (following the RIPA (Directed Surveillance and CHIS) Order 2003).
- April 2010 (following the introduction of the new Codes of Practice on covert surveillance and CHIS; the Regulation of Investigatory Powers (Communications Data) Order 2010; and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010).
- July 2015 (following the significant amendments to RIPA introduced by the Protection of Freedoms Act 2012). These changes are discussed in paragraph 4.5 below.

The Code was redrafted following the Office of Surveillance Commissioners' Inspection on 6 April 2004 and again following the Interception of Communications Commissioner's Office inspection on 19 July 2006.

The Code was further revised in March 2019 following the amendments to the Home Office Codes of Practice in respect of Covert Surveillance and CHIS, and disestablishment of the Office of the Surveillance Commissioner (OSC) and the Interception of Communications Commissioners Office (ICCO).

The following documents are available on the Council's intranet (see **11**.1):

- Home Office Statutory Codes of Practice on:
  - Covert Surveillance and Property Interference
  - Covert Human Intelligence Sources
  - Acquisition and Disclosure of Communications Data
- Home Office Guidance on Protection of Freedoms Act 2012 – changes to RIPA
- lists of authorising officers and designated persons (posts and names);
- RIPA forms for covert surveillance; CHIS and acquisition and disclosure of communications data;
- application for Judicial approval and Order made for Judicial approval;
- the corporate CCTV policy;
- corporate RIPA training

The City Solicitor is the Council's Senior Responsible Officer (SRO) and is responsible for the following roles:

- Appointing Authorising Officers (see **9**.1(a))
- Appointing Designated Persons (see **9**.1(a))
- Maintaining a central record of all RIPA authorisations,
- Arranging training to individuals appointed as Authorising Officers and Designated Persons, and
- Carrying out an overall monitoring function as the SRO for the Council's use of RIPA powers.

The City Council's RIPA Co-ordinator is based in the Democratic Legal Services Team, Legal Services.

Any officer who is unsure about any RIPA activity should contact either the City Solicitor or the Democratic Services Legal Team for advice and assistance.

4. Types of Surveillance

Surveillance can be overt or covert and includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance **with or without the assistance of a surveillance device.**

4.1 Overt Surveillance

The majority of the Council's surveillance activity will be overt surveillance i.e. will be carried out openly. For example (i) where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted; and (ii) where the Council advises a tenant that their activities will be monitored as a result of neighbour nuisance allegations **(iii) or where an officer uses body worn cameras and informs the individual that the camera will be switched on and recording will take place.** This type of overt surveillance is normal Council business and is not regulated by RIPA.

4.2 Covert Surveillance

This is where surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware it is taking place.

Where covert surveillance activities are unlikely to result in obtaining of any private information about a person (because the surveillance although covert is general or low level, and is not directed at particular individuals), no interference with Article 8 rights occurs, and an authorisation under RIPA is not required. RIPA authorisation may be required where the surveillance is repeated for a particular purpose and could amount to systematic surveillance of an individual; if in doubt seek advice from the Democratic Services Legal Team.

Covert surveillance can be intrusive or directed. **The Council is not permitted to carry out covert intrusive surveillance**. Para 4.3 below explains when covert surveillance is intrusive and therefore not permitted. The Council is permitted to carry out covert directed surveillance subject to strict compliance with RIPA. Paragraph 4.4 below explains when covert surveillance is directed.

4.3 Covert Intrusive Surveillance

Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private vehicle and which involves the presence of an individual or surveillance device on the premises or in the vehicle, or which uses a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside.

Additionally, the Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation.

4.4 Covert Directed Surveillance

This is surveillance that is:

- covert
- not intrusive;
- for the purposes of a specific investigation or operation;
- likely to obtain private information[1] about a person (whether or not that person was the target of the investigation or operation); and
- not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place.

4.5 Directed Surveillance Crime Threshold

Following the changes to RIPA introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 a crime threshold applies to the authorisation of directed surveillance by local authorities.

Local Authority Authorising Officers may not authorise directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND meets the following:

- The criminal offence is punishable by a maximum term **of at least 6 months imprisonment**, or
- Would constitute an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 **(offences involving sale of tobacco and alcohol to underage children)** regardless of length of prison term.

The Crime threshold **only** applies to Directed Surveillance, not to CHIS or Communications Data.

The Home Office Code of Practice for covert surveillance can be found on the Home Office website at https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice.

4.6 Confidential Information

A higher level of authorisation to apply to the Magistrates Court is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained. For the purpose of RIPA this includes:

- communications subject to legal privilege[2];

[1] Private information includes any information relating to a person's private and family life, home and correspondence (whether at home, in a public place or in the work place).

[2] Legal privilege is defined in section 98 of the Police Act 1997 as:
- communications between a professional legal adviser and his client, or any person representing his client which are made in connection with the giving of legal advice to the client.

- communications between a member of parliament and another person on constituency matters;
- confidential personal information[3]; and
- confidential journalistic material[4]

The authorising officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. **Authorisation can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service.**

Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from the City Solicitor or the Democratic Services Legal Team prior to making any application.

5. Covert Human Intelligence Sources ("CHIS")

5.1 CHIS

The Council is permitted to use CHIS subject to strict compliance with RIPA.

A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:

(a) covertly using the relationship to obtain information or provide access to information to another person, or
(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf. Authorisation for CHIS can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder."

- communications between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.
- items enclosed with or referred to in communications of the kind mentioned above and made in connection with the giving of legal advice, or in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

Communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

If advice is required on this point, officers should contact the City Solicitor or the Democratic Services Legal Team.

[3] Confidential personal information is described at **paragraph 9.29 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice.**

[4] Confidential journalistic material is described at **paragraph 9.38 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice**.

Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

However, by virtue of section 26(8) (c) of RIPA, there may be instances where an individual*, who* covertly discloses information though not tasked to do so may nevertheless be a CHIS. The important question is how did the member of the public acquire the information which they volunteer. If they acquired it in the course of, or as a result of the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS. If the Council then makes use of the information, and the informant is thereby put at risk, the Council may be in breach of its duty of care owed to the individual. It is recommended that legal advice is sought in any such circumstances.

The Home Office Covert Human Intelligence Sources Code of Practice can be found on the Home Office website.

5.2 Vulnerable Individuals / Juvenile CHIS

Additional requirements apply to the use of a vulnerable individual[5] or a person under the age of 18 as a CHIS. In both cases **authorisation for an application to the Magistrates Court can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service**. **Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the City Solicitor or the Democratic Services Legal Team prior to making the application.**

The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them.

In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

6. CCTV

The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. However, there are specific provisions regulating the use of CCTV cameras in public places and buildings and the Council has drawn up a Corporate CCTV Policy which officers must comply with and which can be found on the Council's intranet. However if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.

---

[5] A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation. However, the use of the same CCTV system to conduct planned surveillance of an individual and record his movements is likely to require authorisation.

Protocols should be agreed with any external agencies requesting use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

7. Acquisition and Disclosure of Communications Data

7.1 Communication Service Providers ("CSPs")

CSPs are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Council must obtain communications data from CSPs in strict compliance with RIPA.

7.2 Types of Communications Data

Communications data is the 'who', 'where', 'when' and 'how' of a communication such as a letter, phone call or e-mail but not the content, not what was said or written. The Council is not able to use RIPA to authorise the interception or acquisition of the content of communications. There are three types of communication data:

Service Use Information – this is data relating to the use made by any person of a postal or telecommunications, internet service, or any part of it. For example itemised telephone call records, itemised records of connection to internet services, itemised timing and duration of calls, connection/disconnection/reconnection data, use of forwarding or re-direction services, additional telecom services and records of postal items.

Subscriber Information – This is information held or obtained by the CSP about persons to whom the CSP provides or has provided a communications service. For instance, subscribers of email and telephone accounts, account information including payment details, address for installing and billing, abstract personal records and sign up data.

Traffic Information – this is data that is comprised in or attached to a communication for the purpose of transmitting it and which identifies a person or location to or from which it is transmitted. **The Council is not permitted to access traffic data.**

7.3 Authorisation and Notices

RIPA provides for acquisition and disclosure of communications data by two alternative means:

- authorisation of a person within the Council to engage in specific conduct, in order to obtain communications data (a section 22(3) RIPA authorisation); and
- a notice issued to a CSP requiring them to collect or retrieve and then provide the communications data (a section 22(4) RIPA notice).

A section 22(3) RIPA authorisation is appropriate where (for instance) there is an agreement in place between the Council and the relevant CSP regarding the disclosure of communications data which means a notice is not necessary (currently

the Council does not have any such agreements in place); or the Council needs to identify an individual to whom communication services are provided but the relevant CSP is not yet known to the Council, making it impossible to issue a notice.

A section 22(4) RIPA notice is appropriate where the Council receives specific communications data from a known CSP. A notice may require a CSP to obtain any communications data, if that data is not already in its possession. However, a notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do.

As a local authority the Council must fulfil two additional requirements when acquiring communications. Firstly, the request must be made through a SPoC at NAFN (see more about NAFN at **9**.1(b) and **9**.4). Secondly, the request must receive prior judicial approval.

Under sections 23A and 23B of RIPA the Council must also obtain judicial approval for all requests for communications data. Judicial approval must be requested once all the Council's internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. The authorisation must be provided by a magistrate.

The Home Office Acquisition and Disclosure of Communications Data Code of Practice can be found on the Home Office website and on the intranet.

8. Use of Social Media / Internet

The internet may be utilised to obtain information including viewing specific user profiles on Social Networking Sites ('SNS'), or searching SNS to try to find profiles that contain useful information. Used correctly, research of SNS might provide invaluable evidence or at least useful intelligence.

Some activity on SNS might however constitute Directed Surveillance or require CHIS authorisation, some may not. Similarly some research might be likely to result in the obtaining of private information, some may not. Activity that does not meet the threshold for RIPA authorisation but might be likely to result in obtaining private information will require consideration of Human Rights issues such as balancing the protection of rights with the breach of privacy, necessity and proportionality. It is important to note that images of persons are private information, and also for officers to be aware that it is possible they might obtain private information about other individuals not just the specific user on the profiles which are viewed, captured or recorded. These individuals might not even be aware this private information has been made public by the profile/account holder.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

If it is necessary and proportionate for an officer to breach access controls covertly, 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). This could occur if an officer covertly asks to become a 'friend' of someone on a SNS. It is not unlawful for a member of 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.

Use of an established overt presence of the public authority on the SNS website to look at publicly available information on the profile is possible and viable if the Council already has an established presence on the SNS which is used to publicly and overtly make the presence of the Council known, however this does not mean that information freely displayed on a profile is "fair game". The first visit to an SNS profile which might be displaying lots of private information could be regarded as a 'drive by' however any subsequent visits, particularly on a regular basis are likely to require authorisation for directed surveillance if the Council is likely to obtain private information, and this would be obvious as a result of the initial visit.

9. Authorisation Procedures

9.1 (a) Authorising Officers/Designated Persons for directed surveillance and CHIS

Authorising Officers are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

Designated Persons fulfil a similar role in relation to applications to obtaining communications data, assessing and approving authorisations and notices.

It is the responsibility of Authorising Officers and Designated Persons to ensure that when applying for authorisation the principles of necessity and proportionality (see 9.2 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (9.8- 9.10 below).

Lists of authorising officers and designated persons are available on the Council's intranet. Any requests for amendments to the lists must be **made in writing and** sent to the City Solicitor.

Schedule 1 of statutory instrument No. 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). Schedule 2 of statutory instrument No. 480 (2010) prescribes the rank or position of designated person for the purposes of Section 25(2) of RIPA (access to communications data). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent". The term Director is not defined within the Act but in Manchester City Council it has been determined that it would normally equate to second or third tier management unless otherwise determined by the City Solicitor.

The City Solicitor designates which officers can be authorising officers or designated persons. Only these officers can authorise directed surveillance, the use of CHIS and acquisition and disclosure of communications data. **All authorisations must follow the procedures set out in the Policy.** Authorising officers/designated persons are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the City Solicitor.

9.1 (b) Single Point of Contact (SPoC)

SPoCs are responsible for advising officers within the Council on how best to go about obtaining communications data, for liaising with CSPs, and advising whether applications and notices are lawful. As required under the latest Acquisition and Disclosure of Communications Data Code of Practice, the Council has engaged the National Anti-Fraud Network (NAFN). NAFN's SPoC services relate only to communications data.

For information on using NAFN, see **9**.4 below.

9.2 Authorisation of Covert Directed Surveillance, Use of a CHIS and Acquisition and Disclosure of Communications Data.

RIPA applies to all covert directed surveillance, use of CHIS and acquisition and disclosure of communications data whether by Council employees or external agencies engaged by the Council. Council officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant application form (see para **9.**6) and forward it to the relevant authorising officer. Authorisations or notices in relation to communications data should be referred to NAFN.

All uses of RIPA should be referred to the Democratic Services Legal Team for preliminary advice.

Directed surveillance, use of a CHIS and acquisition and disclosure of communications data can only be authorised if the authorising officer/designated person is satisfied that the activity is:-

(a) **in accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council. As such the Council is unable to access communications data for disciplinary matters;

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and there is a crime threshold for directed surveillance as described in paragraph 4.5 above; and

(c) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

Applicant officers should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the ECHR

- what other reasonable methods of obtaining information have been considered and why they have been discounted

Authorising officers/designated persons should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

Particular consideration should be given to **collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation**. Collateral intrusion occurs when an officer undertaking covert surveillance on a subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the authorising officer/designated person, particularly when considering the proportionality of the surveillance.

Particular care must be taken in cases where **confidential information** is involved e.g. matters subject to legal privilege; confidential personal information; confidential journalistic material; confidential medical information; and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to the City Solicitor or the Democratic Services Legal Team for advice.

The activity must be authorised before it takes place.

At the time of authorisation the authorising officer/designated person must set a date for review of the authorisation and review it on that date (see **9**.8).

A copy of the completed Home Office application and authorisation form must be forwarded to the Democratic Services Legal Team within one week of the authorisation by fax or e-mailed as a scanned document. In the case of a section 22(4) RIPA notice requiring disclosure of communications data a copy of the notice must be attached to the application form. The Democratic Services Legal Team will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

Approval by Magistrates Court

Following changes under the Protection of Freedoms Act 2012, there is now an additional stage in the process for all three investigatory activities (Directed Surveillance, CHIS and Communications Data). After the Authorisation form has been countersigned by the authorising officer/designated person, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

The magistrate will have to decide whether the council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the surveillance techniques (i.e. Directed Surveillance, CHIS and Communications Data) at the same time.

In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation, but could create an unnecessary administrative burden. Where the Council is not the lead authority in the circumstances, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

It should be noted that only the initial authorisation and any renewal of the authorisation require magistrates' approval.

There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified but they do need to be authorised by the City Solicitor to represent the Council in court.

The Role of the Magistrates Court

The role of the Magistrates Court is set out in section 23A RIPA (for communications data) and section 32A RIPA (for directed surveillance and CHIS).

These sections provide that the authorisation, or in the case of Communications Data, the notice, shall not take effect until the Magistrates Court has made an order approving such authorisation or notice. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
    - arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;
- The local authority application has been authorised by an authorising officer or designated person (as appropriate);
- The grant of the authorisation or, in the case of communications data, notice was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
    - 25(3) (for communications data),
    - 29(7)(a) (for CHIS),
    - 30(3) (for directed surveillance and CHIS)

The procedure for applying for directed surveillance or use of a CHIS is:

Applicant officer obtains preliminary legal advice from Democratic Services Legal Team

Applicant officer completes an application

Authorisation is sought from the Authorising Officer

Applicant officer/legal representative creates court pack and applicant *officer* proceeds to court

Applicant officer organises the directed surveillance or use of a CHIS to take place

Applicant officer sends copy Magistrates Court order to Democratic Services Legal Team

9.3 Additional Requirements for Authorisation of a CHIS

A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day to day responsibility for dealing with the CHIS **(CHIS handler**) and a senior Council officer with oversight of the use made of the CHIS **(CHIS controller**);
- a risk assessment has been undertaken to take account of the CHIS security and welfare;
- a Council officer is responsible for maintaining a record of the use made of the CHIS;
- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS

9.4 Additional Requirements for Authorisation of Acquisition and Disclosure of Communications Data

The rules on the granting of authorisations for the acquisition of communications data are slightly different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:

- Applicant Officer
- Designated Person
- Single Point of Contact

<u>Applicant</u>

This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The application form must:

- set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder.

- describe the communications data required i.e. the telephone number, email address, the specific date or period of the data and the type of data required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted.

- explain why the conduct is necessary and proportionate.

- consider and describe any meaningful collateral intrusion. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it.

Designated Person

This is the person who considers the application. A designated person's role is the same as an authorising officer's role in relation to directed surveillance and CHIS authorisations. The designated person assesses the necessity for any conduct to obtain communications data taking account of any advice provided by the single point of contact (SPoC). If the designated person believes it is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

Single Point of Contact (SPoC)

The accredited SPoCs at NAFN scrutinise the applications independently, and provide advice to applicant officers and designated persons ensuring the Council acts in an informed and lawful manner.

The procedure for applying for acquisition of communications data:

Applicant obtains preliminary legal advice from Democratic Services Legal Team

Applicant officer creates an application using the Cycomms Web Viewer on the NAFN website

SPoC Officer at NAFN triages and accepts the application into the Cyclops system

SPoC Officer uses Cyclops to update the application details and completes the SPoC report

Approval is sought from the Designated Person (DP)

SPoC sends request for Court Pack preparation to Applicant/Legal Representative

Applicant/legal representative generates court pack using the Web Viewer and applicant proceeds to court

SPoC receives signed court documents and sends requests to Communications Service Provider (CSP)

SPoC receives results back from CSP and returns results to Applicant

Applicant accesses the Web Viewer and downloads results

Applicant sends copy Magistrates Court order to Democratic Services Legal Team

9.5 Urgent Authorisations

By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are no longer available.

9.6 Application Forms

Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation.

(a) Directed Surveillance (external site)

Application for Authority for Directed Surveillance
Application for Judicial Approval for Directed Surveillance
Review of Directed Surveillance Authority
Cancellation of Directed Surveillance
Renewal of Directed Surveillance Authority

(b) CHIS

Application for Authority for Conduct and Use of a CHIS
Review of Conduct and Use of a CHIS
Cancellation of Conduct and Use of a CHIS
Renewal of Conduct and Use of a CHIS

(c) Acquisition and Disclosure of Communications Data

Application for a section 22(4) RIPA Notice
Notice under section 22(4) RIPA requiring Communications Data to be Obtained and Disclosed

9.7 Duration of the Authorisation

Authorisation/notice durations are:

- for covert directed surveillance the authorisation remains valid for 3 months after the date of authorisation
- for a CHIS the authorisation remains valid for 12 months after the date of authorisation (or **four** months if a juvenile CHIS is used).
- a communications data notice remains valid for a maximum of 1 month.

Authorisations should not be permitted to expire, they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all authorisations must be reviewed to decide whether to cancel or renew them.

9.8 Review of Authorisations

As referred to at **9.**2 authorising officers/designated persons must make arrangements to periodically review any authorised RIPA activity.

Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the authorising officer/designated person if there is any doubt as to whether it should continue. **For Juvenile CHIS's, the Code of Practice stipulates that the authorisation should be reviewed on a monthly basis.**
Reviews should be recorded on the appropriate Home Office form (see **9**.6).

A copy of the Council's notice of review of an authorisation must be sent to the Democratic Services Legal Team within one week of the review to enable the central record on RIPA to be authorised.

9.9 Renewal of Authorisations

If the authorising officer/designated person considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained. Renewed authorisations will normally be for a period of up to 3 months for covert directed surveillance, 12 months in the case of CHIS, **4 months** in the case of juvenile CHIS and 1 month in the case of a communications data authorisation or notice. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation. Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form (see **9**.6). The reasoning for seeking renewal of a communications data authorisation or RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

All renewals will require an order of the Magistrates Court in accordance with the requirements in para **9**.2 above.

A copy of the Council's notice of renewal of an authorisation must be sent to the Democratic Services Legal Team within one week of the renewal together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

9.10 Cancellation of Authorisations

The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance, CHIS or communications data authorisation or notice no longer meets the criteria for authorisation. Cancellations must be made on the appropriate Home Office form (see **9**.6). In relation to a section 22(4) notice to a CSP, the cancellation must be reported to the CSP by the designated person directly or by the SPoC on that person's behalf.

Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters are addressed.

A copy of the Council's notice of cancellation of an authorisation must be sent the Democratic Services Legal Team within one week of the cancellation to enable the central record on RIPA to be updated.

9.11 What happens if the surveillance has unexpected results?

Those carrying out the covert surveillance should inform the authorising officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

9.12 Errors

Proper application of the RIPA provisions, and robust technical systems, should reduce the scope for making errors. A senior officer within a public authority is required to undertake a regular review of errors and a written record must be made of each review. For the Council, this will be the City Solicitor.

An error may be reported if it is a "relevant error". Under section 231(9) of the Investigatory Powers Act 2016, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.

Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Codes of Practice.

Where a relevant error has been identified, the Council should notify the Investigatory Powers Commissioner (IPCO) as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO). The process for informing IPCO is set out in the relevant Home Office Codes of Practice, which can be found on the intranet.

10. Records and Documentation

10.1 Departmental Records

Applications, renewals cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation, **and destroyed in accordance with the Council's Retention and Disposal Policy.** Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

In relation to communications data, records must be held centrally by the SPoC. These records must be available for inspection by **the IPCO** and retained to allow the Investigatory Powers Tribunal, established under **the IPA 2016**, to carry out its functions.

10.2 Central Record of Authorisations, Renewals, Reviews and Cancellations

A central record of directed surveillance, CHIS and access to communications data authorisations is maintained by:

The City Solicitor
City Solicitor's Division
PO Box 532,
Albert Square
Manchester
M60 2LA

The central record is maintained in accordance with the requirements set out in the Home Office codes of practice. In order to keep the central record up to date authorising officers/designated persons must, in addition to sending through the Home Office application, authorisation form and Magistrates Court order within one week of the authorisation being approved by the Magistrates Court (see **9**.2), send notification (by e-mail) of every renewal, cancellation and review on the Council's notification forms (see **9**.9 – **9**.11).

Using the information on the central record the City Solicitors Division will:

- remind authorising officers/designated persons in advance of the expiry of authorisations;

- remind authorising officers of the need to ensure surveillance does not continue beyond the authorised period;
- remind authorising officers/designated persons to regularly review current authorisations;
- on the anniversary of each authorisation, remind authorising officers/designated persons to consider the destruction of the results of surveillance operations; and
- on the fifth anniversary of each authorisation remind authorising officers/designated persons to consider destruction of the forms of authorisation, renewal, cancellation or review.

10.3 Surveillance products and communications data

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

Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.

Material obtained through the use of directed surveillance, CHIS or acquisition of communications data containing personal information will be protected by **the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)**. **In addition** to the considerations above, material obtained must be used, stored and destroyed in compliance with **any other legal requirements, including confidentiality**, and the Council's Data Protection, Information Security and Records Management Policies available on the intranet at the Protecting Information pages.

11. Training & Advice and Departmental policies, procedures and codes of conduct

11.1 Training & Advice

The City Solicitor will arrange regular training on RIPA. All authorising officers; designated persons and investigating officers should attend at least one session every two years and further sessions as and when required. Training can be arranged on request and requests should be made to the Democratic Services Legal Team. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

The following resources are available on the intranet:

- the Corporate Policy and Procedures;
- Home Office codes of practice on covert surveillance and CHIS;
- Home Office code on acquisition and disclosure of communications data;
- lists of authorising officers and designated persons (posts and names);
- RIPA forms for covert surveillance, CHIS and acquisition and disclosure of communications data;
- the corporate CCTV policy;
- corporate RIPA training;
- request for designation as an authorising officer or designated person;
- Council notifications of RIPA renewal.

If officers have any concerns, they should seek advice on RIPA from the City Solicitor or the Democratic Services Legal Team.

11.2 Departmental policies, procedures and codes of conduct

Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from the City Solicitor or the Democratic Services Legal Team.

12. Complaints

Any person who believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the City Solicitor (as Monitoring Officer) who will investigate the complaint.

They may also complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

13. Monitoring of Authorisations

The City Solicitor is the senior responsible officer in relation to RIPA and is responsible for:

- the integrity of the process in place to authorise directed surveillance, the use of CHIS's and the acquisition and disclosure of communications data
- compliance with Part II of RIPA, **the relevant Home Office Codes of Practice** and this Policy
- engagement with the **Commissioner or Inspectors of the IPCO** when they conduct inspections, and
- where necessary, overseeing the implementation of any post-inspection plans recommended or approved by a Commissioner

The City Solicitor is also required by law to ensure that the Council does not act unlawfully and will undertake audits of files to ensure that RIPA is being complied with and will provide feedback to the authorising officer/designated person where deficiencies in the RIPA process are noted.

To facilitate the City Solicitor's role as the senior responsible officer, the Democratic Services Legal Team will provide a periodic update on use of RIPA powers by the Council.

The City Solicitor will invite members every year through the Executive to review the Council's RIPA Policy for that period and to recommend any changes to the Council's policy or procedures and will also provide members with an annual update on use.

The **IPCO** has a duty to keep under review the exercise and performance of the Council's use of covert directed surveillance, CHIS, and the exercise and performance of the Council's use of its acquisition and disclosure of communications data powers. **The IPCO** will periodically inspect the Council and may carry out spot checks unannounced.