

Legal, Licensing & Registration Services

Regulation of Investigatory Powers Act 2000

Guidance and Procedure

1. INTRODUCTION

- ◆ The Regulation of Investigatory Powers Act (RIPA) controls and regulates surveillance, and other means of gathering information, which public bodies employ in the discharge of their functions. Information gathering is one of the Council's many activities which could involve an interference with an individual's human rights, specifically an individual's rights under Article 8.
- ◆ Article 8 provides:
 - Everyone has the right to respect for his private and family life, his home and his correspondence.
 - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- ◆ RIPA provides an authorisation process for certain types of surveillance and information gathering, and that process can be used as a defence against certain human rights claims. Conversely, if the Council chose not to use that process, where it could have done, the courts might find that the Council's actions were not "in accordance with the law".
- ◆ It is important to distinguish between the types of surveillance and information gathering regulated by RIPA, and normal general observation, in the course of discharging the Council's functions. It is acknowledged that low-level general observation will not usually be regulated under the provisions of RIPA. The Covert Surveillance and Property Interference Revised Code of Practice referred to later in this document, gives the following examples of this kind of general observation:
 - patrolling to prevent and detect crime,
 - officers attending a car boot sale where it is suspected that counterfeit goods are being sold, but where the intention is, through reactive "policing", to identify and tackle offenders.

2. WHICH KINDS OF SURVEILLANCE AND INFORMATION GATHERING METHODS ARE REGULATED BY RIPA?

- ◆ Covert surveillance which consists of directed surveillance, intrusive surveillance, the conduct and use of covert human intelligence sources, and intercepting communications are all regulated by RIPA.

3. HOW HAS THE GOVERNMENT IMPLEMENTED RIPA?

- ◆ The government has issued a Covert Surveillance and Property Interference Revised Code of Practice, a Covert Human Intelligence Sources Code of Practice and an Interception of Communications Code of Practice. These Codes, along with the text of RIPA and copies of approved forms are available on the Home Office, Office for Security and Anti-Terrorism website at <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/>. If you do not have access to the internet, copies of these materials can be obtained from Legal, Licensing & Registration Services (Legal). References in this document to “the relevant Code”, are references to one or other of these Codes as appropriate.
- ◆ The Council must have regard to these Codes of Practice, and they should be given careful consideration by all those involved in activities regulated by RIPA.
- ◆ The Codes and this document must be made readily available to members of staff, customers, and elected Members.
- ◆ The Office of Surveillance Commissioners (OSC) keeps under review the performance of functions relating to covert surveillance, and makes periodic inspections for these purposes. Details of the Council’s latest inspection report can be obtained from Legal.

4. HOW HAS THE COUNCIL IMPLEMENTED RIPA?

- ◆ Under the Council’s constitution, the following matters are the responsibility of the Assistant Chief Executive (Corporate Governance):
 - Preparing policies and strategies for approval
 - Guidance and advice
 - Monitoring compliance
- ◆ Legal maintain the RIPA Central Record, and are responsible for monitoring and quality control. The relevant procedures are in Appendix 2 and Appendix 3 respectively.
- ◆ The following matters are the responsibility of Directors/Chief Officers:
 - To implement and secure compliance with the rules on surveillance activities, the Council’s policies on these matters, and guidance and advice from Legal on these matters.
 - To designate officers with specific responsibilities for these matters (RIPA practitioners).
- ◆ The Council has approved a RIPA policy. This is in Appendix 1. The relevant Code requires local authorities to involve elected Members in strategic oversight, including

setting the policy and reviewing use at least once a year, and considering reports on use on at least a quarterly basis. The Council has decided the use of covert surveillance will be reviewed by Corporate Governance and Audit Committee on a quarterly basis, and that the Committee will review the policy on an annual basis.

- ◆ These delegations mean that you should refer day to day queries which you may have on RIPA matters, to the RIPA practitioner for your service. They may then of course choose to refer some of these matters to Legal.
- ◆ If RIPA practitioners want to issue their own guidance relating to the activities of their own service, this must first be approved by Legal.

5. WHAT DOES “SURVEILLANCE” MEAN?

- ◆ RIPA says “surveillance” means monitoring, observing or listening to persons, their movements, conversations, other activities or communications, recording anything monitored observed or listened to in the course of surveillance, and surveillance with a surveillance device (which means anything designed or adapted for surveillance use).

6. WHEN DOES SURVEILLANCE BECOME “DIRECTED SURVEILLANCE”?

- ◆ Surveillance becomes “directed surveillance” when **ALL** of the following criteria are satisfied. The surveillance must:
 - be “covert”. This means surveillance which is carried out in a way that is “calculated to ensure” that the subjects are unaware that it is or may be taking place. “Calculated to ensure” means there must be a deliberate effort by the Council to make sure the subjects aren’t aware of the surveillance
 - be for the purposes of a “specific investigation” or a “specific operation”. General observations which do not involve the systematic surveillance of an individual, will not be directed surveillance
 - be undertaken in such a manner as is likely to result in the obtaining of “private information” (this includes any information relating to a person’s private or family life) (whether or not that person is the subject of the investigation). The relevant Code says private information should be taken generally to include any aspect of a person’s private or personal relationship with others, including family and professional or business relationships, and that “family” should be treated as extending beyond the formal relationships created by marriage or civil partnership. The relevant Code also says that whilst “a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person’s activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is made by a public authority of that person’s activities for future consideration or analysis”. As a result, where an investigation includes covert surveillance using CCTV cameras, the creation of a record by filming activities even in a “public” place such as in the street, may amount to obtaining “private” information. The relevant Code also suggests that if several records are to be analysed together (even if some pieces of information have been obtained overtly), “the totality of information gleaned may constitute private information even if individual records do not”. The use of surveillance devices designed or adapted for the purpose of providing information about the location of a vehicle alone will not necessarily provide private information

about any individual. If one or both ends of a telephone conversation were to be monitored by a surveillance device, even if this did not amount to an “interception”, it would still result in “private” information being obtained.

- not be done as an immediate response to events or circumstances, where it would not be reasonably practicable to try and get an authorisation
- not be intrusive (please see below)

7. EXAMPLES OF SURVEILLANCE WHICH WOULD NOT BE “DIRECTED SURVEILLANCE”

- ◆ Council officers openly observing the activities of residents whilst patrolling the streets, as part of activities to combat anti-social behaviour. Note “openly” means there mustn’t be any deliberate effort to make sure individuals aren’t aware that this is taking place.
- ◆ Generally, the use of CCTV cameras, where these are properly signed.
- ◆ Routine planning enforcement visits, to check up on the physical development of a site.
- ◆ Covert surveillance of premises (as opposed to individuals) by environmental health officers, as part of their routine duties to detect statutory nuisances.
- ◆ Covert surveillance of anti-social behaviour towards others, actually occurring in a “public” place, such as the street.
- ◆ Recording, for example on a file or computer record of anything monitored, observed or listened to, after the surveillance has taken place.
- ◆ Monitoring an activity after it has ceased. For example, examining a web log of internet sites which an individual has visited after those visits have taken place.
- ◆ The covert surveillance of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises, and the recording device is calibrated to record only excessive noise levels.

8. DOES DIRECTED SURVEILLANCE HAVE TO BE AUTHORISED?

- ◆ The Council’s current policy referred to above, is that directed surveillance should be authorised, although RIPA doesn’t require this. RIPA says surveillance is lawful for all purposes, if an authorisation has been properly granted, and the surveillance is in accordance with that authorisation. Consequently, a proper authorisation should be a full protection, in the event of a claim by an individual who has been the subject of surveillance, for breach of their Article 8 rights.
- ◆ The Council can authorise its directed surveillance. The approved forms on the Home Office website mentioned above, must be used.

9. WHAT ARE COVERT HUMAN INTELLIGENCE SOURCES?

- ◆ The term Covert Human Intelligence Source (CHIS) is used to describe people who are more commonly known as informants. Informants are used more widely by the Police and other law enforcement organisations than by the Council.
- ◆ However, a CHIS would also include work by officers working “undercover” whereby a covert relationship is established with another person. This type of activity may sometimes be undertaken by officers. This guidance only deals with circumstances when a CHIS authorisation would be needed for officers. It should only be in exceptional circumstances that it is proposed to use a person who is not an officer, and in this event further guidance must be sought from Legal.
- ◆ A person is a covert human intelligence source if:
 - he/she establishes or maintains a personal or other relationship with a person for the covert purpose of
 - covertly using the relationship to obtain information or to provide access to any information to another person; or
 - covertly disclosing information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.
- ◆ A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
- ◆ A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is 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.
- ◆ A routine test purchase, which does not go beyond a normal transaction, would not be considered a CHIS activity. Many sources volunteer or provide information that is within their personal knowledge, for example a member of the public volunteering information about something he has witnessed in his neighbourhood, where a relationship will not have been established or maintained for a covert purpose. Where members of staff are required to comply with the Money Laundering Regulations and report suspicious transactions, this will not result in these individuals meeting the definition of a CHIS.

10. CAN THE COUNCIL AUTHORISE THE USE OF A CHIS?

- ◆ Yes. Again, the Council can authorise its use of a CHIS. Applications for authorisation, and decisions to authorise or not, must be made in the same way, and subject to the same rules as for directed surveillance. Again, the Home Office prescribed forms must be used. Care must be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are risk assessed. The use or conduct of a CHIS can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management.
- ◆ Note however, authorisation must not be given unless:
 - there is a person (known as the “handler”) in the service, with day to day responsibility for dealing with the CHIS, and for monitoring their security and welfare

- there is another person in the service (known as the “controller”), who will have general oversight of the use made of the CHIS, and will normally be responsible for the management and supervision of the “handler”.
 - there is a person in the service with responsibility for maintaining a record of the use made of the CHIS
 - that records disclosing the identity of the CHIS will not be available to persons except to the extent that there is a need for access.
- ◆ **Note also the relevant Code says vulnerable individuals should only be authorised to act as a CHIS in the most exceptional circumstances.** A “Vulnerable individual” is defined as a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Authorisation in such a case would need to be by the Head of Paid Service (Chief Executive).
 - ◆ **Note also there are special safeguards for the use or conduct of a CHIS who is a juvenile, i.e. who is under 18.** The relevant Code says on no occasion should the use or conduct of a source under 16 be authorised to give information against their parents, or any person who has parental responsibility for them. In other cases, special provisions must be complied with, and again authorisation would need to be by the Head of Paid Service (Chief Executive). The duration of such an authorisation would be only one month.
 - ◆ The relevant Code says that any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.
 - ◆ Applicants or authorising officers who are uncertain whether an officer is being asked to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS, or who are uncertain about the management of a CHIS must seek advice from Legal.

11. WHO CAN GIVE DIRECTED SURVEILLANCE AND CHIS AUTHORISATIONS?

- ◆ Generally, The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 permits a “Director, Head of Service, Service Manager or equivalent” to grant authorisations. This will also include anyone in a more senior position. The Council’s RIPA policy says authorisations will only be granted by Directors.
- ◆ **Note the relevant Code says that “particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information**

consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material". In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation, and in the Council's case the authorising officer is the Head of Paid Service (Chief Executive).

- ◆ The relevant Code defines confidential personal information as information held in confidence relating to the physical or mental health, or spiritual counselling of a person (whether living or dead) who can be identified from it.
- ◆ The relevant Code defines confidential journalistic material as including material acquired or created for the purposes of journalism, and held subject to an undertaking to hold it in confidence, and communications resulting in information being acquired for the purposes of journalism, and held subject to such an undertaking.
- ◆ ***The relevant Code says where confidential information has been acquired and retained, this should be reported to the Commissioner or Inspector during the next inspection, and the material should be made available to them if requested. Consequently, applications need to specify this so that the Central Record can be properly maintained by Legal.***
- ◆ ***If there is any doubt about whether confidential information is likely to be acquired, retained, or disseminated advice should always be sought from Legal.***

12. WHAT ABOUT EDUCATION (LEEDS) AND THE ALMOS?

- ◆ ***Neither Education (Leeds), nor the ALMOs (housing arms length management companies) are designated as public authorities under the RIPA rules, and so they are unable to grant authorisations.*** However, it is possible that they could still be sued for human rights breaches, on the strength of commitments given by them in their agreements with the Council, or that the Council could be sued by individuals for human rights breaches by the companies. ***Consequently, these companies must always complete a Human Rights Audit (form in Appendix 4).***
- ◆ Note the distinction between the Council's and the companies' responsibilities, may sometimes need careful consideration. For example, the ALMOs are responsible for their members of staff, but might request the Council's internal auditors to assist in a disciplinary, or fraud investigation. In these circumstances, the ALMO would need to complete a Human Rights Audit Form, (but the Council's auditors would not need to arrange for a directed surveillance authorisation) because responsibility for the investigation would lie with the ALMO.

13. WHEN CAN AUTHORISATION PROPERLY BE GIVEN?

- An authorisation cannot be granted unless the authorising officer believes that the authorisation is "**necessary**" on certain specified grounds, and that it is proportionate to what is sought to be achieved by carrying it out. "Necessary" means more than simply convenient or desirable for the Council. Authorising officers should be sure that the use of overt investigation methods has always been considered before considering whether

an authorisation is required. Covert investigation authorised under RIPA should be used only when other reasonable options have been considered and ruled out.

- **“Proportionate”** means that the Council needs to try and strike a fair balance between the intrusiveness of the activity on the subject and others who might be affected by it, against the need for the activity in operational terms and the public interest in preventing the relevant crime or disorder. This means the activity must not be excessive or heavy-handed, and must take account of the particular circumstances of the subject and others affected, and the particular sensitivities of the communities in which they live. Authorising officers should seek to limit surveillance to the minimum level required to meet the outcome. The relevant Code says the following elements of proportionality should therefore be considered
- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence, or disorder;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

◆ **The only specified ground upon which the Council can grant an authorisation is:**

- preventing or detecting crime or preventing disorder

14. WHAT IF THE PURPOSE DOESN'T FIT INTO THE SPECIFIED GROUND?

- ◆ For example, where audit investigations undertaken to safeguard the financial resources of the Council, include covert surveillance, there may be no RIPA ground for authorising directed surveillance. ***In these circumstances, a RIPA authorisation cannot be given, but a Human Rights Audit must be completed.***

15. WHAT DO APPLICANTS AND AUTHORISING OFFICERS NEED TO DO?

- ◆ An authorising officer must give authorisations in writing, except that in urgent cases they may be given orally by the authorising officer. Authorisations given orally will last for 72 hours. Written authorisations will last for 3 months. Written authorisation for use of a CHIS can last for a period of 12 months. The Codes say cases should not be regarded as urgent, unless the delay would, in the authorising officer's judgement, be likely to endanger life or jeopardise the investigation or operation for which the authorisation is being given. An authorisation should not be regarded as urgent, simply because the need for an authorisation has been neglected, and the urgency is of the applicant's or authorising officer's own making.
- ◆ Where authorisation is given **orally**, authorising officers must make sure the following are also recorded in writing on the relevant file, as soon as reasonably practicable:

- The identities of those subject to surveillance
 - The nature of the surveillance
 - The reasons why the authorising officer considered the case to be so urgent, that an oral instead of a written authorisation was given
 - Although not required by the relevant Code, it would also be best practice for the applicant and authorising officer to subsequently record in writing on the relevant file, the information which would normally be included in an application for written authorisation, in case the Council later receives a human rights claim arising from the surveillance.
- ◆ Applications for authorisation must include an assessment of the risk of any **collateral intrusion** or interference with the privacy of persons, other than the subject of the surveillance, and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed activity. Authorising officers must make sure that the activity is managed in such a way, and that measures are taken wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. If surveillance is specifically proposed against an individual who is not suspected of direct or culpable involvement in the relevant crime or disorder, any interference with their privacy should be considered as intended, rather than collateral intrusion. Any such surveillance should be carefully considered against the necessity and proportionality criteria referred to above.
- ◆ ***Every directed surveillance and CHIS authorisation must be sent to Legal for inclusion in the Central Record. Please note Legal must make the Central Record available to the relevant Commissioner or Inspector from the OSC, upon request. Please note the original application and authorisation, and any documents referred to in that form would be of critical importance in the event of a human rights claim against the Council. It is therefore essential that the original forms are sent to Legal, and that any background documents are preserved appropriately by the applicant or authorising officer.***

16. HOW SHOULD THE RIPA FORMS BE FILLED IN?

- ◆ The Home Office prescribed application form includes:
- a description of the purpose of the specific operation or investigation. This should include a concise and balanced summary of the alleged crime or disorder, and the specific objectives of the investigation, with a description of the evidence it is sought to gather.
 - A description of the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment that may be used. The type of surveillance, for example static or mobile, needs to be described, as well as how the surveillance will be conducted, for example by CCTV or by observation. The place where the surveillance is to be conducted, the number of officers involved, and the duration of the surveillance need to be specified. If any equipment is to be used, a technical description should be given, and also a description of the level of intrusion. For example, if cameras are to be used how will they be directed, or if sound recording equipment is to be used, will it record speech? Note sufficient detail needs

- to be given, so the authorising officer can properly assess whether the operation is proportionate, and the likelihood of collateral intrusion.
- the information that it is desired to obtain as a result of the directed surveillance. This should explain the levels of evidence which the applicant hopes to obtain, and how this will go to prove or disprove the allegations of crime or disorder.
 - The ground on which the directed surveillance is “necessary” – see above. If it is not possible to identify a specific crime in the application or grant, the Investigatory Powers Tribunal have said it must be “reasonably clear what sort of criminal offence might be prevented”, and there must be a “reasonable belief” that such an offence was or would be committed.
 - An explanation of why the proposed surveillance is “necessary” on the ground identified – see above. This must include evidence that the Council has considered whether measures other than covert surveillance were feasible and sufficiently effective, and if such measures have been tried and failed, a description of those measures. This must also explain why the applicant believes covert surveillance is the only method left available to progress the investigation.
 - Any collateral intrusion and why it is unavoidable, and the precautions taken to minimise such intrusion. This should state who the surveillance is likely to intrude upon, including the subject, and others as appropriate, for example others known to be in their household (in particular, any children), neighbours, work colleagues, and members of the public in the surveillance locations. The actions to be taken to reduce that risk must be stated, with an explanation how and why the methods to be adopted will cause the least possible intrusion on the subject and others listed. For example, how officers or equipment can be positioned to minimise intrusion, whether surveillance is to be limited to specific times, and whether the number of officers involved can be reduced depending on the location.
 - Why the directed surveillance is proportionate to what it seeks to achieve – see above. It must be shown that the surveillance is not excessive in the circumstances of the case, or arbitrary or unfair. Again, there must be a reasonable belief that the surveillance is proportionate, and the setting of reasonable conditions and limitations on the surveillance is likely to be key. For example, measures should be taken to ensure that young children who are not believed to be parties to the suspected crime or disorder, are not also made targets of the surveillance by default.
 - Confidential information – see above. It is important to identify any likelihood of acquiring this information, because particular care needs to be taken in such cases, and a special level of authorisation is needed.
 - Authorising officer’s statement, and why they believe the surveillance is necessary and proportionate. This must demonstrate that the authorising officer has actively considered and has understood the surveillance proposals, and has set conditions and limitations where appropriate. The activity which is being authorised must be fully specified, and a full justification for the surveillance must be given. Note it is for the authorising officer personally to justify the surveillance. This cannot be delegated, and the authorising officer must show they have done more than simply rely upon the judgement of other less senior colleagues.

17. SHOULD AUTHORISATIONS BE REVIEWED?

- Where a continuing investigation or operation is authorised, regular reviews should be undertaken using the Home Office recommended form. There is a need to review authorisations frequently where the surveillance involves a high degree of intrusion into private life, or significant collateral intrusion, or where confidential information is likely to

be obtained. A review is the responsibility of the original authorising officer and so should be conducted by them, or failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

- Any proposed or unforeseen changes to the nature or extent of the surveillance that may result in further or greater intrusion should be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether these changes are necessary and proportionate (bearing in mind any extra intended intrusion into privacy, or collateral intrusion), before approving or rejecting them.
- Where an authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals, and a review should be convened for this purpose. There will be no need for a new authorisation if the scope of the original authorisation envisaged surveillance of these individuals.
- ***Any reviews should be supplied to Legal for inclusion in the Central Record mentioned above.***

18. CAN AUTHORISATIONS BE RENEWED?

- ◆ Yes. If at any time before a directed surveillance authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he/she may renew it in writing for a further period of 3 months. Again, renewals may also be granted orally in urgent cases, and last for 72 hours. The renewal will take effect at the time at which the authorisation would have ceased to have effect but for the renewal. Renewals should be recorded using the Home Office recommended form.
- ◆ Applications for renewal must record (at the time of application, or when reasonably practicable in the case of urgent cases approved orally)
 - Whether this is the first renewal, or every occasion on which the authorisation has been renewed previously
 - Any significant changes to the information in the initial application
 - The reasons why the authorisation for directed surveillance should continue
 - The content and value to the investigation or operation, of the information so far obtained by the surveillance
 - The results of regular reviews of the investigation or operation
- ◆ ***Renewals must be supplied to Legal for inclusion in the Central Record mentioned above.***

19. DO AUTHORISATIONS HAVE TO BE CANCELLED?

- ◆ Yes. The authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, and they must cancel it, if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original authorising officer is no longer available, this duty will fall on the person who

has taken over this role, or who is entitled to act as authorising officer as mentioned above.

- ◆ As written authorisations are granted automatically for 3 months/12 months, this means each written authorisation needs to be cancelled, whatever the actual duration of the investigation or operation. The Home Office recommended form should be used. The reason for the cancellation will usually be that the objectives of the surveillance have been achieved, and this should be fully explained on the form. Best practice suggests that the authorising officer's comments should include a direction as to how the material, (or product) from the surveillance should be stored, and for how long.
- ◆ ***Cancellations must be supplied to Legal, for inclusion in the Central Record mentioned above.***

20. WHEN CAN SURVEILLANCE BE “INTRUSIVE?”

- ◆ Intrusive surveillance means covert surveillance which:
 - is carried out in relation to anything taking place on any **residential premises** (not including common areas, nor as suggested by the relevant Code of Practice, the front garden or driveway of premises readily visible to the public) or in any **private vehicle**; **and**
 - involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device
 - or is directed surveillance that is carried out in relation to anything taking place on so much of certain specified premises, as is, at any time during the surveillance, used for the purposes of legal consultation.
 - Intrusive surveillance may take place by means of a person or device located in the residential premises or private vehicle or place for legal consultation. It may also take place by means of a device **outside** the premises or vehicle or place for legal consultation which consistently provides information of the same quality and detail as might be expected to be obtained from a device inside. The use of a zoom lens for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.
- ◆ **Note the Council cannot authorise surveillance which is intrusive.** If it appears that a proposed surveillance investigation or operation, may fall within the scope of intrusive surveillance, then further guidance must be sought from Legal.

21. HOW DOES RIPA REGULATE THE INTERCEPTION OF COMMUNICATIONS?

- ◆ RIPA regulates the interception of communications in the course of transmission by means of a public postal service, or a public or private telecommunication system. This would include mail received by post or fax, the Council's phone systems and the Council's computer network.
- ◆ It would be a criminal offence to “intercept” mail, faxes, phone calls or e-mail whilst in the public system, unless the Council has lawful authority.

- ◆ Once mail and faxes have been received by the Council, interception would not be an offence, and the interception of phone calls or e-mail within the Council's private telecommunications systems will not be an offence as long as the Council has the right (as it usually will) to control the operation or use of the system, or as long as the Council again has lawful authority.
- ◆ However, the interception in the course of transmission by the Council of phone calls or e-mail within the Council's private telecommunications systems would mean the Council could be sued by the sender, recipient or intended recipient, unless again the Council has lawful authority.
- ◆ Interception in the course of transmission means modifying or interfering with the system, or its operation, or monitoring transmissions, so as to make some or all of the contents of the communication available, *while being transmitted*, to a person other than the sender or intended recipient. Modifying a system includes attaching any apparatus to, or other modification of, or interference with any part of the system. Being transmitted includes time when the system is used for storing the communication in a way that enables the intended recipient to collect it, or otherwise have access to it. Making available while being transmitted, includes cases where the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.
- ◆ Consequently, opening emails in an e-mail account, where these have already been sent or received, will only amount to an "interception" where e-mails remained unopened by the intended recipient. It would not seem that re-opening previously opened e-mails could constitute "surveillance", but plainly if a manager opened or re-opened an e-mail which contained information which was self-evidently not related to a member of staff's day-to-day working duties, that member of staff might complain that there had been unfair processing of their personal data, or that there had been an interference with their Article 8 rights. Consequently, where ICT are asked by a manager to provide access to a member of staff's e-mail account, they will require confirmation that a Human Rights Audit has been completed. The most appropriate human rights ground for access will usually be "the protection of the rights and freedoms of others". This ground will include the Council's rights as employer to prevent misconduct, the public's right to the effective and efficient delivery of services, and other e-mail users' rights to be protected from inappropriate e-mail use.
- ◆ ***If any activity is proposed, which you think might constitute the interception of a communication in the course of transmission by means of the public postal service, or a public telecoms system, advice must be sought from Legal.***
- ◆ ***If any activity is proposed, which constitutes the interception of a communication in one of the Council's private telecoms systems, this must only be done where the Council has "lawful authority".***
- ◆ Lawful authority can be given in a number of ways. One of these is where legitimate business practices can be authorised by the Secretary of State. Various practices have been so authorised by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These practices are listed in the Interception Audit Form in Appendix 5, and one or other of these practices must be identified. ***An Interception Audit Form must be completed and retained, in case the Council receives a claim for an unlawful interception.***

22. WHAT ABOUT CCTV AND ANPR (AUTOMATIC NUMBER PLATE RECOGNITION) SYSTEMS?

- ◆ Generally, RIPA does not affect CCTV systems where these are properly signed. This is because any surveillance is usually overt, rather than covert, and there is not usually a specific investigation or operation. If a CCTV system or ANPR were used to gather information as part of a reactive operation, for example to identify individuals who have committed criminal damage after the event, that would not be directed surveillance if the equipment was overt, and there was no covert targeting. However, if a system were temporarily diverted from its usual functions for the surveillance of a specific person or group of people, and the other usual criteria for directed surveillance were met, this would go beyond the intended use of the system for the general prevention or detection of crime and protection of the public, and could mean there was directed surveillance. For example, if a signed CCTV system on a housing estate, which was generally used only for general security purposes in “public areas”, was used specifically for monitoring a particular disturbance, this could constitute directed surveillance.
- ◆ Where CCTV systems are not signed, then unless the cameras are clearly visible surveillance will be covert, and there will be directed surveillance if the other criteria for directed surveillance are present.

23. WHERE CAN I GET MORE ADVICE?

- ◆ This document cannot provide a definitive statement of the law, in all situations, nor a full description of all aspects of the Codes. If you or your RIPA practitioner have any doubt about whether a particular activity is lawful, you should always seek further advice from Legal, contacting Mark Turnbull, Head of Property, Finance & Technology, Legal, Licensing & Registration Services, tel. 0113 2474408, e-mail mark.turnbull@leeds.gov.uk, in the first instance.

Appendix 1

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

1.0 Extent

This policy applies to the authorisation of directed surveillance under Sec 28(1) of RIPA. This policy does not cover the authorisation of covert human intelligence sources under Sec 29 of RIPA. Nor does it cover intrusive surveillance (which the Council is not entitled to authorise under RIPA).

2.0 Safeguards

2.1 The Council will apply a presumption in favour of overt investigation methods. The Council will always consider using a variety of overt investigatory tools, before considering whether an authorisation is required. Covert investigation will be used only when other reasonable options have been considered, and ruled out.

2.2 In order to comply with the duties in Sec 28(2) of RIPA, that a person shall not grant an authorisation for the carrying out of directed surveillance unless they believe that the authorisation is “necessary” on the ground of preventing or detecting crime or preventing disorder, and in accordance with the Covert Surveillance and Property Interference Revised Code of Practice, the Council will

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence, or disorder;
- explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, as far as reasonably practicable, what other methods were considered and why they were not implemented.

2.3 The Council will only use covert surveillance when the problem is serious and/or persistent, and where overt surveillance would not provide evidence and/or might displace the problem elsewhere.

2.4 The Council will not use covert surveillance to address minor matters, but instead will focus on those issues which are of greatest concern to the community – environmental damage such as flytipping and graffiti, and anti-social behaviour where individuals or families are targeted or threatened.

2.5 The Council will only use covert surveillance either to obtain evidence that can be presented at court, or where another positive outcome relating to the prevention or detection of crime or the prevention of disorder has been identified, for example through the positive identification of perpetrators.

2.6 The Council will give responsibilities to a single member of its Corporate Leadership Team, Nicole Jackson, Assistant Chief Executive (Corporate Governance) to ensure

that designated authorising officers meet the standards required by the Office of Surveillance Commissioners.

- 2.7 The Council will ensure that the quality of authorisations is monitored by Legal, Licensing and Registration Services.
- 2.8 The Council will ensure applicants and authorising officers receive an appropriate level of training.
- 2.9 The Council will ensure that in accordance with The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, authorisations will only be granted by Directors. This will avoid any perception that authorising officers are directly involved with the investigations they authorise. Authorising officers will therefore be able to apply more independently reasoned judgment of the issues
- 3.0 **Review**
- 3.1 This policy will be reviewed on an annual basis, and reports on the use of authorisations will be considered on a quarterly basis, in each case by Corporate Governance and Audit Committee.

Appendix 2

Regulatory of Investigatory Powers Act 2000

New Procedure for Central Record

Authorisations for Directed Surveillance

1. On deciding that an authorisation form for directed surveillance ('the authorisation') is required, the officer responsible for completing the first part of the authorisation ('the Applicant') will contact the officer responsible for administering the central record in Legal Services ('the Administrator') in order to obtain the unique reference number.
2. The unique reference number will consist of the following: the initials of the name of the directorate / the initials of the name of the service / the calendar year / the number of the authorisation within that year. For example, E&N / ASBU/ 09/ 01. The Administrator will confirm the unique reference number to the Applicant by e-mail, with a link to the Home Office recommended authorisation form.
3. Once the authorisation has been signed by the authorising officer, then it is the Applicant's responsibility to ensure that the original authorisation is sent to the Administrator to be stored on the central record. The Applicant retains a copy of the signed authorisation.
4. If the Administrator does not receive the authorisation within one week of issuing the unique reference number, the Administrator will contact the Applicant and remind him / her that the authorisation has not yet been received. The Administrator will send further reminders, at weekly intervals, until either the authorisation is received, or written confirmation is received from the Applicant that the covert surveillance is not proceeding, or that the application has not been authorised. The Administrator will store such confirmation on the central record.
5. On receiving the signed authorisation, the Administrator will record in the central record index:
 - a. the unique reference number;
 - b. the title of the investigation / operation;
 - c. the name of the Applicant;
 - d. the name and rank / grade of the authorising officer;
 - e. the automatic start and expiry dates. The start date is the date the surveillance is authorised. The automatic expiry date is 3 months from the start date. For example, an authorisation granted on 5 September 2010 will expire on 4 December 2010.
 - f. the estimated date for the actual end of the surveillance operation - if set out in the authorisation (see box 3).
 - g. the date of the first review - if this box has been completed by the authorising officer (see box 14).
 - h. whether the confidential information authorisation has been completed by the authorising officer (see box 14).
 - i. whether the urgency provisions were used (see box 15).

6. On the review date(s) (if provided), the Administrator will contact the Applicant and remind him / her that the original review form(s) must be sent through to Legal Services to be stored on the central record. The Administrator will send further reminders, at weekly intervals, until a copy of the review form(s) is/are received. The Administrator will then update the central record index accordingly.
7. On the estimated date for the end of the surveillance, the Administrator will contact the Applicant to ascertain whether the surveillance operation has been cancelled. If so, the Administrator will remind the Applicant to send through the original of the signed cancellation form. The Administrator will send further reminders, at weekly intervals, until a copy of the cancellation form is received. The Administrator will then update the central record index with the date and the time at which the instruction was given by the authorising officer to cease the surveillance operation, and also the date the authorisation was cancelled.
8. In the absence of an estimated date for the end of the surveillance, the Administrator will contact the Applicant at monthly intervals until the automatic expiry date to ascertain whether the surveillance operation is still continuing. If, one week before the automatic expiry date, the authorisation has not been cancelled then the Administrator will contact the Applicant to ascertain whether a renewal form is to be completed. If so, then the Administrator will remind the Applicant that the original renewal form must be sent through to Legal Services. The Administrator will send further reminders, at weekly intervals, until either the cancellation form or the renewal form has been received. The Administrator will then update the central record index accordingly. Where an authorisation is renewed, the index must contain the date of the renewal and the name of the officer who authorised the renewal.
9. In urgent cases an authorising officer may grant the authorisation orally. In these circumstances, it is the authorising officer's responsibility to inform the Administrator and to ensure that the original signed authorisation form, once completed, is sent through to Legal Services. The Administrator will then follow the steps set out in points 5 to 8 above.

Authorisations for Covert Human Intelligence Sources (CHIS)

1. Steps 1 to 9 above will apply for authorisations for CHIS.
2. In relation to Step 5, the automatic expiry date is 12 months for example, an authorisation granted on 5 September 2009 will expire on 4 September 2010.

Appendix 3

Regulation of Investigatory Powers Act 2000 (RIPA) - Monitoring and Quality Control Procedure

1. Introduction

This Procedure sets out the monitoring and quality control measures in relation to directed surveillance and CHIS authorisations, and associated documentation issued under RIPA. For general guidance on RIPA, and for details about how the Council's Central Record is maintained, reference should be made to the RIPA Guidance and Procedure document, and the procedure for the RIPA Central Record respectively.

2. Record keeping

In accordance with the Guidance and Procedure document, and the procedure for the RIPA Central Record, the Chief Officer, Legal, Licensing and Registration will maintain

- The authorisations register
- Original applications/ authorisations
- Original reviews of authorisations
- Original renewals of authorisations
- Original cancellations

in a Central Record, for at least 3 years.

3. Monitoring - General

The Chief Officer, Legal, Licensing and Registration will monitor and ensure the following in relation to authorisations generally,

- That RIPA authorisations, and human rights audits are being completed in appropriate circumstances, as specified in the Guidance and Procedure document
- That authorisations relating to the following are exceptional, and are reported appropriately to the relevant Commissioner or Inspector
 - confidential information
 - an authorising officer authorising their own investigation
 - vulnerable individuals or juveniles
- That specific advice is given where surveillance could amount to intrusive surveillance
- That there is a renewal and/or cancellation for each authorisation
- That authorisations are not being renewed unnecessarily
- That authorisations are being cancelled in a timely manner

4. Monitoring – Specific

In relation to each original authorisation received, the Chief Officer, Legal, Licensing and Registration will monitor the following

- The correct Home Office prescribed form has been used, (unless the use of a modified form has been approved)
- The applicant has undertaken the standard training for applicants
- Necessity has been explained adequately

- Proportionality has been explained adequately
- The correct RIPA ground has been specified
- Measures have been specified to minimise collateral intrusion, where necessary
- The authorising officer has undertaken the standard training for authorising officers
- The authorising officer has given an appropriate summary of the conduct to be authorised
- The date and start time have been specified

5. Training and Feedback

The Chief Officer, Legal, Licensing and Registration will provide standard training for all applicants, and standard training for all authorising officers, and will maintain a central register recording which officers have received such training. Refresher training will be provided not less than once every 18 months.

Feedback from the general monitoring and specific monitoring specified above, will be provided to the authorising officers and to the relevant services not less than once every 3 months. This feedback will also be sent to the Assistant Chief Executive (Corporate Governance) who is the single member of the Council's management team (CLT) whose responsibilities include ensuring that designated authorising officers meet the standards required by the Office of Surveillance Commissioners.

The Guidance and Procedure document, the procedure for the RIPA Central Record, and this Monitoring and Quality Control Procedure will be reviewed once every 18 months.

Appendix 4

Human Rights Act 1998

Human Rights Audit

Public Authority <i>(including full address)</i>	Leeds City Council, Civic Hall, Leeds LS1 1UR.		
Name & Job Title of Officer			
Full Address			
Contact Details			

DETAILS OF AUDIT
1. Describe the purpose of the surveillance.
2. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
3. The identities, where known, of those to be subject of the surveillance.
<ul style="list-style-type: none">• Name:• Address:• DOB:• Other information as appropriate:
4. Explain the information that it is desired to obtain as a result of the surveillance.

5. Identify on which ground in Article 8.2 of the Human Rights Act 1998 the surveillance is necessary. *Delete those that are inapplicable.*

- In the interests of national security;
- In the interests of public safety;
- In the interests of the economic well-being of the United Kingdom or the Leeds area;
- For the prevention of disorder or crime;
- For the protection of health or morals;
- For the protection of the rights and freedoms of others (including those of the Council);

6. Explain why this surveillance is necessary on the grounds you have identified.

7. **Supply details of any potential collateral intrusion and why the intrusion is unavoidable.**

Describe precautions you will take to minimise collateral intrusion.

8. Explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

Appendix 5

REGULATION OF INVESTIGATORY POWERS ACT 2000

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

INTERCEPTION AUDIT

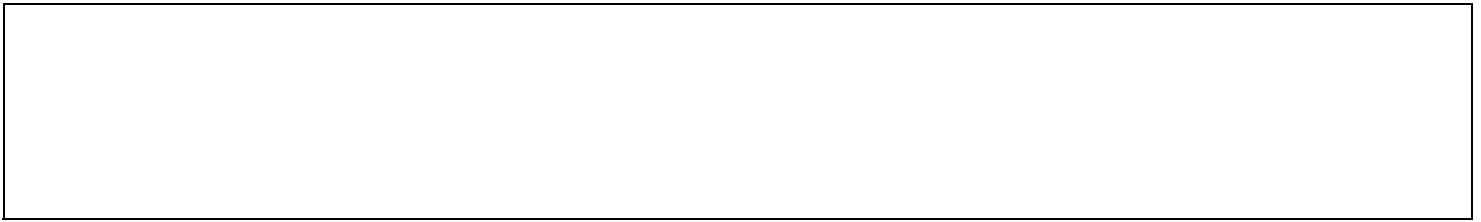
Public Authority <i>(including full address)</i>	Leeds City Council, Civic Hall, Leeds LS1 1UR
---	---

Name of Applicant		Directorate	
Full Address			
Contact Details			

Note this form should only be used where it is proposed to intercept a communication (such as e-mail, or phone calls) in the course of transmission via one of the Council's telecommunication systems.

For checking sent/received email in an email account, complete a Human Rights Audit.

For intercepting communications while being transmitted via a public system, seek advice from Legal, Licensing & Registration Services.



1. Grounds for interception

I confirm,

- ◆ This interception is done with the express or implied consent of the Council as system controller; and is (delete as inapplicable)
- ◆ for the monitoring or keeping a record of communications, in order to establish the existence of facts or
- ◆ to ascertain compliance with regulatory practices or procedures (e.g. Financial Procedure Rules, or the Disciplinary Procedures) or
- ◆ to ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties; or
- ◆ for the purpose of preventing or detecting crime; or
- ◆ for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system; or
- ◆ to secure the effective operation of the system, or
- ◆ monitoring communications to determine whether they are relevant to the Council's business;

I also confirm,

- ◆ the interception is for the monitoring or keeping a record of communications relevant to the Council's business (this effectively means anything relating to or taking place in the course of that business); and
- ◆ the telecommunication system is provided for use wholly or partly in connection with the Council's business; and
- ◆ the system controller has made all reasonable efforts to inform every person who may use the system in question that communications may be intercepted; and
- ◆ I am complying with data protection rules.

(Note - Interception can also be with "lawful authority" where

- ◆ it takes place in accordance with an interception warrant issued by the Secretary of State on certain specified statutory grounds, or
- ◆ where both parties consent to the interception or
- ◆ where the Council as sender consents, and where directed surveillance has been authorised.)

2. Explain why the Council can rely on the ground you have identified

3. Who is to be subject of the interception?

Name:

Address:

DOB:

Other information as appropriate

4. Describe the interception to be authorised

5. Explain what information is sought from the interception:

6. Specify anticipated start and duration

Dates:

7. Officer's Details

Name (print)

Tel No:

Job Title

Date

Signature

