TRAFFORD
COUNCIL

Regulation of Investigatory Powers Act 2000

RIPA POLICY AND PROCEDURE

Contents

1.0 INTRODCUTION 3

2.0 POLICY STATEMENT 4

3.0 ROLES AND RESPONSIBILITIES OF SENIOR MANAGERS, SENIOR AUTHORISING OFFICERS, SENIOR RESPONSIBLE OFFICER AND THE RIPA MONITORING OFFICER. 5

3.2 ROLES 5

3.2.1 Authorising Officer 5

3.2.2 Senior Authorising Officer 5

3.2.3 Senior Responsible Officer 5

3.2.4 RIPA Monitoring Officer 6

3.3 RESPONSIBILITIES 6

3.3.1 Departmental Heads and Managers 6

3.3.2 Authorising Officers 7

3.3.3 RIPA Monitoring Officer 7

3.3.4 Contract Managers 7

4.0 RIPA – GENERAL INFORMATION 8

5.0 WHEN IS RIPA AUTHORISATION AVAILABLE? 9

6.0 WHAT RIPA DOES AND DOES NOT DO 10

7.0 TYPES OF SURVEILLANCE 11

7.1 Generally 11

7.2 Overt Surveillance 11

7.3 Covert Surveillance 11

7.4 Directed Surveillance 12

7.5 Intrusive Surveillance 12

7.6 Covert Human Intelligence Source (CHIS) 13

7.7 Private Information 13

7.8 Social Media 13

7.9 The Authorisation Process 15

7.9.1 Authoring Officers 15

7.9.2 Proportionality 16

7.9.3 Necessity 17

7.10 Examples of different types of Surveillance 17

7.11 Confidential Information 18

7.12. Legally Privileged Information 18

7.13 Collateral Intrusion 19

7.14 Changes in Circumstances and Further Review 20

7.16 Retention and Destruction of Products of Surveillance 20

8.0 Conduct and Use of a Covert Human Intelligence Source (“CHIS”) 21
8.1 Code of Practice 21
8.2 Who is a CHIS? 21
8.3 What must be authorised? 21
8.4 Tasking 22
8.5 Juveniles and Vulnerable Individuals 22
8.6 Test Purchases 23
8.7 Anti-Social Behaviour (Noise, Violence, Racial Abuse etc.) 23
9.0 Acquisition of Communications Data 24
9.1 Communications Data 24
10 Authorisation Process 25
10.1 Overview 25
10.2 Duration and Review of Authorisations 25
10.3 Authorising Officers 26
10.4 Training Records 26
10.5 Grounds for Authorisation 26
10.6 Assessing the Application Form 26
10.7 Additional Safeguards when Authorising a CHIS 28
10.8 Judicial Approval 28
11.0 Working with Other Agencies 31
12.0 Joint Operations 32
13.0 Non-RIPA Authorisations 33
14.0 Record Management 34
14.3 The Central Register 34
14.4 Departmental Records 35
15.0 Reporting 36
16.0 Concluding Remarks 37
Appendix A – Specified Forms 38
Appendix B – Flow Charts 39
Appendix C – Key Personnel 40

1.0 INTRODCUTION

1.1 This policy us the framework on which the Council applies the provisions of the Regulation of Investigatory Powers Act 2000 ("RIPA") as it relates to covert surveillance. Certain covert investigatory powers are available to local authorities under RIPA and the Investigatory Powers Act 2016 ("IPA") which can be used in appropriate circumstances provided that the Council complies with the statutory provisions and the associated Codes of Practice which establish good practice.

1.2 The use of covert surveillance will be a rare occurrence and must only be used where there is no other less intrusive method of obtaining necessary evidence during a criminal investigation.

1.3 The Investigatory Powers Commissioners Office ("IPCO") oversees the use of covert investigatory powers by local authorities.

1.4 This policy should be read in conjunction with the Home Office Covert Surveillance and Property Interference Revised Code of Practice and the Covert Human Intelligence Sources Code of Practice which are available on their web site. The Codes of Practice may be updated and it is the responsibility of all those involved in the use of directed surveillance and the use and management of a CHIS to check the Home Office website regularly to ensure that they are familiar with and apply the current version of those codes of practice.

1.6 The RIPA Monitoring Officer is responsible for keeping this policy and the forms specified for use within it up to date and compliant with the relevant legislation and the codes of practice.

1.7 The RIPA monitoring office will submit reports on the use of the Council's surveillance powers to:

- The Council's Executive Committee on a three monthly basis or as necessary, if the Council has used its powers under RIPA within the proceedings three months, and to:
- The Council's Accounts and Audit Committee annually on this policy and, if relevant, the Councils use of its RIPA powers.

1.8 **Authorising Officers must bring any suggestions for continuous improvement of this policy to the attention of the RIPA Monitoring Officer at the earlies possible opportunity.**

1.9 If there are any amendments to the governing legislation or any of the Home Office Codes of Practice change, this policy will be amended accordingly.

2.0 POLICY STATEMENT

2.1 The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in respect of the sue of its surveillance powers. The RIPA Monitoring Officer has been authorised by the Council to keep this Policy up to date and to amend, delete, substitute relevant provisions as necessary. The Executive Committee will receive a report every three months where the Council has used its surveillance powers during that period or where this policy has been amended during that period. That sets out the type of surveillance carried out, without revealing details of specific operations and, if appropriate, details of any amendments that have been made to this policy. An annual report will be submitted to the Council's Accounts and Audit Committee setting out any amendments to this policy.

2.2 It is the Council's policy that where RIPA applies (see below) surveillance should only be carried out in accordance with this Policy. This Policy covers the use of directed surveillance, intrusive surveillance and the deployment of Covert Human Intelligence Sources by the Council. These types of surveillance are described in greater detail within section 7 of this policy.

2.3 Where RIPA does not apply, surveillance may be properly carried out provided that the appropriate rules and procedures are followed. For example' surveillance connected with an employment issue will have to be carried out in accordance the General Data Protection Regulations (GDPR) and the Councils policies. The Council has adopted a Non-RIPA Authorisation policy which Officers must follow for surveillance which falls outside of RIPA. Advice on non-RIPA surveillance may be sought from Authorising Officers, the RIPA Monitoring Officer or the Council's legal services department.

3.0 ROLES AND RESPONSIBILITIES OF SENIOR MANAGERS, SENIOR AUTHORISING OFFICERS, SENIOR RESPONSIBLE OFFICER AND THE RIPA MONITORING OFFICER.

3.1 This section sets out the various roles and responsibilities in relation to the use of RIPA. It is essential that senior managers and authorising officers take personal responsibility for the effective and efficient use of this Policy and the implementation of RIPA within their departments.

3.2 ROLES

3.2.1 Authorising Officer

3.2.1.1 An Authorising Officer is a person who considers whether or not to grant an application to use directed surveillance. The Authorising Officer must believe that that the activities to be authorised are necessary for the purposes of preventing or detecting crime and that they are proportionate to what is sought to be achieved by carrying them out. Their authorisation is subject to judicial approval.

3.2.1.2 **An Authorising Officer may not, except in the case of urgency, consider an application to use directed surveillance if the Applying Officer is an officer within their service area or if the Authorising Officer has direct involvement in the investigation to which the application relates.**

3.2.2 Senior Authorising Officer

3.2.2.1 A Senior Authorising Officer is a person responsible for considering whether or not to grant an authorisation where confidential information is likely to be obtained or for use of a CHIS

3.2.3 Senior Responsible Officer

3.2.3.1 The Senior Responsible Officer has overall responsibility for the use and operation of RIPA with the Council and oversees the competence of Authorising Officers and the processes used in the Council. The Senior Responsible Officer is not an Authorising Officer as it would be inappropriate for a Responsible Officer to review their own decisions. The Senior Officer will be a member of the Council's Management Team.

3.2.3.2 The Senior Responsible Officer is responsible for:

- The integrity of the processes in place within the Council for the management of CHIS and directed surveillance;
- Compliance with the statutory provisions and Codes of Practice;
- Training or arranging training for Authorising Officers, together with the RIPA Monitoring Officer;
- Ensuring Officers understand the provisions relating to covert surveillance and Covert Human Intelligence Sources;
- Engaging with the IPCO Inspectors when they conduct their inspections;
- Ensuring that all Authorising Officers are sufficiently competent in the light of any post inspection report;

- Addressing any concerns within an IPCO inspection report, and;
- Overseeing the implementation of any post-inspections action plans.

3.2.4 RIPA Monitoring Officer

3.2.4.1 The RIPA Monitoring Officer has:

- The duty to maintain the list of Authorising Officers;
- The power to suspend from the list of Authorising Officers any Authorising Officer who does not follow the procedure set out within this policy or who does not attend any training sessions; and
- The power to cancel any authorisation that is manifestly wrong.

3.3 RESPONSIBILITIES

3.3.1 Departmental Heads and Managers

3.3.1.1 Department Heads and Managers are responsible for:

- Identifying team members who conduct investigations which may involve the use of directed surveillance or the use of Covert Human Information Sources;
- Ensuring that those team members are aware of the requirements of this policy and that they do not conduct any form of surveillance governed by RIPA without obtaining the necessary authorisation;
- That those officers understand that a deliberate failure to comply with the requirements of this policy will be regarded by the Council as gross misconduct;, and;
- That those officers are properly trained as Applying Officers.

3.3.1.2 Department Heads and Managers must consider whether or not a proposed investigation present any risk of the acquisition of confidential information which may affect the admissibility of the evidence in any subsequent proceedings. Where there is a risk that confidential information may be acquired during the course of the investigation the application must be considered by a Senior Authorising Officer.

3.3.1.3 Prior to making an application for authorisation, Department Heads and Managers must consider how any information or material obtained during the course of the investigation will be retained and disposed of and implement those arrangements.

3.3.1.4 All Department Heads, Managers, and Authorising Officers must pay particular attention to the health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances should Department Heads, Managers or Authorising Officers permit an application to be made unless and until they are satisfied that a risk assessment has been undertake to assess the risks involved in undertaking the surveillance has been identified and have been addressed or minimised to the extent necessary to be proportionate to the value of the surveillance being undertaken. A risk assessment template is available within Appendix A which should be completed by the applying officer.

3.3.1.5 **If a Department Head, Manager, or Authorising Officers is any doubt as to the health and safety risks involved or the proportionality of the value of the proposed surveillance, they should seek the advice of the RIPA Monitoring Officer.**

3.3.2 Authorising Officers

3.3.2.1 Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office. A failure to consider and apply the Codes of Practice when considering an application for RIPA authorised surveillance exposes the Council to unnecessary legal risk, criticism from IPCO and the risk that authorisation will be declined by the court.

3.3.2.2 The risk that confidential information will be acquired during the course of the surveillance must be considered before an application is made and during the authorisation. **If there is a risk that confidential material will be discovered during the course of the surveillance, the application must be considered by a Senior Authorising Officer.** Additional consideration must be given as to how any material discovered during the course of the surveillance shall be retained and disposed of.

3.3.2.3 Authorising Officers must give appropriate consideration to the **necessity and proportionality** provisions when authorising applications. An Authorising Officer must give bespoke written reasons for granting an application avoiding the use of stock phrases which might create the impression that insufficient consideration had been given to the application and the particular circumstances of the subject of the surveillance.

3.3.2.4 Authorising Officers are also responsible for ensuring that any equipment which is to be used during the course of surveillance is properly identified, controlled, stored and maintained for the purposes of audit.

3.3.3 RIPA Monitoring Officer

3.3.3.1 The RIPA Monitoring Officer is responsible for maintaining, updating and enforcing this Policy. In conjunction with the Senior Responsible Officer, the RIPA Monitoring Officer is responsible for ensuring that all Applying and Authorising Officers have received appropriate training and that no Authorising Officer authorises any application in the absence of having completed that training.

3.3.3.1 The RIPA Monitoring Officer shall also ensure that adequate records are maintained in accordance with the relevant Codes of Practice and to ensure that reviews are conducted in a timely manner. The RIPA Monitoring Officer must ensure that all cancellations and renewals are affected before the authorisation cease to have effect.

3.3.4 Contract Managers

3.3.4.1 Contract managers are responsible for ensuring that any Agency employed by the Council is aware of this policy and the need to apply to the Council's Authorising Officers for authorisation of any directed surveillance or other RIPA regulated activity they propose to conduct on behalf of the Council.

4.0 RIPA – GENERAL INFORMATION

4.1 Trafford Council has a statutory obligation pursuant to the Human Rights Act 1998 to ensure that it does not act in manner which is incompatible with a right given within the European Convention on Human Rights.

4.2 Article 8 of the Convention prohibits interference with a person's home, private and family life save and accept in accordance with the law where such interference is necessary in the interests of national security, public safety, the economic well-being of the country, for the prevention of crime and disorder, for the protection of health or morals or for the protection of the freedom of others.

4.3 RIPA provides a statutory mechanism where what would otherwise be an unlawful interference with a person's Article 8 rights provided that the interference is **necessary and proportionate**. RIPA is therefore intended to balance public interest and the human rights of an individual.

4.4 All directly employed staff, agents and agencies working for the Council must comply with the requirements of RIPA. Therefore, if an external agency is to carry out any form of directed surveillance during the court of their work with the Council they must be properly authorised to undertake that work by one of the Council's Authorising Officers.

4.5 If the correct procedures are not followed:

- The court's may disallow any evidence discovered during the course of the investigation;
- A complaint of maladministration may be made to the Ombudsman;
- The Council may be the subject of an adverse report by the IPCO;
- The Council may be exposed to an action for damages and/or injunctive relief by any person who contends that their Human Rights have been unlawfully breached.

4.6 A failure to observe the correct procedures is also likely to result in adverse media attention which will damage the Council's reputation and the trust the inhabitants of Trafford place in it.

4.7 The procedure for authorisation is described in greater detail within the following sections of this policy and is summarised in the flow charts within Appendix B

5.0 WHEN IS RIPA AUTHORISATION AVAILABLE?

5.1 RIPA authorisation is only available for surveillance which relates to the prevention and detection of crime which is a “core function” of the Council.

5.2 A “core function” is defined as a “specific public function” which is distinct from its “ordinary functions”. “Ordinary function” are by contrast anything any public authority carries out, such as the entering into contractual arrangements for the supply of goods or services or the employment of staff.

5.3 Where the Council seeks to carry out surveillance which is not related to the prevention or detection of crime, but which is related to one of its other ordinary functions, that surveillance is not regulated by RIPA. As a matter of good practice, the Council has devised a policy for the authorisation of surveillance which is not regulated by RIPA which is set out in section 13 of this policy.

5.4 Any internal authorisation for directed surveillance or the use of a CHIS will not become effective until judicial approval has been obtained from the Manchester magistrates’ court. Under no circumstances can any form of RIPA regulated surveillance or use of CHIS commence until judicial approval has been obtained. The magistrates’ court will only grant approval where a district judge or justice of the peace is satisfied that all the statutory criterion have been met and that the surveillance is necessary and proportionate. Further details of the process for obtaining judicial approval are set out in section 10.8 of this policy.

6.0 WHAT RIPA DOES AND DOES NOT DO

6.1 RIPA and the policies and procedures the Council has adopted to ensure it is correctly implemented and applied, are intended to ensure that a proper balance is maintained between the public interest in conducting appropriate investigations to prevent and detect crime with the human rights of those who are to be subjected to surveillance.

6.2 **RIPA does**:

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

6.3 **RIPA does not**:

- Make anything unlawful which is otherwise lawful;
- Make anything lawful which is otherwise unlawful;
- Prejudice or dis-apply any existing power available to the Council to obtain information, such as for example the power to request and obtain information from the DVLA or HM Land Registry as to the ownership of land or vehicles.

6.4 Where any officer within the Council has any doubt or concern as to whether an activity or enquiry they have been asked to carry out requires authorisation under RIPA or the Council's policy on non-RIPA surveillance, they should seek the advice of an authorising officer before beginning to carry out that task.

7.0 TYPES OF SURVEILLANCE

7.1 Generally

7.1.2 "Surveillance" is defined within RIPA so as to include:

- 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
- the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if, and only if:
    - the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to him; and;
    - there is no interception warrant authorising the interception.

7.1.3 Surveillance may be "overt" or "covert" in nature.

7.2 Overt Surveillance

7.2.1 Overt surveillance is surveillance which is not conducted openly and not clandestinely or secretly or through the use of hidden officers or equipment.

7.2.3 Most of the surveillance undertaken by the Council will be overt.

7.2.4 Examples of overt surveillance include:

- The activities and observations of uniformed street wardens;
- The monitoring of noise nuisance where the alleged perpetrator has been informed the noise monitoring will be carried out;
- Most test purchases;
- Visits and inspection by licensing officers to establish that a licensee is abiding by their licensing conditions in circumstances where the licensee has been warned that unannounced tests will be undertaken.

7.3 Covert Surveillance

7.3.1 RIPA regulates two types of covert surveillance, directed surveillance and the use of a covert human intelligence source (CHIS).

7.3.2 Surveillance is defined by RIPA as being covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

7.3.3 Where the activity relates to the use of a CHIS the activity is defined as being covert by RIPA where:

- The CHIS has a relationship which conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose; and
- The relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

7.3.4 Covert surveillance must not be used if there is a reasonably available overt method of obtaining the required information. However, if the use of the only available overt means of surveillance is likely to seriously undermine the purposes of the investigation or to place innocent persons at risk, the use of covert surveillance may be authorised.

7.4 Directed Surveillance

7.4.1 "Directed Surveillance" is surveillance which:

- Is covert but not intrusive surveillance;
- Is conducted for the purposes of a specific investigation or operation;
- Is likely to result in private information being obtained about any person (whether the subject of the investigation or anyone else);
- Is not an immediate response to events or circumstances where it would not be reasonably practicable seek authorisation under the Act, for example where an assault is witnessed on CCTV and the assailant is tracked by CCTV operators until they are detained by the police.

7.5 Intrusive Surveillance

The Council cannot use or authorise intrusive surveillance under RIPA or use it powers to interfere with private property. The Act reserves the use of intrusive surveillance to the police and other authorised government agencies

7.5.1 Intrusive surveillance is surveillance which:

- Is covert;
- Relates to residential premises and/or private vehicles
- Involves the presence of an investigator or similar person in the premises or private vehicle;
- Involves the presence of a surveillance device in the premises or private vehicle.

7.5.2 "Residential premises" means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used).

7.5.3 "Private vehicle" means any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it.

7.5.3 Surveillance will always be intrusive where it is conducted:

- In any part of any premises being used for the purposes of any legal consultation, for example any room on Council premises being used by a legal advisor and their client for the purposes of a private legal consultation, before, during or after an interview under caution.
- In any prison, remand or detention centre.
- In a police station;
- At the place of business of any professional legal adviser, or:

- At any court house or other place being used for the sittings of a court or tribunal.

7.5.4 Where surveillance is conducted through the use of a surveillance device that is situated on the outside of residential premises or a private vehicle, it is unlikely to be regarded as intrusive unless the device consistently provides information and detail that would be of the same quality as if the device were mounted within the premises.

7.6 Covert Human Intelligence Source (CHIS)

7.6.1 A person must be regarded as a CHIS if they establish or maintain a personal or other relationship with a person for the covert purpose of enabling them to:

- covertly use that relationship to obtain information or to provide access to any information to another person; or
- covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

7.7 Private Information

7.7.1 “Private Information” is any information that relates to a person’s family or private life and includes any aspect of a person’s private or personal relationships with others. Relevant person relationships include their business, family and social relationships.

7.7.2 The fact that covert surveillance takes place in business premises or a public place does not mean that private information will not be obtained during the surveillance. There will always be a risk of obtaining private information whenever prolonged directed surveillance is targeted at a specific individual because that surveillance will identify person the subject comes into contact with.

7.7.3 For example, although the routine use of street CCTV systems will not require the authorisation, authorisation will be required where the cameras are to be directed at a particular person for a specific person. That process is bound to reveal details of whom the subject meets and how they go about their business. That information will include information that meets the definition of private information.

7.8 Social Media

7.8.1 “Social Media” is not defined by RIPA which pre-dates the evolution of social media.

7.8.2 For the purposes of this Policy “social media” means any website or application that enables users to create and share content or to participate in social networking”. It includes, but is not limited to websites and applications known as “Facebook”, “YouTube”, “WhatsApp”, “Instagarm”, “WeChat” and “TikTok” as new social media applications are constantly being launched, merged and withdrawn.

7.8.3 Social media can provide useful information as part of an investigation, however investigators and authorising officers must consider whether their specific and

intended use of social media during an investigation is likely to require authorisation under RIPA.

7.8.4 In general terms, authorisation is unlikely to be necessary where an initial search of social media is made to establish a fact or to collate an intelligence picture.

7.8.5 Authorisation is likely to be required where:

- There is to be a repeated and systematic viewing and monitoring of a person's social media account – for example repeatedly viewing a Facebook account where a record of information is kept for use in the investigation;
- Where a "friend request" has to be made and accepted to enable the investigator to view information that would otherwise be unavailable;
- Where the examination of a person's social media account is likely to reveal "private information";
- Any other activity which is likely to result in a repeated and systematic collection of personal information.

7.8.6 Where the owner of a Social Media account has consented to access to the account the investigating officer must still consider whether there is a risk that by accessing the account they will come across private information relating to other persons who have not given their consent to that information being acquired. In such circumstances, if there is a likelihood private information of others will be obtained during the investigation, an application for directed surveillance must be made.

7.8.7 Most social media platforms enable the user to set privacy setting to govern who may access their personal information. Where privacy settings are available but not applied, the material on display may reasonably be regarded as being open source so that authorisation is not required. However care must be taken to understand how each social media platform operates and what privacy settings are and are not available, before regarding material as being open source material.

7.8.8 Care must also be taken into the interception and use of direct or instant messages, which may be regarded as being private communications still in provision.

7.8.9 If it is deemed necessary and proportionate to covertly breach any access controls to gain access to information on social media, RIPA authorisation must be sought for directed surveillance.

7.8.10 Where it is intended to gain access to material on a social media platform by the use of a friend request which will on its face establish a relationship between the investigator and the social media account holder an application for authorisation of a CHIS must be sought.

7.8.11 It is not unlawful for an investigator to set up a false persona for use during an investigation, but where that is done for the purposes of undertaking covert surveillance RIPA authorisation must be sought. The use of photographs depicting other persons without their consent in order to support a false identity infringes other laws and must not be used.

7.8.12 When considering whether authorisation is required investigators and authorised officers should consider whether any of the following criterion apply. If any one of them does apply authorisation must be sought:

- Whether the investigation or research is directed towards a specific individual or organisation;
- Whether it is likely to result in obtaining private information about any individual(s);
- Whether it is likely to involve visiting websites or social media platforms to build up an intelligence picture profile;
- Whether the information will be recorded and retained;
- Whether the information is likely to reveal a person's lifestyle;
- Whether the information, on its own or combined with other information or intelligence amounts to information concerning a person's private life;
- Whether the investigation or research is part of an ongoing piece of work resulting in repeated viewing of the subject's social media platform(s);
- Whether the investigation or research is likely to involve identifying and recording information about third parties, including but not limited to the subject's family members or friends or information posted on the social media platform by third parties.

7.8.13 To avoid the potential for inadvertent use of social media platforms in investigative and enforcement roles investigators should:

- Not create a false identity to befriend individuals on social media platforms without obtaining RIPA authorisation:
- When viewing a person's public profile on a social network should only do so to the minimum extent necessary and proportionate to support or refute an allegation;
- Not repeatedly view a person's profile or social media platform to gather evidence or acquire information about an individual's status without RIPA authorisation;
- Be aware that information published on social media platforms may not be true, accurate or reliable. Where it is intended to use that information as evidence all reasonable steps should be taken to verify its reliability.

7.9 The Authorisation Process

7.9.1 Authoring Officers

7.9.1.1 Only those officers who have been designated, trained and appointed as Authorising Officers for the purposes of RIPA can authorise directed surveillance. They can only do so if and only if the policies and procedures set out within this policy have been followed and where:

- The purpose of the investigation of for the prevention an detection of crime, and:
- The offence under investigation is punishable by six months imprisonment or more, or it is an offence contrary to the Licensing Act 2003, sections 146, 147 and 147A or the Children and Young Persons Act 1933, section 7, and:

- Where the Authorising Officer is satisfied that it is necessary and proportionate to approve the application.

7.9.1.2 Even if an Authorising Officer approves an application, the authorisation will not become effective until judicial approval has been obtained. Under no circumstances must any directed surveillance be commenced until judicial approval has been granted.

7.9.1.3 The Home Office Codes of Practice provide guidance on the use of covert surveillance and must be consulted.

7.9.1.4 If an authorised officer is any doubt whether the use of covert surveillance is appropriate within the criminal investigation that is being conducted they should seek the advice of the Council's legal services department before making their decision.

7.9.2 Proportionality

7.9.2.1 The authorisation of covert surveillance will only be proportionate if the authorised surveillance is capable of achieving the expected benefit within the investigation with the minimum possible level of intrusiveness. In other words, the covert surveillance will not be proportionate if the same benefit to the investigation could be achieved using covert methods of surveillance or less intrusive methods of covert surveillance.

7.9.2.2 When considering whether or not to authorise covert surveillance, an authorising officer should:

- Balance the size and scope of the proposed activity against the gravity and extent of the offence under investigation;
- Be able to explain, within their authorisation, why the authorised methods of covert surveillance are the least intrusive methods of surveillance available to achieved the expected benefits of the surveillance;
- Be able to evidence what other methods of investigation were considered as an appropriate to the authorised covert surveillance, and:
- Be able to explain why they consider that the authorised surveillance is capable of being authorised under the legislative regime and the standards of good practice.

7.9.2.3 In summary, the authorising officer must ensure that they are not being asked to use a sledgehammer to crack a nut but are instead authorising the minimum level of covert surveillance possible to meet the needs of the investigation. This requires the authorising officer to have regard to the level of intrusiveness likely to be caused by the covert surveillance and balancing the rights of the suspect anyone else who is likely to be impacted by the investigation with the gravity of the matter under investigation.

7.9.2.4 The issue of whether the use of covert surveillance is proportionate is fact specific and will differ in every investigation and application for authorisation presented to an authorising officer. Authorising officer must give individual fact specific reasons for their decision in each case, and when doing so should avoid the use of generic phrases and statements which may imply that necessary level of objectivity was not applied in any particular decision.

7.9.3 Necessity

7.9.3.1 In addition to being “proportionate” the use of covert surveillance must be “necessary” in all the circumstances.

7.9.3.2 In considering whether the use of covert surveillance is “necessary” the authorising officer must consider whether:

- The evidence which is expected to be obtained via covert surveillance is evidence that is required to prove the offence under investigation;
- Whether that or other sufficient evidence is already on the possession of the investigator, and;
- Whether the evidence is available from some other source or could be obtained by other less intrusive means.

7.9.3.3 The issue of whether the use of covert surveillance is necessary is fact specific and will differ in every investigation and application for authorisation presented to an authorising officer. Authorising officer must give individual fact specific reasons for their decision in each case, and when doing so should avoid the use of generic phrases and statements which may imply that necessary level of objectivity was not applied in any particular decision.

7.10 Examples of different types of Surveillance

7.10.1 It is not possible within this policy to list every type of surveillance activity that might be proposed within an investigation and to categorise that activity. What follows is a list of generic examples of different types of investigative activity. If an authorising officer has any doubts whether an activity is covert and therefore requires authorisation they should have regard to the examples within the Codes of Practice or seek the advice of the Council’s legal serves department.

7.10.2 Table of Examples

Type	Examples
OVERT	• Patrolling enforcement officer • Recording noise from outside premises creating noise • Most test purchases where the investigator behaves no different from a member of the public
OVERT (but regulated by other legislation outside the scope of RIPA)	• Town Centre CCTV systems in normal use • ANPR cameras used for enforcing road traffic offences • CCTV systems operated by local authorities in public places.
COVERT (not requiring prior authorisation under RIPA)	• CCTV cameras providing general traffic, crime or public safety information.
DIRECTED SURVEILLANCE (requiring authorisation under RIPA)	• Officers maintaining observations on a subject over a period to establish whether the subject is working whilst claiming to be unfit for work;

	• Repeated visits to a suspects social media platforms to establish their involvement in an offence; • Test purchases with the use of a concealed camera and/or audio device where there is a risk of private information being gathered about the suspect.
INTRUSIVE SURVEILANCE or INTERFERENCE WITH PRIVATE PROPERTY (which requires authorisation under RIPA but cannot be authorised or used by a local authority).	• Use of surveillance device inside a suspects home, private vehicle or private business premises; • Using a surveillance device outside a suspects home, vehicle or private business address which is capable of recording and retaining the same level of material as if the device was planted inside those premises.

7.10.3 The Council maintains separate codes of practice in relation to its town centre CCTV system and its other Camera surveillance systems in use across its estates. Investigation Officers and Monitoring Officers must ensure that they are familiar with those systems and the codes of practice and rules that apply to them.

7.11 Confidential Information

7.11.1 "Confidential information" includes material which may contain information which is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. It also includes material within a person's medical records, their communications with their doctors, medical professionals and spiritual advisors.

7.11.2 Further guidance as to what amounts to confidential information is set out with section 9 of the Code of Practice.

7.11.3 Where an investigating officer or an Authorising Officer considers that there is a risk that confidential information will be obtained during authorised directed surveillance, the application must be referred to and can only be granted by a Senior Authorising Officer.

7.12. Legally Privileged Information

7.12.1 Directed surveillance which is intended to result in the acquisition of legally privileged information cannot be authorised.

7.12.2 Where the proposed surveillance creates a risk that legally privileged information will be obtained investigators must draw the risk that such material is likely to be obtained within their application, which must be referred to a Senior Authorising Officer.

7.12.3 Where a Senior Authorising Officer is presented with an application for authorisation of directed surveillance that carries a risk that legally privileged

information may be acquired, the Senior Authorising Officer will only grant that application where:

- The application is for the purposes of preventing or detecting serious crime. Serious crime is defined in sections 81(2) and (3) of RIPA as crime that comprises an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose;

- The level of risk that legally privileged information is likely to obtained, the greater risk making it less likely that it would be proportionate to authorise the surveillance;

- All other relevant circumstances, including whether the investigation should be referred to the police or other statutory enforcement agency having regard to the seriousness of the allegation and greater resources available to the police and other enforcement authorities.

7.12.4 When assessing whether an offence amounts to "serious crime" guidance as to the likely sentence can be obtained can be obtained from the Sentencing Council.

7.13 Collateral Intrusion

7.13.1 "Collateral Intrusion" refers to the acquisition of someone other than the subject of the surveillance during the course of the investigation. For example it would include circumstances where during the course of observations being made on a suspect, details of the comings, goings and lifestyle of the suspect's family members was obtained, or where during the examination of a suspects social media accounts, personal information about the identity and lifestyles of their social media "friends" was obtained.

7.13.2 Investigating Officers must identify the risk of any collateral intrusion within their application for authorisation. For example, where it is intended to carry our directed surveillance of a suspect at their home address, the Investigating Officer should set out whether the suspect is believed to live alone or with other family members and / or house mates who may be the subject of collateral intrusion.

7.13.3 When considering whether or not to grant an application Authorising Officers must consider whether:

- Whether the risk of collateral intrusion is proportionate to the expected benefits of the investigation;
- What steps can be taken to eradicate or minimise those risk, and:
- If a risk remains what steps can be taken to ensure that any third party is protected from any adverse consequence from the acquisition of confidential information about them, for example by ensuring that material is not retained.

7.14 Changes in Circumstances and Further Review

7.14.1 If there is any material change in circumstances whilst an Investigating Officers is undertaking directed surveillance that change in circumstances must be reported to the Authorising Officer who approved the application, or in their absence another Authorising Officer of equivalent rank in order that the authorisation can be reviewed.

7.14.2 A “material change in circumstances” includes, but is not limited to:

- Any change in the level of risk relating to the personal safety of the officer(s) conducting the investigation or to any other person likely to be affected by the ongoing investigation;
- Any occasion where confidential information is unexpectedly acquired;
- Any occasion where legally privileged information is acquired;
- Any occasion where private information of someone other than the subject of the surveillance is acquired;
- When the investigation is ended during the period of authorised surveillance or where conduct of the investigation is assumed by another investigative body, such as the police.

7.14.3 Where a change of circumstances is reported to an Authorising Officer they will re-consider the application, applying the same criterion that applied to the initial application but taking account of the new information that is available.

7.15.4 Where the result of the Authorising Officer results in the scope of the authorisation being expanded, further judicial approval will be required.

7.16 Retention and Destruction of Products of Surveillance

7.16.1 The Criminal Procedure and Investigation Act 1985 (“CPIA”) and the Code of Practice made under the provisions of that Act makes provision about the retention, storage and disclosure of evidence acquired during criminal investigations and its use during criminal proceedings. Investigating Officers and Authorising Officers must ensure that appropriate arrangements are in place for the recording, retention, storage and disclose of all relevant material during the course of their investigation and throughout.

7.16.2 Investigating Officers and Authorising Officers must also ensure that any material gathered during their investigation are securely destroyed in accordance with the provisions of the CPIA and its Code of Practice when the retention of that information is no longer required.

7.16.3 RIPA does not prevent material that was obtained during an investigation, which is relevant material in respect of another investigation, but Investigating Officers and Authorising Officers must ensure that any disclosure to another investigating officer or prosecuting authority is appropriately authorised and compliant with all data protection legislation.

8.0 Conduct and Use of a Covert Human Intelligence Source ("CHIS")

8.1 Code of Practice

8.1.1 The Home Office has published a separate Code of Practice relating to Covert Human Intelligence Sources which provides additional guidance and which must be regularly consulted by Investigating Officers and Authorising Officers to ensure they are familiar with it.

8.1.2 That code of practice must be read in conjunction with the Code of Practice relating to Covert Surveillance and Property Inference and the other statutory material referred to in this policy.

8.2 Who is a CHIS?

8.2.1 A CHIS is a person who establishes or maintains a personal or other relationship for the covert purpose of using that relationship to obtain information during the course of an investigation. Examples include investigators developing a relationship with a member of a protest group to discover information about their intended protests, or an investigator who initiates a "friend request" on social media in order to maintain a relationship to enable them to gather information from a social media account.

8.2.3 The definition of a CHIS does not extend to a member of the public who volunteer's information to the Council on a single occasion. However, where such a person makes repeated disclosures to the Council about the same or separate subjects, serious consideration should be given as to whether that person has become a CHIS so that their activities must be authorised. It follows that it is possible that a person will become a CHIS even though they have not been approached or encouraged to act in that capacity.

8.2.4 Similarly, most tests purchases will not involve and investigator becoming a CHIS provided that they do not develop or maintain a personal relationship with the subject of the investigation.

8.3 What must be authorised?

8.3.1 The conduct or use of a CHIS requires prior authorisation in accordance with the procedures set out within this policy.

- "Conduct of a CHIS" means establishing or maintaining a personal or other relationship with a person for the covert purpose of (or which is incidental to) the acquisition and passing of information.

- "Use of a CHIS" means any actions which include asking or assisting a person to act as a CHIS in the first place.

8.3.2 Most authorisations will require authorisation of both conduct and use on the grounds that it is likely that the Council will take proactive action in response to information acquired by the CHIS which may include "tasking" the CHIS to obtain specific information which is to be reported to the Council.

8.3.3 Detailed records must be kept in relation to each and every CHIS.

8.3.4 Authorisations to use a CHIS may only be granted by a Senior Authorising Officer and will require judicial approval. The person responsible for the day to day management of a CHIS or the oversight of the CHIS must be appointed by the Senior Responsible Person.

8.3.5 A Senior Authorising may only authorise the use of a CHIS, if and only if authorisation is sought for the prevention and direction of crime and if and only if the procedures set out within this policy have been followed.

8.3.5 Before a person is authorised as a CHIS a full and comprehensive risk assessment must be carried out which identifies any and all potential risks to the CHIS and anyone connected with them which arise as a result of activities of the CHIS. The welfare and security of the CHIS whilst undertaking their role and afterwards must be a matter of paramount importance when determining whether to grant authorisation of a CHIS.

8.4 Tasking

8.4.1 "Tasking" is an assignment given to a CHIS by regulation of investigatory powers by a person within the Council who has day to day responsibility for managing that source of information and who has responsibility for the source's security and welfare or some other person within the Council who has responsibility for the general oversight of that source.

8.4.2 Where ever a CHIS is to be authorised the Senior Responsible Officer must appoint an officer within the Council to:

- have responsibility for the day to day management of CHIS, or
- to oversee the day today management of a CHIS.

8.4.3 The persons appointed by the Senior Responsible Officer for the day to day management of a CHIS will have responsibility for:

- Dealing with the CHIS on a day to day basis;
- Directing the Directing the day to day activities of the CHIS;
- Monitoring the welfare and security of the CHIS, and:
- Recording the information by the CHIS.

8.4.2 The person appointed to have general oversight of the CHIS has the responsibility for overseeing the role of the CHIS and making relevant decisions where the person who has responsibility for the CHIS is not available.

8.4.3 A person must be authorised as a CHIS before they are assigned to any specific task that it is intended to provide information that is relevant to any investigation.

8.5 Juveniles and Vulnerable Individuals

8.5.1 Special safeguards apply to the use of juvenile sources. A "juvenile source" refers to any person under the age of 18 years. Under no circumstances may any person under 16 be authorised to provide information against their parents.

8.5.2 A "vulnerable person" is a person who is a person aged 18 or over who may need community care services because of a disability (mental or other), age, or illness. They may also be considered to be vulnerable if they are unable to look after

themselves, protect themselves from harm or exploitation or are unable to report abuse.

8.5.3 Where there are any grounds to suspect that a person may be vulnerable, they should be regarded as being vulnerable unless there is compelling evidence to the contrary.

8.5.4 Vulnerable individuals and juveniles will only be authorised to act as CHIS in exceptional circumstances and authorisation may only be granted for the use of such persons as a CHIS by a Senior Authorising Officer.

8.6 Test Purchases

8.6.1 Carrying out test purchases does not usually require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and therefore the purchaser will not normally be a CHIS.

8.6.2 Where it is proposed to deploy the use of a mobile hidden recording devices or CCTV devices to record what takes place within the shop during the test purchase an authorisation for directed surveillance will be required which may be combined with authorisation for the use of a CHIS.

8.7 Anti-Social Behaviour (Noise, Violence, Racial Abuse etc.)

8.7.1 Where persons who complain about anti-social behaviour and are asked to maintain a diary they will not normally need to be regarded as a CHIS because the act of maintaining a diary does not require the establishment or maintenance of a personal relationship and will not usually require authorisation.

8.7.2 Where a record of noise is made which only measures the volume of that noise rather than a recording which can be played back to identify speech or music, no private information will be captured and therefore authorisation is not required.

8.7.3 Where a recording of noise is made with a recorder placed on private premises which is capable of playing back any captured conversation could constitute intrusive surveillance which cannot be authorised by the Council, unless it is done covertly, where for example written notice has been given to the subject that such recordings are to be made.

8.7.4 Recordings of noise made from outside any premises of speech that can be heard in the street or other public place are unlikely to require authorisation as by permitting that noise to be audible in the street, the subject is likely to have forfeited any reasonable expectation of privacy.

8.7.5 Placing covert mobile or stationary video devices on any residential estate for the purposes of detecting crime or disorder will require prior authorisation as such procedures amount to directed surveillance.

9.0 Acquisition of Communications Data

9.1 Communications Data

9.1.1 “Communications data” means any traffic or information that is or has been sent by or over a telecommunications system or through the postal system, together with data that is captured about a person’s use of those systems.

9.1.2 The Communications Act 2003 defines telecommunications networks widely so that it includes services transmitted over the telephone line system, over a mobile network such as Vodafone or O², via the internet through an internet service provider and by VOIP (voice over internet protocol). It follows that the definition of communications data is wide enough to include messages and other material shared by social media applications, text messaging services and the internet.

9.1.3 Section 60A of the Investigatory Powers Act 2016 provides a procedure whereby a local authority may apply to the Investigatory Powers Commissioner for authorisation to obtain communications data. That application process is outside the scope of this policy and where it is proposed to make such an application, the request must be directed to the RIPA Monitoring Officer.

10 Authorisation Process

10.1 Overview

10.1.1 Directed Surveillance and the use of a CHIS may only take place after the authorisation process specified within this police have been complied with and after judicial approval has been granted.

10.1.2 There are two stages to the authorisation process:

- Internal authorisation by an Authorised Officer
- Judicial approval.

10.1.3 The forms that must be used during the application and authorisation process are shown at Appendix A

10.1.4 A flow chart of the application process is shown at Appendix B

10.2 Duration and Review of Authorisations

10.2.1 Any authorisation granted in respect of directed surveillance will last for a period of three months from the date upon which judicial approval was granted, unless extended upon application.

10.2.2 Any authorisation granted in respect of the development or maintenance of a CHIS will last for a period of:

- Four months from the date upon which judicial approval was granted, where the application relates to an authorisation in respect of a juvenile or vulnerable person, or:
- Twelve months in relation to a CHIS in any other circumstances.

10.2.3 Where an authorisation ceases to be required during its operational period, the Investigating Officer is responsible for making application to the Authorising Officer for the authorisation to be cancelled.

10.2.4 Where an Investigating Officer believes that the authorisation needs to be extended beyond the initial period, the Investigating Officer must apply for an extension of the authorisation to the Authorising Officer at least 10 working days before the authorisation will expire to allow sufficient time for the application to be considered and for judicial approval to be obtained for that extension.

10.2.5 Where an Authorising Officer receives an application for renewal, they must consider the matter afresh applying the criterion set out within this policy and taking account of the effectiveness or otherwise of the activity to date and any unexpected risks that have arisen during the course of the investigation.

10.2.6 Where the period during which an authorised activity may take place has expired, the authorisation cannot be renewed. In such circumstances a fresh application must be made.

10.2.7 Whenever an authorised activity is not used, or no longer required, the authorisation will not cease to be valid until it has been reviewed and cancelled by an Authorising Officer. Until an authorisation has been cancelled, the activity must be reviewed in accordance with this policy and upon review an Authorising Officer

should consider whether in the absence of use of the activity the authorisation should be cancelled.

10.3 Authorising Officers

10.3.1 Only those persons who have been appropriately trained and appointed as authorised officers and whose details appear on the central register are entitled to consider and determine authorisations.

10.3.2 Authorisation is particular to the named individual, not their post. Therefore, in the event that an authorised officer leaves the Council's employment, their immediate successor will not acquire the position of an authorised officer.

10.3.3 The RIPA Monitoring Officer has the power to appoint or dismiss Authorised Officers and is responsible for maintaining the register of Authorised Officers.

10.4 Training Records

10.4.1 All Council staff engaged in the application, authorisation and management of covert activity will receive induction and refresher training in respect of all aspects of directed surveillance and the establishment and control of a CHIS. Training will also be delivered as required to all relevant officers to address any changes in the law, guidance or good practice.

10.4.2 Periodic testing will be undertaken to establish levels of competence and to identify training needs.

10.4.3 The RIPA Monitoring Officer will keep a record of the trainings received by relevant officers in conjunction with HR.

10.5 Grounds for Authorisation

10.5.1 The only power available to authorise directed surveillance or the use of a CHIS which is available to the Council is for the purposes of preventing or detecting crime. An application which cites any other statutory cause must be refused.

10.6 Assessing the Application Form

10.6.1 An Authorising Officer must reject any incomplete or inadequately completed application form or nay application that is made otherwise than on the forms specified within this application.

10.6.2 Before approving an application the Authorising Officer must:

(a) Consider an apply this policy, the relevant statutory material and guidance, together with any other internal guidance that may be issued from time to time;

(b) In cases of doubt, seek the advice of the RIPA Monitoring Officer or the Council's legal services department;

(c) Be clear that there are no ambiguities in the application or their authorisation as to what is being applied for and what is being authorised;

(d) Ensure that their statement of reasons establishes:

- Who the subject of the investigation is;
- What is being applied for / authorised;
- Where the authorised activity will take place;
- When the authorised activity will take place;
- Why that activity is necessary and proportionate to the investigation;
- How the authorised activity will take place

(e) Be satisfied that the use of RIPA powers is:

- In accordance with the law;
- Necessary in the circumstances of the particular case on the grounds set out with the application, and;
- Proportionate to what is sought to be achieved.

(f) In assessing whether the proposed activity is necessary to use covert surveillance at all or whether the same information could be obtained by overt or other means.

(g) In assessing whether the proposed surveillance is proportionate, consider whether there are any non-intrusive methods of obtaining the information and, if there are nine, whether the proposed surveillance is not more than the minimum necessary to achieve the required objective, as judicial approval will only be given to the least intrusive method of surveillance possible.

(h) Take into account the risk of collateral intrusion and the Investigating Officer's plan to minimise that intrusion. Measures must be taken wherever possible to avoid or minimise collateral intrusion. When considering proportionality, the Authorising Officer must consider the right to privacy of both the subject and the third parties.

(i) Allocate a sequential unique reference to the forms and the application which follows the last entry in central register and which follows the format: 001/2022, 002/2022 etc.

(j) Set and record dates on the application and the central register for (1) the review of the application and (2) the time and date upon which the authorisation shall expire, having regard to the type of application and the applicable operational periods.

(k) Ensure that the Central Register is properly updated and that copies of the application and its authorisation are forwarded to the RIPA Monitoring Officer.

10.6.3 When completing the authorisation section of the form, the Authorising officer must bear in mind that they may be called upon to justify the grant of that authorisation before the Court and give sufficient reasons to enable an impartial person with no prior knowledge of the matter to understand from those reasons, what was being sought and why the application was granted. As a rule of thumb, if after reading the recorded reasons for granting the application it is still possible to ask why the application was granted, the reasons are not sufficiently detailed.

10.6.4 Reasons for granting an authorisation must be written using the Authorising Officers own words and avoiding generic words, phrases and sentences.

10.7 Additional Safeguards when Authorising a CHIS

10.7.1 Where an Authorising Officer is assessing an application for the conduct or use of a CHIS the Authorising Officer must also be satisfied that:

(a) The persons who are to have day to day responsibility for the CHIS and oversight of the CHIS have been authorised for that purpose by the Senior Responsible Officer;

(b) Be satisfied that the conduct and use of a CHIS is proportionate to what is sought to be achieved;

(c) Consider the degree of intrusion of all persons who are likely to be affected by the use of the CHIS;

(d) Consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or as a consequence of the information obtained.

(e) Ensure that records which contain particulars of the CHIS and associated information are restricted only to those who need to know those details, and:

(f) In any case where there is any degree of uncertainty, take the advice of the RIPA Monitoring Officer before signing the forms or authorising the activity.

10.8 Judicial Approval

10.8.1 If an Authorising Officer authorises or renews an application for directed surveillance or a Senior Authorising Officer authorises or renews an application for a CHIS, the Council must apply to the Manchester and Salford Magistrates' Court for judicial approval. The authorisation will not become effective unless and until judicial approval has been granted.

10.8.2 In order to apply for Judicial Approval, the Investigating Officer or the Authorising Officer must supply to the Council's legal services department:

- A copy of the application and authorisation by the appropriate officer, and:
- An application for judicial approval using the form specified within Appendix A.

10.8.3 The officer submitting the application must ensure that the application for judicial approval contains sufficient information to enable the court to determine the application without the need for further oral evidence at court. In particular the written application must be capable of justifying:

- Whether the application has been made and authorised in accordance with the Council's policy and the statutory requirements;
- Whether the application has been properly authorised with the Council by an Authorising Officer of an appropriate grade, and:
- Whether the proposed activity is necessary and proportionate.

In cases of doubt, the assistance of the assigned officer within the Council's legal services department should be sought.

10.8.4 Only those Council's officers who have been authorised to conduct legal proceedings on behalf of the Council in accordance with the Local Government Act 1972, s223(1) or who hold a recognised right of audience which entitles them to conduct legal proceedings in accordance with the provisions of the Legal Services Act 2007 may appear before the court to assist the applying officer make their application.

10.8.5 On receipt of those documents, the nominated officer in the Council's legal services department will:

- Review the application to ensure that the documentation required by the Court has been properly completed and that the application is valid;

- Contact the court's listing officer to make an appointment to attend at court to make the application for judicial approval. Local practices dictate that the court will usually make applications to consider urgent applications at the start of the next morning or afternoon court session on standard business days. During holiday and bank holiday periods the early advice f the Council's legal services department should be sought. It is the court's normal practice to hold special courts on Saturdays and Bank Holidays. The court does not sit on Sundays, save in exceptional circumstances or on Christmas Day or on Good Friday;

- Attend at court with the Investigating or Authorised Officer who is to make the application before the Court and two copies of the application bundle.

10.8.5 The magistrates' court may consist of a District Judge or Justice of the Peace sitting alone, who may be assisted by a legal advisor. It is standard local practice for such applications to be heard in chambers, which in practical terms means that no one other than those persons directly involved in making or determining the application will be present.

10.8.6 Having considered the application the court may:

- Refuse to approve the application – in which case the proposed activity cannot take place. A copy of the Court's order refusing to authorise the application must be retained and filed in the Council's central register of documents and on the investigation file.

- Approve the application for authorisation or approval – in which case the proposed activity may take place or continue to take place, but only to the extent of the authorisation granted by the Court. A copy of the Court's order authorising the application must be retained and filed in the Council's central register of documents and on the investigation file.

10.8.7 The Manchester and Salford magistrate's court's contact details are:

Manchester and Salford Magistrates' Court
Address: Crown Square, Manchester, M60 1PR
E Mail: gm-manmcadmin@justice.gov.uk
Telephone: 0161 830 4200

10.8.8 A flow chart depicting the process for applying for judicial approval is shown in Appendix B.

11.0 Working with Other Agencies

11.1.1 Where the Council instructs some other agency to conduct activities on its behalf that require authorisation under RIPA, this policy and the procedures specified within it apply. An agency should not be instructed to conduct and activity which requires authorisation, unless and until:

- The agency has been made explicitly aware in writing of the need to comply with the requirements of this policy, and:

- The activity has been properly authorised and judicial approval has been granted following the procedures and using the forms and processes specified in this policy.

11.1.2 Where an external statutory investigatory agency, such as the Police, HM Customs and Excise, or the Department for Work and Pensions:

- Wishes to use the Council's resources, that agency must use its own RIPA procedures and before any officer agrees to allow the Council's resources to be used for that external agencies purposes they must obtain a copy of that organisations RIPA authorisation, which must be passed to the RIPA Monitoring Officer and be recorded on the Council's Central Register. In appropriate circumstances the external agencies RIPA authorisation form may be redacted to exclude any parts of that authorisation which does not form part of the request for assistance, save and accept that the RIPA Monitoring Officer must be satisfied that the authorisation is sufficiently detailed to justify the Council permitting the use of its facilities. Such applications should normally be considered by an Authoring Officer and be recorded as a non RIPA activity in the Council's central register.

- Wishes to use the Council's premises for its own RIPA action and is expressly seeking the assistance of the Council. In such circumstances the use of the Council's RIPA procedure will not be required, as the Council is merely assisting in the activity and is not involved in it. Such requests should normally be approved unless there are security, operational or another good reason why the request should be declined. Consideration must be given as to whether it would be appropriate to seek an indemnity or evidence of insurance is required to ensure the adequate protection. Such applications should normally be considered by an Authoring Officer and be recorded as a non RIPA activity in the Council's central register.

11.1.3 If the police or some other statutory investigatory agency wish to use the Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate written application should be sought from the external agency detailing the proposed use of the facility, the extent of the remit, its duration, who will be undertaking the surveillance and the purpose of it. The matter should be considered by an Authorising Officer in conjunction with the appropriate Head of Department. A record of the application and the result should be recorded within the Councils Central Register of Non- RIPA activity.

12.0 Joint Operations

12.1 Where the Council is conducting a joint investigation with another agency, such as the Police or HSE and authorisation is required to deploy directed surveillance or a CHIS, only one application for authorisation is required.

12.2 At the start of a joint investigation the Council's Senior Investigating Officer in consultation with their Head of Department and their opposite numbers in the partner agency must agree which organisation shall be the lead authority which will have overall responsibility for the management and direction of the investigation, the retention of evidence etc.

12.3 Where RIPA authorisation is required during a joint investigation, the appropriate officer within the lead organisation is responsible for securing RIPA authority according to their own internal policies and procedures.

12.4 Where an external agency obtains a RIPA authorisation that relates to an activity in which the Council's officers will be involved, copy of that authorisation should be obtained and be provided to the RIPA Monitoring Officer for inclusion in the Council's Central register to ensure that the Council can demonstrate that its officers have complied with the relevant statutory criterion.

13.0 Non-RIPA Authorisations

13.1 Where an activity being or intended to be conducted by an officer of the Council which falls outside of the parameters of the Regulation of Investigatory Powers Act 2000 for any reason, but which may interfere with the rights of an individual to privacy or which is for some other reason is comparable to an activity which would require authorisation but for the fact that RIPA does not apply, good practice and transparency requires that proper consideration should be given for the need to conduct that activity and whether it is proportionate to what is seeks to achieve.

13.2 Examples of such activities may include, but are not limited to:

- The Council is conducting an investigation which is not for the purposes of preventing or detecting crime;
- Circumstances where the Council's officers are assisting in an investigation where activities have been authorised under RIPA by another organisation;
- Circumstances where social media is being used to trace a person or something which fall outside the parameters of a criminal investigation but which may lead to private information being obtained, or:
- The use of CCTV and ANPR systems in manner which does not require authorisation;
- Test purchasing which does not require authorisation;
- Any activity which is directly comparable to an activity that would require authorisation under RIPA if the Act applied to the circumstances of that activity

13.3 In such circumstances Investigation Officers, in conjunction with Authorising Officers must consider whether such an activity is necessary and proportionate, adopting as a framework the criterion that would apply under RIPA and Authorising Officers should record those activities in the Central Register of Non RIPA activity held within the Central Register Maintained by the RIPA Monitoring Officer.

13.4 Recording the use of non-RIPA powers in that way enables the RIPA Monitoring Officer to ensure that the Council's use of its powers are open and transparent and for quality management purposes by ensuring that appropriate decisions are being made as to when and when not RIPA authorisation is required.

13.5 The RIPA Monitoring Officer will monitor and review the Council's use of non-RIPA powers as part of their scheme of review for quality assurance purposes and will record the results of those reviews within their report to members.

13.6 Forms for seeking to use non-RIPA powers and their authorisation are contained within Appendix A.

13.7 Judicial approval for non-RIPA authorisations is not required and is not available.

14.0 Record Management

14.1 The Council is required to keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections together with all application forms, decisions and judicial approvals or rejections for a period of three years to enable those documents to be audited by the IPCO and to facilitate effective monitoring and reporting of RIPA actions by the RIPA Monitoring Officer.

14.2 In order to comply with the requirements of the Criminal Procedure and Investigation Act 1985 and its Code of Practice, records of all RIPA decisions that relate to a proposed on ongoing criminal case, must be kept throughout those proceedings and for such period afterwards as is required by that Act.

14.3 The Central Register

14.3.1 The RIPA Monitoring Officer will maintain a central electronic register which records:

- A register of applications, which records:
  - whether those applications were authorised or refused
  - whether judicial approval was granted or refused
  - The dates of application
  - The date upon which the activity was authorised
  - The date and result of any review
  - The date and result of any application to renew
  - The end or cancellation date
- A register of non RIPA regulated activity;
  - whether those applications were authorised or refused
  - The dates of application
  - The date upon which the activity was authorised
  - The date and result of any review
  - The date and result of any application to renew
  - The end or cancellation date
- A register of those officers responsible for discharging this policy and:
  - Their contact details
  - The date of their employment
  - Their relevant training record
  - The date they ceased to be a responsible officer
- A register of Investigating Officers entitled to apply for RIPA authorisation and:
  - Their job title and role;
  - Their department;
  - Their contact details;
  - The date of their last RIPA related training.

14.3.2 Additionally, the RIPA Monitoring Officer will securely retain copies of the applications for authorisation, renewals and cancellation, reviews and applications for judicial approval and the court's decisions within a secure electronic file.

14.3.3 Access to the Central Register is made available for the duration of their appointment to:

- The Senior Responsible Officer
- RIPA Monitoring Officer

- Senior Authorising Officers
- Authorising Officers

14.3.4 Authorising Officers are responsible for ensuring that:

- Details of any application referred to them are entered into the Central Register at the time of receipt;
- That the application is allocated the next sequential unique reference number available on the register;
- That the register is updated at each stage of the application process and throughout the duration of the authority, and:
- That all relevant forms are sent to and have been received by the RIPA Monitoring Officer within 48 hours of any relevant decision for inclusion in the RIPA Monitoring Officer's central record.

14.3.5 The RIPA Monitoring Officer is responsible for ensuring that:

- The accuracy of the register is maintained by ensuring that it is properly updated by Authorised Officers at all times;
- The lists of Responsible Officers and Investigating Officers is up to data and records the most recent training provided to these officers.
- For monitoring the data held within the register and reporting upon it.

14.4 Departmental Records

14.4.1 Investigating Officers are responsible for keeping a record of all RIPA activity, applications for authorisation, renewal and cancellation and the results of those applications within their department.

14.4.2 Investigating Officer also have a duty under parts 4 and 5 of the Code of Practice made under the Criminal Procedure and Investigation Act 1985 to record and retain information which overlap with the requirements of this Policy and which must also be strictly observed

14.4.2 Investigation Officers must also keep records of all activity conducted as a result of a RIPA authorisation and make arrangements for the retention of any material obtained as a result of that process so as to comply with this Policy and the Code of Practice.

15.0 Reporting

15.1 The RIPA monitoring office will submit reports on the use of the Council's surveillance powers to:

- The Council's Executive Committee on a three monthly basis or as necessary, if the Council has used its powers under RIPA within the proceedings three months, and to:

- The Council's Accounts and Audit Committee annually on this policy and, if relevant, the Councils use of its RIPA powers.

15.2 The RIPA Monitoring Officer will also report to those Committee's at the next scheduled meeting after:

- A substantial breach of the procedures and policies set out within this policy;

- A substantial change in legislation of the Codes of Practice that underpin this policy, or:

- After a material change to this policy.

16.0 Concluding Remarks

16.1 Whenever the Council's investigative activities create a risk of interference with a person rights under the European Convention on Human Rights, those activities will only be lawful if they are according to law and necessary and proportionate.

16.2 This requirements and procedures within this policy are intended to ensure that the Council's activities are lawful, necessary and proportionate at all times. By following and abiding by this policy the Council's officers can be assured that their actions are properly authorised and subject to the safeguards set out with the legal framework and this policy.

16.3 This policy will only be effective if:

- Everyone who is required to participate in the processes set out within it strictly observe all the requirements of the policy;
- Application forms and decision makers reasons are properly filled out with reliable and detailed information that is sufficient to enable good quality decision making and from which independent observers can understand and approve the reasons for those decisions;
- Authorising Officer properly apply their minds to each individual application that come before them and never rubber stamp an application without giving full attention to their responsibilities and those of the Council.

16.4 Proper reporting as set out within this report will enable the RIPA Monitoring Officer and the Committee's to whom they report to validate and quality assure the Council's processes and identify areas capable of improvement.

16.5 The consequences of not complying with this policy are that:

- A court may find that the Council acted unlawfully in acting as it did;
- A court may refuse to admit any evidence that was unfairly or unlawfully obtained which may result in the collapse of a criminal case and the loss of time, effort and expense of brining that case before the Court;
- Potential exposure of the Council or an individual to criminal or civil sanctions as a result of that breach of policy;
- Disciplinary action being taken against a person responsible for a breach of policy, and;
- Reputational damage to the Council.

16.6 All those risks can be avoided or minimised by following the guidance and procedures within this policy and by seeking appropriate advice in any case of doubt from the RIPA Monitoring Officer or the Council's legal services department.

Appendix A – Specified Forms

DS 1	Application for Directed Surveillance
DS 2	Review of Directed Surveillance
DS 3	Application for Renewal of directed surveillance
DS 4	Application for Cancellation of Directed Surveillance
CHIS 1	Application for Use or Conduct of CHIS
CHIS 2	Review of CHIS
CHIS 3	Application for Renewal for Use or Conduct of CHIS
CHIS 4	Application for Cancellation of CHIS
DPIA	Data Protection Impact Assessment
HS&W 1	Health and Safety and Welfare Assessment – Officers and 3rd Parties
HS&W 2	Health and Safety and Welfare Assessment – Officers and 3rd Parties
JA1	Application for Judicial Approval
NR1	Application for Authorisation on Non-RIPA Activity
NR2	Review of Non-RIPA Activity
NR3	Cancellation of Non-RIPA Activity

Appendix B – Flow Charts

Flow Chart – Decision Making Process for CHIS and Directed Surveillance

Flow Chart – CHIS Awareness

Appendix C – Key Personnel

Schematic list of key personnel