CORPORATE SURVEILLANCE POLICY

TEST VALLEY
BOROUGH COUNCIL

October 2021

INDEX

APPENDICES

1 BACKGROUND

1.1 The Human Rights Act 1998 makes fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.

1.2 Section 6 of the Human Rights Act 1998 states that:

> "It is unlawful for a public authority to act in a way which is incompatible with a convention right."

1.3 Article 8 of the Convention on Human Rights provides that everyone has the right to respect for his private and family life, home and correspondence.

1.4 Council investigating officers may engage in covert surveillance from time to time, which interferes with a person's right under Article 8 of the Convention Rights to respect for a person's private and family life, home and correspondence.

1.5 Under the Convention of Human Rights a local authority may carry out this surveillance if it does so in accordance with the law and it is for the prevention or detection of crime or the prevention of disorder. In the case of the Council the powers are most frequently used to obtain evidence in relation to matters such as proposed serious fraud prosecutions and fly tipping. In addition authorisation may only be granted if the conditions set out in paragraphs (2) and (3) of Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended are met:

(2) The first condition is that the authorisation under section 28 is for the purpose of preventing or detecting conduct which—

(a) constitutes one or more criminal offences, or

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

(3) The second condition is that the criminal offence or one of the criminal offences referred to in the first condition is or would be—

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

(b) an offence under—

(i) section 146 of the Licensing Act 2003(a) (sale of alcohol to children);

(ii) section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);

(iii) section 147A of the Licensing Act 2003(b) (persistently selling alcohol to children);

(iv) section 7 of the Children and Young Persons Act 1933(c) (sale of tobacco etc. to persons under eighteen)"

1.5.1 The Regulation of Investigatory Powers Act 2000 (RIPA) ("the Act") establishes a regulatory framework by setting up an authorisation procedure in respect of covert surveillance. It imposes duties on public bodies, including local authorities, when carrying out investigations that involve covert surveillance and the conduct and use of covert human intelligence sources.

1.6 A policy has been prepared to set out the relevant responsibilities and to ensure that any covert surveillance or the conduct and use of covert human intelligence sources is conducted by officers in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA. Pursuance of this policy will assist the Council if it is required at any time to demonstrate that it has acted lawfully.

1.7 Appendix A outlines the procedure which should be followed.

2 DEFINITIONS:

Surveillance

2.1 Surveillance includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

2.2 All static observations that are covert (see below) count as either surveillance or the gathering of photographic intelligence and require proper application and authorisation under the rules.

2.3 **CCTV** surveillance **:**

2.3.1 **does not** require authorisation **if**:

- overt CCTV is being used; **and**
- special requests have not been made about the direction that it points.

2.3.2 **does** require authorisation **if:**

- overt CCTV is being used; and
- it is focussed on one or more targets.

This is the responsibility of the investigation manager.

Covert Surveillance

2.4 Covert surveillance is surveillance carried out in a manner calculated to ensure that subjects of it are unaware that it is or may be taking place. Covert surveillance involves the systematic surveillance of an individual. The everyday functions of law enforcement will not usually involve covert surveillance. This policy applies only to covert surveillance.

Directed Surveillance

2.5 Directed surveillance is the type of surveillance with which Council officers may be involved.

Directed surveillance is:

- covert **and**
- not intrusive (see below) **and**
- undertaken for the purposes of a specific investigation or a specific operation **and**
- carried out in such a manner which is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) **and**
- planned.

It cannot be an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Intrusive Surveillance

2.6 Intrusive surveillance involves the presence of an officer in a residence where activities are being investigated or in a private vehicle, or use of a surveillance device in such residence or vehicle, where the surveillance device, e.g. camera with a long lens or directional microphone, consistently provides information of the same quality and detail as would expect to be obtained from a devise in the residence or vehicle.

2.7 Council Officers **do not and cannot legally** engage in intrusive surveillance. There is no power under RIPA for this Council's officers to engage in intrusive surveillance.

The Conduct and Use of Covert Human Intelligence Sources ("CHIS")

2.8 The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

1. for the covert purpose of using the relationship to obtain information or to provide access to any information to another person **or**

2. to covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

2.9 "Use" includes inducing, asking or assisting a person to engage in the conduct of such a source, or to obtain information by means of the conduct of such a source.

2.10 Officers of the Council may on rare occasions engage in the conduct and use of covert human intelligence sources.

2.11 Where a covert human intelligence source is used his or her safety and welfare must be taken into account. This will require a risk assessment to be carried out and a record to be kept that gives details of matters such as his or her identity, the person having general oversight of him or her, how he or she was recruited, etc.

2.12 Proper arrangements must be established for the oversight and management of a CHIS.

2.12.1 In accordance with the Act both a “handler” and a “controller” must be appointed for each CHIS.

2.12.2 The “handler” will have day to day responsibility for dealing with the CHIS on behalf of the Council; including directing their day to day activities and recording the information they provide. The “handler” will have day to day responsibility for the CHIS’s security and welfare. Generally, a “handler” will be of a rank or position below the Authorising Officer.

2.12.3 The “controller” will be responsible for the management and supervision of the “handler” and general oversight of the use made of the CHIS.

2.12.4 The handler is responsible for bringing to the attention of the controller any concerns about the personal circumstances of the CHIS that may affect the validity of the current risk assessment, the conduct of the CHIS and/or the health and safety of the CHIS.

2.12.5 As described above, the safety and welfare of the CHIS must be taken into account and the Authorising Officer must carry out a Risk Assessment prior to authorisation. The Assessment must be updated to take account of any developments during the course of deployment and post-deployment. This includes consideration of and mitigation against any risk of the identity of the CHIS being revealed both in the short and long-term e.g. in future court proceedings. The Council should attempt to protect the identity of the CHIS by all lawful means.

2.12.6 Extreme care must be taken to safeguard information obtained by a CHIS. This information should be retained for no longer than is necessary and in any event in accordance with the Council’s Retention Policies and then confidentially destroyed. Material identifying a specific CHIS should be handled as highly sensitive and the minimum number of persons possible should have access to it. Copying of material obtained via CHIS (or any part of it) should be minimised to the barest extent necessary. Physical material must be stored so as to prevent unauthorised access to it and material stored on IT systems should similarly be stored to avoid unauthorised access.

2.12.7 The Regulation of Investigatory Powers (Source Records) Regulations 2000 set out a list of matters which **must** be included in the records relating to each CHIS which comprise:

a) the identity of the CHIS;

b) the identity, where known, used by the CHIS;

c) details of any relevant investigating authority other than the Council;

d) the means by which the CHIS is referred to within each relevant investigating authority;

e) any other significant information connected with the security and welfare of the source;

f) any confirmation made by the authorising (including authorisation on review) officer that the information in d) above has been considered and that any identified risks for the security and welfare of the CHIS have been properly explained to and understood by the CHIS

g) the date when, and the circumstances in which the CHIS was recruited;

h) the identities of the persons appointed as “handler”, “ controller” and the person responsible for maintaining a record of the use made of the CHIS;

i) the periods during which those persons have discharged those responsibilities;

j) the tasks given to the CHIS and the demands made of hi or her in relation to his activities as a source;

k) all contacts or communications between the CHIS and the Council (or anyone acting for the Council) or any other investigating authority;

l) the information obtained by the Council and any other investigating authority via the CHIS;

m) any sharing of the information by the Council of the information obtained by the CHIS; and

n) every payment, benefit, reward or offer of payment, benefit or reward made by the Council or any other investigating authority in respect of the CHIS’s activities.

2.12.8 This information should be retained in accordance with the Council’s retention policy (currently current year plus 6 for adult CHIS).

2.12.9 Where an officer is considering the use of a covert human intelligence source he or she must consult with the Head of Legal & Democratic Services or one of her staff beforehand.

Collateral Intrusion

2.13 Collateral intrusion is where there is a risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation. All applications for authorisation should include an assessment of the risk of collateral intrusion to enable the Authorising Officer to take account of it in his/her proportionality assessment of the overall actions proposed. Measures should be taken to limit collateral intrusion.

Confidential information

2.14 Confidential information consists of matters subject to legal privilege, confidential or spiritual personal information, or confidential journalistic material, eg information held at premises used by lawyers or for any form of medical or professional counselling or therapy.

Communications Data

2.16 Whilst not governed by the RIPA authorisation process it is considered appropriate to include reference to the acquisition of communications data in this policy. Communications data means for telecommunications, the subscriber's detail, the names addresses and numbers of those contacted and web addresses visited and, for postal communications, anything written on the outside of the items. It does not include the content of any such communication.

2.17 Occasionally Council Officers may need to obtain such data in connection with investigations in relation to preventing or detecting crime or preventing disorder or some examples would be fly tipping by a lorry with a telephone number on its side or an allegation that a benefit claimant is carrying out hairdressing and has a card in the local newsagent with a telephone number on. The Council may be able to find out the name and address of the person in whose name the telephone is registered.

3 AUTHORISATIONS

3.1 It is the Council's position that authorisation is required for the use of directed surveillance and for the conduct and use of covert human intelligence sources where the criteria for applying for authorisation are met (i.e. relating to an offence punishable by a maximum term of six months' imprisonment or more or relating the sale of alcohol, tobacco or nicotine products to minors). In the case of a CHIS, authority should be sought for both (a) the use of a CHIS and (b) the task which they are to carry out.

Authorisation

3.2 Each officer who undertakes investigations on behalf of the Council **must** seek authorisation in **writing** for any directed surveillance or for the conduct and use of any covert human intelligence sources from an Authorising Officer which must be then approved by a Justice of the Peace to become effective.

Duration

3.3 An adult CHIS authorisation will last for twelve months from the date of Magistrate approval unless renewed or cancelled.

3.4 An authorisation for Directed Surveillance will last for three months from the date of Magistrate approval.

Renewal

3.5 An authorisation may be renewed (more than once if necessary and proportionate) **before** it ceases to have effect if an authorising officer considers it necessary for the authorisation to continue. The renewal must be approved by a Justice of the Peace before it can take effect in the same way as an original authorisation must be. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary and proportionate a renewal can be made more than once provided a review of the authorisation has been carried out and the criteria for authorisation continue to be met.

The Authorising Officer

3.6 Surveillance under RIPA, which is **not** likely to result in the acquisition of confidential information requires authorisation from **1 authorising officer** listed in Appendix B

3.7 If the surveillance is likely to result in the acquisition of **confidential information or relates to juvenile or vulnerable CHIS** authorisation must be obtained from **1 authorising officer** listed in Appendix B, namely the Chief Executive or in his absence the person authorised to act as Chief Executive in his place.

3.8 The power to authorise surveillance under RIPA cannot be delegated to anyone else.

Judicial Authority

3.9 Once the authorising officer has authorised the directed surveillance or CHIS an application must be made to a Justice of the Peace for judicial approval. The authority does not take effect and the surveillance or use of a CHIS cannot be undertaken until it has been approved by a Justice of the Peace.

3.10 All applications for judicial authority will be made by the Head of Legal & Democratic Services or a lawyer within her Service. It will be the responsibility of the officer wishing to carry out the surveillance to provide the Head of Legal & Democratic Services with such information and statements as is necessary to make the application.

4. STANDARD FORMS

4.1 The authorisation must be sought using the Part II standard forms which can be found in the RIPA part of the Legal section under Business Support on the Council's Intranet.

4.2 Applications to the Court will be completed using the relevant application forms and draft order appended to the Home Office guidance: "Protection from Freedoms Act 2012- changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)" October 2012.

5. USE OF THE INTERNET AND SOCIAL NETWORKING SITES FOR INVESTIGATIONS OR INFORMATION GATHERING

5.1 With the ever-increasing and wide ranging amount of information available on-line and in particular social networking sites, the Council will often have recourse to the internet in the course of investigations. Much of the on-line information can be accessed without concern.

5.2 However, individuals' legitimate expectations of privacy will depend on the circumstances. Someone who posts on a social media site in the full knowledge that it can be seen by the world is of course less likely to have a reasonable expectation of privacy however that does not mean that no authorisation is required. The rationale being that whilst such a person can reasonably expect the world at large to be able to view content, their intention when making that information available was not for it to be used for covert investigative activity.

5.3 In his annual report, the Chief Surveillance Commissioner says "*Perhaps more than ever, public authorities now make use of the wide availability of details about individuals, groups and locations that are provided on social networking sites and a myriad of other means of open communication between people using the internet and their mobile communication devices. I repeat my view that just because this material is out in the open, it does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA <u>and this includes repetitive viewing of what are deemed to be "open source" sites for the purpose if intelligence gathering and data collection".</u>*

5.4 Simply taking an initial look at those open-source sites is unlikely to engage privacy concerns but where repeated or persistent viewing of the sites take place and/or where information from the site is recorded or collected then we are in the territory where an application for directed surveillance may be necessary. Please seek advice from the legal department.

5.5 There is no formal definition of what is "persistent" or "repeated" and it will vary on a case by case basis. Viewing a profile or site as few as three or four times may be sufficient. Individuals' legitimate expectation of privacy may also depend to a degree on application of any privacy settings. You must seek advice from Legal Services before proceeding if repeated or systematic viewing and/or recording of information from or monitoring of social media sites is contemplated and obtain advice on whether an application for authorisation is possible and/or necessary and how to proceed generally.

5.6 The situation may arise whereby a person acting for the Council may use social media platforms to interact with third parties.

5.7 Where a person acting on behalf of the Council intends to engage with others on line without disclosing their identity or under an assumed identity, a CHIS authorisation is likely to be needed (provided the other criteria are met). It is expected that the need for this type of activity – where there is a degree of interaction with the subject - will only be required or appropriate in exceptional circumstances and advice must be sought from Legal Services before

commencing it. The Authorising Officer must satisfy themselves that they have full and effective oversight of the on-line surveillance from preparation to post-completion.

5.8 In such circumstances if it is intended that more than one individual or officer will share the same on-line persona, each officer should be clearly identifiable within the authorisation for that particular operation specifying the requirements of each officer and carrying out a risk assessment for each individual or officer.

5.9 Any assumed identities should be listed in a register prepared for the purpose and centrally recorded.

6. ROLE OF THE AUTHORISING OFFICER

6.1 The authorising officer must satisfy themselves that authorisation is necessary and proportionate. The authorising officer must consider the relevant Code of Practice. These can be found in the RIPA part of the Legal section under Business Support on the Council's Intranet

Necessary

6.2 An authorisation under RIPA may be granted by an authorising officer if he believes that the authorisation is **necessary** for the purpose of preventing or detecting crime or of preventing disorder (subject to the caveat below). Authorisation cannot be given for any other reason. As set out in paragraph 1.5 above, authorisation may only be granted in relation to crimes which are punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment or are related to the underage sale of alcohol, tobacco or nicotine inhaling products. An authorisation may only be granted in relation to prevention of disorder if it involves conduct constituting a criminal offence or offences punishable by a maximum term of at least six months imprisonment. Disorder falling short of this criteria does not fall within the scope of RIPA authorisation.

In the case of a CHIS, authorisation must not be granted unless the authorising officer believes that arrangements are in place ensuring that there is at all times a person appointed with responsibility for maintaining a record of the use made of the CHIS.

Proportionate

6.3 If the surveillance activities are necessary on the above grounds (see 5.2) the authorising officer must also believe that the surveillance activities are "proportionate" to what is sought to be achieved by carrying them out. The activities will not be proportionate if the activities are excessive in the circumstances of the case or if the information could be obtained by a less intrusive means.

6.4 Paragraph 3.6 of the 2010 Home Office Code of Practice for Covert Surveillance and Property Interference provides:

3.6 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;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and 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.

Risk of Collateral Intrusion

6.5 Collateral intrusion is where there is a risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

6.6 The authorising officer must consider the risk of collateral intrusion and describe in the authorisation form what will be done for any that is considered likely.

6.7 The person carrying out the surveillance must inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The authorising officer must then consider whether the authorisation should continue.

Confidential Material

6.8 "Confidential information" for the purposes of RIPA consists of:
(a) matters subject to legal privilege; and
(b) confidential *personal* information is information held in confidence (whether expressly or implied) concerning an individual (living or dead) who can be identified from it and the material relates to the person's physical or mental health or to spiritual counselling.

6.9 If the directed surveillance or the conduct and use of any covert human intelligence sources is likely to result in the acquisition of confidential material the authorising officer, when considering the application, must assess how likely it is that confidential material will be acquired.

6.10 Applications in which the directed surveillance is likely to result in the acquisition of confidential material will only be considered in **exceptional and compelling circumstances** with full regard to the proportionality issues this raises.

6.11 Where the likely consequence of the directed surveillance would be for any person to acquire knowledge of confidential material, the authorising officer must be the Chief Executive or in his absence, the person authorised to act in his place.

6.12 The authorising officer must give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

6.13 The Code of Practice issued under the Act must be taken into account and is reflected in this policy.

7. ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The application officer must make enquiries of other public authorities whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

8. DATA PROTECTION

Authorising officers must ensure that there is compliance with the appropriate data protection requirements and the Council's policies and practices in the handling and storage of material.

9. DESTRUCTION OF WHOLLY UNRELATED MATERIAL

9.1 Where material is obtained by directed surveillance which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, it must be destroyed immediately, but not if civil or criminal proceedings are contemplated. Where court proceedings are contemplated, all material is potentially relevant and must be retained and will be disclosed in the usual way.

9.2 The applicant officer must, if appropriate, seek authority to destroy any wholly unrelated material where there will be no court proceedings.

10. DESTRUCTION AND RETENTION OF CONFIDENTIAL MATERIAL

10.1 Investigating officers must be alert to anything that may be confidential material. Where there is doubt, advice must be sought from the Head of Legal & Democratic Services before further dissemination of the material takes place.

10.2 Confidential material must not be retained or copied unless it is necessary for a specified purpose. Details of any that is retained or copied must be given to the Monitoring Officer who will make a note only for the central record

10.3 Confidential material must only be disseminated where an appropriate officer (having sought advice from the Head of Legal & Democratic Services) is satisfied that it is necessary for a specific purpose.

10.4 A clear warning stating that the information is confidential in nature must accompany the confidential information, which is retained or disseminated. Reasonable steps must be taken to prevent the material from becoming available, or its contents being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

10.5 Confidential material must be destroyed as soon as it is no longer necessary to retain if for a specified purpose.

11. TRAINING

Authorising officers and an investigating Council officer must undertake appropriate training before carrying out any investigation under RIPA. This is to ensure that investigations and operations that he/she carries out will be conducted lawfully. The training will be carried out by Officers from within Legal Services or external providers.

12. REVIEWS

12.1 Regular reviews of authorisations must be undertaken to assess the need for surveillance to continue. The results of the review must be recorded on the central record of authorisations.

12.2 The authorising officer shall determine how often a review should take place. However frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information.

12.3 This review will take into account any subsequent action by the Council arising from the produce of the surveillance, which may be in the form of the issue of notices, orders, or determinations by the Council, or the bringing of criminal or civil proceedings, or any other action.

13. CANCELLATIONS

13.1 An authorising officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply e.g. the aims have been met; risks have changed and authorisation is no longer appropriate.

13.2 The authorising officer must inform those involved in the surveillance to stop all surveillance of the subject(s).

14. ACQUISITION OF COMMUNICATIONS DATA

14.1 Authorisation is required for obtaining communications data and it can only be obtained through an authorised Single Point of Contact (SPOC).

14.2 The Council subscribes to the National Anti-Fraud Network (NAFN) which acts as the channel through which any applications for communications data are made.

Application Procedure

14.3 Each officer wishing to obtain communications data must complete the required form that can be found online on the NAFN website.

14.4 NAFN will then notify the Council’s SPOC.

14.5 NAFN will then review the application and either authorise or reject it or may suggest a re-work. If authorised, the NAFN will follow its processes and obtain the information from the service provider in question.

15. RECORD OF DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE AUTHORISATIONS

15.1 The written records shall be confidential and shall be kept accurately and conveniently. Each authorisation must be allocated its own Unique Reference Number ("URN") which should be used throughout the life of the authorisation and applied to documentation associated with it.

Central Record of All Authorisations

15.2 A central record of all authorised surveillance will be kept by the Head of Legal & Democratic Services. The central record must be readily available for inspection on request by the Office of Surveillance Commissioners.

Other Records

15.3 The following documents need not form part of the centrally retrievable record. Each service must keep a written record of each of the authorisations made by an authorising officer for the service:

1. a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of approval given by the authorising officer;

2. a record of the period over which the surveillance has taken place

3. the frequency of the reviews prescribed by the authorising officer

4. a record of the result of each review

5. a copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested

6. the date and time any instruction was given by the authorising officer, including cancellation of such authorisation

16 DISCLOSURE

The information obtained during the course of an investigation that might be relevant to that or another investigation or pending or future civil or criminal proceedings must not be destroyed.

17 SENIOR RESPONSIBLE OFFICER

17.1 The Council's Senior Responsible Officer ("SRO") is shown in Appendix B.

17.2 The SRO is responsible for:

- The integrity of the process in place within the public authority for the management of Directed Surveillance and CHIS

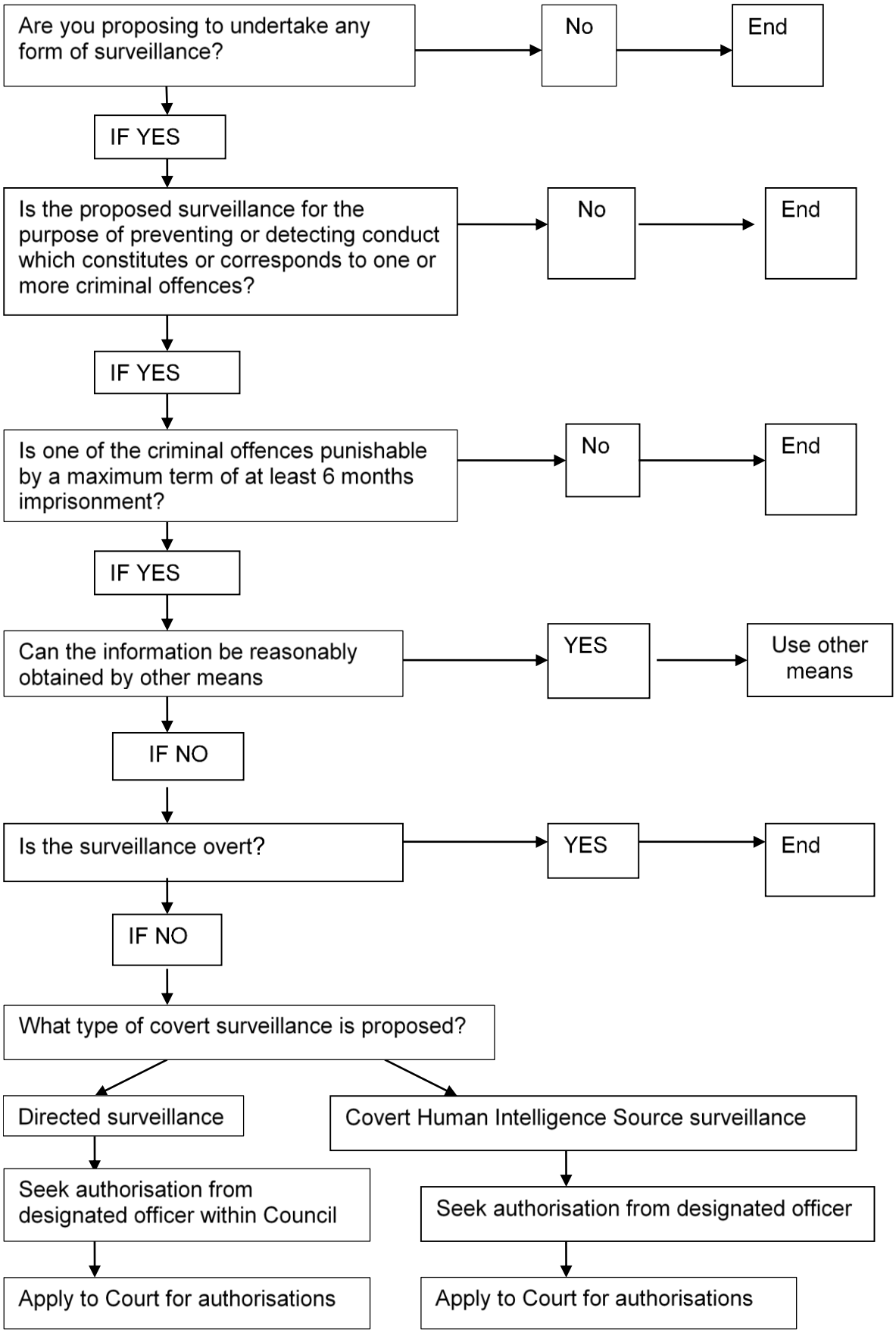
- Compliance with Part 2 of the Act and the Codes of Practice

- Oversight of the reporting of errors to the relevant Oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

- Engagement with the Office of Surveillance Commissioners Inspectors when they conduct their inspections, where applicable and

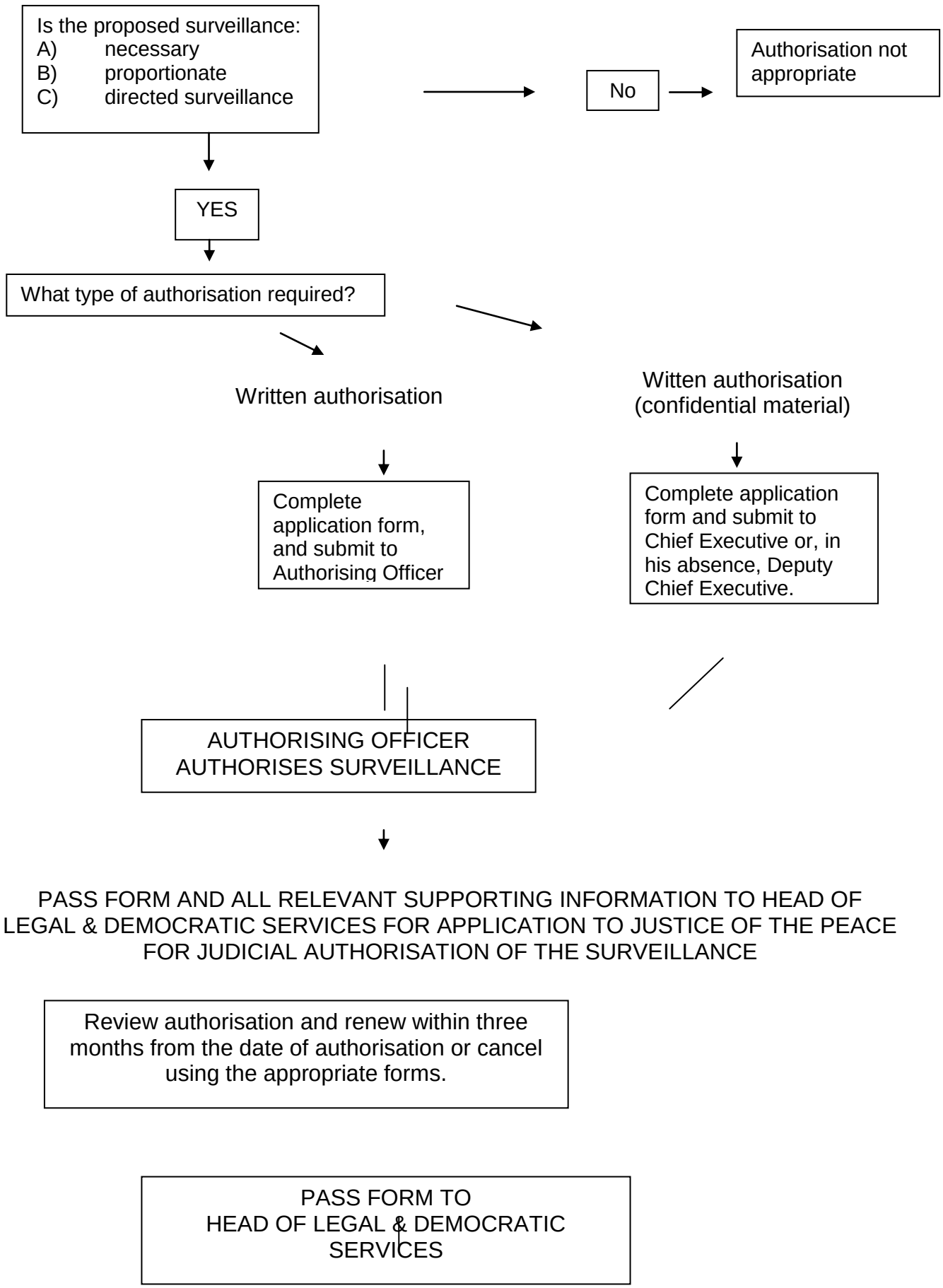
- Where necessary, oversight of the implementation of post-inspections plans approved by the relevant Oversight Commissioner

PROCESS DECISION MAP FOR COVERT SURVEILLANCE



APPENDIX A2

AUTHORISATION OF DIRECTED SURVEILLANCE PROCESS MAP



APPENDIX B

REGULATION OF INVESTIGATORY POWERS ACT 2000
List of Authorised Posts, Designated Persons and Single Point of Contact

Authorised Posts

List of persons empowered to authorise surveillance which is not likely to result in the acquisition of confidential information for the purpose of obtaining communications data

Surveillance, which is not likely to result in the acquisition of confidential information, requires an authorised officer to grant the authorisation.

NAME	POST	SERVICE	EXTN
Phil Turner	Head of Housing Health & Communities	Housing Health & Communities	8601
Carl Whatley	Head of Finance and Revenues Services	Finance & Revenues	8540
Paul Wykes	Head of Environmental Services	Environmental Services	8351

NB. The power to authorise surveillance under RIPA cannot be delegated to anyone else.

List of persons empowered to authorise surveillance which is likely to result in the acquisition of confidential information

Surveillance which is likely to result in the acquisition of confidential information or which authorises use of a juvenile or vulnerable CHIS requires authorisation from:

Authorised Post	Name
Chief Executive	Andrew Ferrier

or in his absence

Deputy Chief Executive	Carol Moore

NB. The power to authorise surveillance under RIPA cannot be delegated to anyone else.

Designated Persons

List of persons empowered to authorise the council's Single Point of Contact to apply to the National Anti-Fraud Network for Communications Details.

NAME	POST	SERVICE	EXTN
Phil Turner	Head of Housing Health & Communities	Housing Health & Communities	8544
Carl Whatley	Head of Finance and Revenues Services	Finance & Revenues	8540
Paul Jackson	Head of Planning & Building	Planning & Building	8186
Paul Wykes	Head of Environmental Services	Environmental Services	8351

Senior Responsible Officer

Deputy Chief Executive	Carol Moore