



**Written Statement of
Operational Procedure for
West Somerset Council's policy in
respect of lawful surveillance
activity to comply with the:**

**REGULATION OF
INVESTIGATORY POWERS
ACT 2000**

Amended January 2012

INDEX

N o	Topic	Page No
1	Introduction	2
2	Definition of terms used	2-5
3	Undertaking Covert Surveillance	5-6
4	Authorisation Officer	6
5	Collateral Intrusion	6
6	Risk Assessment	6
7	Health & Safety	6
8	Procedure for Directed Surveillance	7
	8.1 The Grant of the Authorisation	7
	8.2 Information to be provided in the application for Authorisation	7
	8.3 Duration of the Authorisation	8
	8.4 Review of the Authorisation	8
	8.5 Renewal of the Authorisation	8
	8.6 Cancellation of the Authorisation	9
	8.7 Ceasing of Surveillance Activity	9
9	Use of a Covert Human Intelligence Source (CHIS)	9
	9.1 Introduction	9
	9.2 Definition of a CHIS	10
	9.3 Authorisation	11
	9.4 Management of CHIS	11-12
	9.5 Specific CHIS Records	12
	9.6 Group Manager Records	12
10	Procedure for Monitoring RIPA and Oversight	12
	10.1 Senior Responsible Officer	12
	10.2 Oversight Procedures	12
	10.3 Member Review	13
11	Record Keeping	13
	11.1 Completed Authorisation Applications	13
	11.2 Central Register of Authorisations	13
	11.3 SRO Monitoring	13
	11.4 Service Team Records	13
12	Procedure for the Use of Surveillance Equipment	14
13	Authorisation Restrictions	14
14	Processing Forms	14
15	Procedure for Data Retention	14
	15.1 Retention of Authorisation Forms	14-15
	15.2 Confidential Information	15
16	Data Protection	15

17	Complaints handling	15
17.1	Independent Tribunal	15
17.2	West Somerset District Council's Surveillance Complaints Procedure	15
18	Conclusion	15
19	Referencing	16
20	Appendices Nos 1 to 7 – Including Home Office Forms (version 2008)	17-35

1 Introduction

- 1.1 On the 25 September 2000 the Regulation of Investigatory Powers Act was brought in to force in England and Wales. The purpose of the Act was to ensure that all public authorities were able to carry out covert surveillance on a statutory basis without breaching The Human Rights Act 1998, Article 8 – the right to privacy.
- 1.2 Covert surveillance enables public bodies to detect and/or prevent a crime that has or is about to be committed and also to obtain information about an individual or organisation's activities.
- 1.3 West Somerset District Council ("the Council") is therefore committed to implementing the Act to ensure that an investigation is carried out properly and that the investigation is necessary and proportionate to the alleged offence.
- 1.4 The purpose of this policy is to ensure that the proper procedures are in place in order to carry out covert surveillance; to ensure an individual's right to privacy is not breached; that proper authorisation is obtained for covert surveillance; that the proper procedures have been followed; and that covert surveillance is considered as a last resort having exhausted all other avenues.
- 1.5 The Council's policy is therefore implemented and followed in accordance with the Regulation of the Investigatory Powers Act 2000.

2 Definitions

- 2.1 RIPA 2000** RIPA 2000 stands for the Regulation of Investigatory Powers Act 2000.
- 2.2 Authorisation Officer (AO)** An Authorisation Officer is an employee of the Council and the following employees are nominated as AOs:
 Chief Executive
 Corporate Director
 Group Manager for Housing and Community
 Group Manager for Central Support
 Principal Benefit Officer
- 2.3 Investigating Officer (IO)** An IO is an Officer within the Council who is involved in undertaking a specific investigation or operation.
- 2.4 Covert Surveillance** Covert Surveillance is either Directed Surveillance or conducting surveillance with the use of a Covert Human Intelligence Source. Covert Surveillance can be intrusive and is likely to obtain private information about a person. It should be emphasised, however, that the Council cannot undertake intrusive surveillance.

2.5 Directed Surveillance	Directed Surveillance is defined under section 26(2) of RIPA. Directed Surveillance is as follows: <ul style="list-style-type: none"> (a) for the purposes of a specific investigation or a specific operation; (b) in such a manner as 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 (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.
2.6 CHIS	CHIS is defined as a Covert Human Intelligence Source and is subject to statutory control under section 29 of the RIPA Act 2000. A CHIS is a person who is required to establish or maintain a personal or other relationship with someone to obtain information in order to assist an investigation. Other relationship can include professional, business or working relationship. <p>A CHIS is therefore the person who acts covertly and passes information to the Designated Handler or to a controller with oversight of the use made of the CHIS as set out in s.29(5)(b) of the RIPA Act 2000.</p>
2.7 Designated Handler	A Designated Handler is responsible for directing the day to day activities of the CHIS as well as the security and welfare of the CHIS and will usually be of a rank below that of the AO.
2.8 Intrusive Surveillance	Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in this vehicle or is carried out by means of a surveillance device.
2.9 Private Information	Private Information includes any information relating to a person's private or family life. This includes the right to establish and develop relationships with other human beings and activities that are of a business or professional nature.
2.10 Private Vehicles	Private Vehicles are subject to RIPA where any vehicle is used primarily for the private purposes of the person who owns it or for a person otherwise having the right to use it.
2.11 Residential Premises	Residential Premises are subject to RIPA, where premises are being occupied or used by any person, however temporarily, for residential

purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used).

- 2.12 Necessity** Necessity requires that Directed Surveillance take place when one or more of the statutory grounds set out in s.28(3) RIPA 2000 are met. For the purposes of this policy the only statutory ground applicable to the Council is for the purpose of preventing or detecting crime or of preventing disorder.
- 2.13 Proportionality** The balance of the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.
- 2.14 Collateral Intrusion** Collateral intrusion is where surveillance **indirectly intrudes on to the privacy of individuals** who are not the direct subject of the surveillance i.e. where innocent bystanders are observed in the course of a covert surveillance operation - children are included within this definition.
- 2.15 Surveillance** Surveillance includes:-
a) monitoring, observing or listening to persons, their movements, their conversations or other activities or communication;
b) recording anything monitored, observed or listened to in the course of surveillance; and
c) surveillance by or with the assistance of a surveillance device.
- 2.16 Surveillance Device** Surveillance Device means any apparatus designed or adapted for use in surveillance.
- 2.17 Civil & Criminal Proceedings** Civil proceedings means any proceedings in or before any court or tribunal that are not criminal proceedings;
Criminal, in relation to any proceedings or prosecution in which a criminal sanction may be imposed.
- 2.18 Public Authority** Public Authority means any public authority within the meaning of section 6 of the Human Rights Act 1998 (acts of public authorities) other than a court or tribunal.
- 2.19 Legal privilege** Legal privilege is defined as confidential information, which is obtained in relation to the surveillance being undertaken. This can include oral and written communications between a recognised legal advisor and their client.
- 2.20 Confidential Information** Confidential information, whilst having no special protection under RIPA 2000, consists of communications subject to Legal privilege, communications between a Member of Parliament and another person on constituency matters (Confidential Constituent Information), Confidential

Personal Information or Confidential Journalistic Information. Member of Parliament includes references to members of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly

Confidential Personal Information is information, written and orally, held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead).

Confidential Journalistic Material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence as well as communications resulting in such information being acquired

- 2.21 Human Rights Act** Human Rights Act - the Human Rights Act 1998, Article 8 provides protection to an individual's right to privacy. Section 6 of the Act states that it is unlawful for a public authority to act in a way that is incompatible with a Convention right.
- 2.22 Senior Responsible Officer** The Senior Responsible Officer (SRO) shall be the Corporate Director who shall be responsible for ensuring the compliance of the Council with Part II of RIPA 2000 in accordance with paragraph 10 below
- 2.23 Code of Practice (Surveillance)** The revised Home Office Code of Practice on Covert Surveillance and Property Interference (2010)

3 Undertaking Covert Surveillance

- 3.1** Under Part II of the Regulation of Investigatory Powers Act 2000 public authorities are authorised to undertake Covert Surveillance as defined in paragraph 2.4.
- 3.2** Directed Surveillance is defined under Section 26(2) of RIPA 2000, as being covert, must not be intrusive and is undertaken for the following purposes:-
 - 3.2.1 as a specific investigation or specific operation,
 - 3.2.2 if private information about a person may be obtained,
 - 3.2.3 otherwise than as an immediate response to events, in circumstances where it would not have been reasonably practical for an authorisation to be obtained.
- 3.3** The use of material, which is obtained through Covert Surveillance can be used as evidence at criminal and civil proceedings.
- 3.4** Any material evidence obtained through the course of the surveillance is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigation Act 1996.

4 Authorisation Officer

- 4.1** Part II of the RIPA Act 2000 provides lawful authority for a public authority to carry out surveillance.

- 4.2 An Authorisation Officer (AO) will be responsible for any surveillance either through an investigation or operation to be carried out, or for the use of a CHIS.
- 4.3 The AO will be the Chief Executive. In the event of the AO being unavailable one of the officers nominated under paragraph 2.2 may act as Deputy AO and an Investigating Officer may choose whichever of the listed AOs they consider appropriate in the circumstances.
- 4.4 Where knowledge of confidential information is acquired or is likely to be acquired, the AO will always be the Chief Executive.
- 4.5 An AO should not normally be responsible for authorising operations in which they are directly involved. Where it is unavoidable or where it is necessary to act urgently or for security reasons, the Central Record of Authorisations should highlight this.
- 4.7 It is an AO's responsibility to ensure that the forms have been completed properly.
- 4.8 It is an AO's responsibility to ensure that the authorisation is necessary and proportionate. If necessary the AO must challenge the Officer as to the use of the authorisation if the AO considers:
- 4.8.1 that the correct procedures have not been followed properly,
 - 4.8.2 that an alternative method of obtaining the necessary information can be used,
 - 4.8.3 that a risk assessment has not been properly completed.

5. Collateral Intrusion

- 5.1 The AO must take into account the risk of intrusion into the privacy of persons other than those who are direct subjects of the operational investigation, such as innocent bystanders.
- 5.2 Measures must be taken wherever practical to avoid unnecessary intrusion into the lives of those not directly involved in the operation.

6. Risk Assessment

The Service Team Leader has responsibility for risk assessment for their particular Service Team.

7. Health & Safety

Any form of Covert Surveillance, must be in accordance with the Council's Health & Safety Corporate Policy, which complies with the Health & Safety at Work Act 1974.

8. Procedure on Directed Surveillance

8.1 The Grant of the Authorisation

- 8.1.1 In accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Source) Order 2010 the only ground for which an authorisation for Directed Surveillance may be sought is the purpose of preventing or detecting crime, or of preventing disorder.
- 8.1.2 When considering a request for Directed Surveillance, the AO must ensure that the authorisation is necessary for the **purpose of preventing or detecting crime, or of preventing disorder.**

- 8.1.2 The AO must believe that the surveillance is Necessary and proportionate in order for this to be achieved.
- 8.1.3 Proportionality must be considered. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. The elements of proportionality as set out in paragraph 3.6 of the Code of Practice (Surveillance) and paragraph 105 of the OSC Procedures and Guidance 2010 should be considered.
- 8.1.4 The AO must give the authorisation in writing on the application form. Please see Appendix 4. This should include an explanation of the reasons why the authorisation is considered necessary and proportionate, relying on the considerations made in accordance with paragraph 8.1.3 above.
- 8.1.5 If an urgent case requires an authorisation then it need not be in writing. However, as soon as practically possible the authorisation must be recorded in writing on the application form.

8.2 Information to be provided in the application for Authorisation

8.2.1 A written application for authorisation for Directed Surveillance must: -

- describe the conduct to be authorised;
- the purpose of the investigation or operation.

8.2.2 The application must include the following:-

- the reasons why the authorisation is sought;
- the grounds of the relevant operation or investigation e.g. for the purposes of preventing or detecting crime;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities where known of those to be the subject of surveillance;
- an explanation of the information which is to be obtained as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required for the surveillance or the recommendation of the level of authority required;
- a subsequent record of whether authority was given or refused, by whom and the date and time.

8.2.3 In urgent cases where oral authorisation has been obtained, when the written authorisation is completed this should include the following:-

- the reasons why the AO or the officer entitled to act in urgent cases considered the case so urgent, that an oral, instead of a written authorisation was given,
- the reasons why it was not reasonably practical for the application to be considered by an AO.

8.3 Duration of authorisation

- 8.3.1 A written authorisation will cease to have effect at the end of the 3 month period from when it was obtained.
- 8.3.2 An urgent oral authorisation or written authorisation which has been obtained in an urgent case, will cease to have effect after 72 hours from when it was obtained.

8.4 Reviews of Authorisation

- 8.4.1 Regular reviews of the authorisation must be undertaken to assess the need for the surveillance to continue.
- 8.4.2 Reviews must be undertaken in the following time periods:-
- ordinary written authorisations - reviews should be undertaken as required by each operation. A review date should be decided by the Authorising Officer and recorded on the form when authorisation is agreed. At least once a month is suggested.
 - a review of an oral urgent authorisation must be taken 24 hours after the authorisation was obtained,
 - The review of any authorisation must be completed on the review form. Please see Appendix 7.

8.5 Renewals of Authorisation

- 8.5.1 If an authorisation ceases to have effect, and the AO considers it necessary for the authorisation to continue for the purpose for which it was given, the AO may renew it as follows: -

- for an ordinary authorisation, renewed for a period up to 3 months.

In such circumstance, a renewal must be granted before the original authorisation ceases to have effect.

- 8.5.2 All applications for renewal of authorisations for Directed Surveillance should include:-

- whether this is the first renewal,
- every occasion on which the authorisation has been renewed previously,
- significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation,
- the reasons why it is necessary to continue with the Directed Surveillance,
- the content and value to the investigation or operation of the information so far obtained by the surveillance and the results of regular reviews of the investigation operation.

8.5.3 Authorisations may be renewed more than once and must be recorded as part of the central record of authorisations.

8.5.4 The renewal form should be completed when applying for renewal of an authorisation. Please see Appendix 5.

8.6 Cancellation of Authorisation

8.6.1 The AO who granted or last renewed the authorisation must cancel that authorisation, if s/he is satisfied that the surveillance no longer meets the criteria upon which it was authorised.

8.6.2 Where the AO is no longer available this duty will fall on the person who is taking over the role of AO or any other designated AO within the Council.

8.6.3 The cancellation of surveillance must be completed on the cancellation form which should record the following information:-

- Date and times that the surveillance took place (if at all)
- Date and time when the order to cease the activity was made
- The reason(s) for the cancellation
- Directions for the management of product
- The value of the surveillance.

Please see Appendix 6.

8.7 Ceasing of Surveillance Activity

8.7.1 As soon as the decision is taken that Directed Surveillance should be discontinued, instruction must be given to all those involved in the specific investigation or specific operation to stop all surveillance of the subject(s).

8.7.2 The date and time when an instruction was given to cease surveillance activity must be recorded in the central record of authorisations and the notification of cancellation where relevant.

9 Procedure on Covert Human Intelligence Sources (CHIS)

9.1 Introduction

The Council do not propose to initiate involvement within this area of the Act. Nevertheless, the Council does have the power to do so and, in the unlikely event that such a source presents him/herself unexpectedly, the Council will manage the source in accordance with RIPA, the current Code of Practice and will comply with this paragraph 9.

9.2 Definition of a CHIS

9.2.1 Covert Human Intelligence Source (CHIS) is defined under Section 26(8)(a-c) of RIPA 2000, where information is obtained to assist in the investigation of a crime or to prevent a crime, by a CHIS who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything, which is:

- covertly using a 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.

9.2.2 Members of public volunteering information as part of their normal civic duties are not regarded as a CHIS.

9.3 Authorisation

9.3.1 The Council is only likely to use a CHIS under very exceptional circumstances, and advice should be sought from the Corporate Director before any authorisation is applied for or granted.

9.3.2 Before the AO grants authorisation to use a CHIS, in consultation with the Corporate Director, the Corporate Director should consult with the District Commander within the Police Force Area, which is the Avon & Somerset Constabulary, to ensure that no conflict arises within the area of where the CHIS is deployed but this will not include disclosure of the identity of the CHIS.

9.3.3 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked with an assignment. An authorisation can cover, in broad terms, the nature of the CHIS's task and only if this changes significantly would a new authorisation be needed.

9.3.4 If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation.

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information.
- **Use** of a CHIS = Inducing, asking, or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

9.3.5 In the event of the Council deploying a CHIS they must take into account the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS the Corporate Director shall ensure that a risk assessment is carried out and consideration given to ongoing security, welfare, and management of any requirement to disclose information (including that tending to reveal the existence of the CHIS).

9.3.6 When authorising the conduct or use of a CHIS, the AO must also:

9.3.6.1 be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;

9.3.6.2 consider the likely degree of intrusion for all those potentially affected;

9.3.6.3 consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and

9.3.6.4 ensure that records contain the required particulars set out in 9.5 and that these are not available except on a 'need to know' basis.

9.3.7 If a juvenile or vulnerable individual is contemplated as a CHIS the Chief Executive must be the AO for the purposes of the authorisation.

9.4 Management of a CHIS

- 9.4.1 There are specific legal rules which must be followed in relation to the management of sources. Officers to act as Designated Handlers and controllers (as set out in s.29(5) RIPA 2000) should be appointed. Officers who undertake these roles must have undergone the specific training required by the legislation. Details are given in the relevant Home Office Code of Practice, and further advice can be obtained from the Corporate Director.
- 9.4.2 A controller will have responsibility for the management and supervision of the Designated Handler and general oversight of the use of the CHIS.
- 9.4.3 Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents. Similar safeguards also apply to the use of vulnerable individuals as sources. (A vulnerable individual is 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 himself or herself, or unable to protect himself or herself against significant harm or exploitation.) Further advice must be sought from the Corporate Director before using juveniles or vulnerable individuals as sources, to ensure that all necessary legal requirements are complied with.
- 9.4.4 A CHIS will have his/her identity protected under the relevant legal procedures.

9.5 Specific CHIS Records

In addition to records kept in accordance with section 11 below the following matters will be recorded and maintained in relation to every CHIS.

- 9.5.1 The identity of the CHIS and the identity, where known, used by the CHIS;
- 9.5.2 the date when and the circumstances in which the CHIS was recruited;
- 9.5.3 any significant information connected with the security and welfare of the CHIS;
- 9.5.4 confirmation that any person granting or renewing an authorisation for the conduct or use of a CHIS that the information referred to in 9.13.3 has been considered and that any identified risks have, where appropriate, been explained to and understood by the CHIS;
- 9.5.5 the identities of the persons who in relation to the CHIS are acting as a Designated Handler or controller and the periods during which those persons have so acted;
- 9.5.6 all contact or communications between the CHIS and the person acting on behalf of the Investigating Officer, including all tasks given to and demands made of the CHIS; information received by the conduct or use of the CHIS and the dissemination of any information so obtained;
- 9.5.7 in situations where the relevant investigating authority is different to the Council, the details of that investigation authority and the means by which the CHIS is referred to within each relevant investigating authority.

9.6 Group Manager Records

- 9.6.1 The following information should be maintained by the Group Manager for the Service Team where the authorisation application originated from in relation to any CHIS:
- any risk assessment in relation to the source;
 - the circumstances in which tasks were given to the source;
 - the value of the source to the investigating authority;

- 9.6.2 A 'Surveillance Log Book' should be completed by the Investigating Officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Once completed, the Log Book will be passed to the Group Manager of the relevant Group/Team or to their designated RIPA co-ordinator for safe keeping in a secure place. Each Service will also maintain a record of the issue and movement of all Surveillance Log Books.

10 Procedure for Monitoring RIPA and Oversight

10.1 Senior Responsible Officer

- 10.1.1 The Council's Corporate Director will be the designated SRO and shall be responsible for the following:-
- the integrity of the process in place within West Somerset District Council to authorise Directed Surveillance;
 - compliance with Part II of RIPA 2000 and any associated Codes of Practice;
 - acting as liaison with the Commissioners and inspectors and engaging with them as appropriate;
 - overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.
- 10.1.2 The SRO shall ensure that all AOs are provided with copies of current and updated Codes of Practice and OSC Guidance and Procedure Notes as they are released from time to time.
- 10.1.3 The SRO shall maintain a Central Record of Authorisations..
- 10.1.4 The Deputy Monitoring Officer will assist the SRO in undertaking the tasks as specified at 10.1 above.

10.2 Oversight Procedures

- 10.2.1 The SRO shall establish a maintain regular meetings not less than twice a year with the AOs to check and test processes and address any training requirements. The SRO shall arrange an oversight meeting as soon as practicable following an inspection to discuss issues and outcomes as appropriate.
- 10.2.2 The SRO shall maintain a spreadsheet in order to record any issues arising out of authorisation applications, the statutory considerations, reviews and cancellations and shall review the quality of authorisations granted from time to time.
- 10.2.3 The SRO shall carry out analysis of such issues and shall decide appropriate feedback to the Authorisation Officer. Such information and conclusions shall also inform the reports to the Corporate Policy Advisory Group required under paragraph 10.3 below.

10.3 Member Review

The members of West Somerset District Council's Corporate Policy Advisory Group shall review the use of RIPA 2000 and this policy at least once a year In order to facilitate this the SRO shall provide an annual report to the Corporate Policy Advisory

Group on how RIPA 2000 has been used in the previous three months and whether there are any concerns as to the policy.

11 Record Keeping

The Council must keep a detailed record of all applications for authorisations, grants, refusals, renewals, reviews and cancellations.

11.1 Completed Authorisation Applications

The originals of all completed RIPA forms, including applications (whether granted or refused), authorisations, renewals, cancellations and reviews, must be forwarded by the Authorisation Officer to the Corporate Director within five working days of the date of the relevant decision. Copies of this information should be made available to the Investigating Officers.

11.2 Central Register of Authorisations

A Central Register of Authorisations will be maintained by the Corporate Director containing the information required from time to time by the relevant Home Office Code of Practice for all authorisation applications. In addition the Corporate Director will keep the originals of all information passed to him under paragraph 11.1.

11.3 SRO Monitoring

The Senior Responsible Officer will monitor authorisations and record-keeping to ensure compliance with the relevant law and guidance, and with these policies and procedures. The Office of the Surveillance Commissioner (OSC) can audit and review the Council's policies and procedures, and individual authorisations.

11.4 Service Team Records

Investigating Officers shall maintain copies of the information set out in paragraph 11.1 passed to the Authorisation Officer and shall ensure that their records include the following as a minimum:-

- the URN for the operation or investigation;
- details of any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- a record of the period over which the surveillance has taken place;
- details of the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- the date and time when any instruction was given by the Authorising Officer, (including any instruction to cease directed surveillance or to cease using a CHIS) and a note of that instruction;

11.5 All records will be retained for 3 years from the ending of the authorisation.

12 Procedure for the use of Surveillance Equipment

12.1 Any equipment that is to be used in the course of a Covert Surveillance operation must be authorised for that use by inclusion on the application form.

- 12.2** Any equipment used in the course of a Covert Surveillance must be:
- 12.2.1 labelled clearly as to identity individual pieces of equipments,
 - 12.2.2 stored in a secure area,
 - 12.2.3 logged in and logged out, noting the time, date and officer's name and position and the URN as set out in the particular authorisation
- 12.3** All details must be completed on all authorisation forms if equipment is used, when renewing, reviewing and cancelling authorisations.
- 12.4** Any and all documentation relating to the use of equipment, will need to be made available if requested by the Monitoring Officer, Police and/or the OSC.
- 12.5** The equipment that is currently used by the Council can be seen at Appendix 1.

13 Authorisation Restrictions

- 13.1** Local Authorities are not able to authorise Intrusive Surveillance and therefore West Somerset District Council will not be involved within this area of the Act.
- 13.2** Local Authorities are not able to authorise entry on or interference with property or wireless telegraphy as set out in Part III Police Act 1997 and West Somerset District Council shall not authorise any such entry or interference.
- 13.3** If an application for Directed Surveillance contemplates the possibility of trespass onto property or if an Investigating Officer considers that trespass is required as part of any authorised Directed Surveillance, the matter should be urgently referred to the Corporate Director and no further action taken.

14. Processing Forms

Please see Appendices 2 & 3 for the Authorisation Procedure and Flowchart on form completion.

15 Procedure for Data Retention

15.1 Retention of authorisation forms

- 15.1.1 All authorisation forms must be retained for 3 years from the date on which the authorisation was obtained.
- 15.1.2 Records kept by West Somerset District Council will be maintained to preserve confidentiality of persons who have provided information either through in the course of their civil duty or if they are a CHIS.
- 15.1.3 Any material which is handled, stored or destroyed will be subject to the Data Protection Act 1998.

15.2 Confidential Information

Confidential information and information subject to a legal privilege will be subject to section 98 of the Data Protection Act 1998.

16. Data Protection

This policy governs Directed Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA). However, even where conduct falls outside of this legal framework and this

policy, the Data Protection Act 1998 applies in relation to the use and storage of personal and sensitive personal data. In any given case, the Human Rights Act 1998 and the Freedom of Information Act 2000 also applies along with RIPA.

17 Complaints Handling

17.1 Independent Tribunal

- 17.1.1 The Regulation of Investigatory Powers Act 2000 also establishes an independent tribunal made up of Senior Members of the Judiciary and the Legal Profession and is independent of the government. The tribunal has full powers to investigate and decide any case within its jurisdiction.
- 17.1.2 If a complaint is therefore received from an individual who has been subject to surveillance or by a member of the public then that person or persons should be referred immediately to the Investigatory Powers Tribunal.
- 17.1.3 The address for the Investigatory Powers Tribunal is PO Box 33220 London SW1H 9ZQ. The telephone contact number is 0207 2734514.

17.2 West Somerset District Council's Surveillance Complaints Procedure

- 17.2.1 If a complaint is received from a member of the public or a person who has been subject to any form of surveillance the complaint will be referred to the appropriate Service Team Leader for investigation.
- 17.2.2 The Service Team Leader will decide whether the complaint should be referred to the Monitoring Officer.
- 17.2.3 Thereafter a decision will be taken, as to what action, if any, should be taken.

18 Conclusion

- 18.1 This concludes the written statement of Operational Procedure for West Somerset District Council's Policy in accordance with the Regulation of Investigatory Powers Act 2000.
- 18.2 This Policy will be revised to comply with any statutory amendments.

RIPA POLICY VERSIONS	DATE	STATUS
Version 1	2000	Archived
Version 2	December 2005	Draft
Version 3	28/06/06	Current
Appendices Nos 4 - 7 updated	July 2008	Current
Version 4	October 2011	Draft

19 Referencing

This guidance has been prepared in accordance with information and advice obtained from the following:

- 1. Office of Surveillance Commissioners (OSC)**
- 2. The Regulation of Investigatory Powers Act 2000**
- 3. Data Protection Act 1998**
- 4. Human Rights Act 1998**
- 5. Freedom of Information Act 2000**
- 6. Department for Work and Pensions
Fraud Procedures and Instructions Manual**
- 7. National Anti-Fraud Network**
- 8. Home Office Code of Practice (Surveillance) 2010 and
Code of Practice (CHIS) 2010**

20 Appendices

Appendix No	Document	Page Nos
Appendix 1	Table of Equipment used in Covert Investigations	18
Appendix 2	Procedure for Completion of Authorisation Forms	19

Appendix 3	Flowchart 1 for directed surveillance (For guidance and training purposes)	20
Appendix 4	Home Office Form (version 2008)	
Updated July 2008	Application for Authority for Directed Surveillance	21
Appendix 5	Home Office Form (version 2008)	
Updated July 2008	Application for Renewal of Directed Surveillance	28
Appendix 6	Home Office Form (version 2008)	
Updated July 2008	Cancellation of Authority for Directed Surveillance	31
Appendix 7	Home Office Form (version 2008)	
Updated July 2008	Review of Directed Surveillance	33

TABLE OF EQUIPMENT

Service Team	Identify the Equipment	Equipment Label	Location where the Equipment is stored	What is the purpose of using the Equipment when conducting a Covert Surveillance
Benefits	Digital Camera (1)	Panasonic Lumix DMC-FX9 No. EN6DD03802R	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Built Environment	Digital Camera (2)	Olympus FE 100 Olympus FE 100	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Corporate Finance				
Customer Advice	Digital Camera (1)	Creative Model No. PD0160	Customer Centre, Summerland Road	Evidence gathering in covert investigations.
Environmental Health and Licensing	Digital Camera (4)	Olympus Serial No. 00641 Olympus Serial No. 00631 Olympus Canon A80 No 7236031702	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Housing				
ICT				
Leisure and Community				
Liveability	Digital Camera (1)	Olympus FE 100	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Members and Central Administration	Digital Camera (1)	Olympus FE 100	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Planning	Digital Camera (2)	Panasonic Lumix DMC-FX7 Nos ER5BD001560 ER5BD001524	West Somerset House, Killick Way, Williton	Evidence gathering in covert investigations.
Regeneration and Policy				
Revenues				

***All Equipment is subject to change and variation of uses

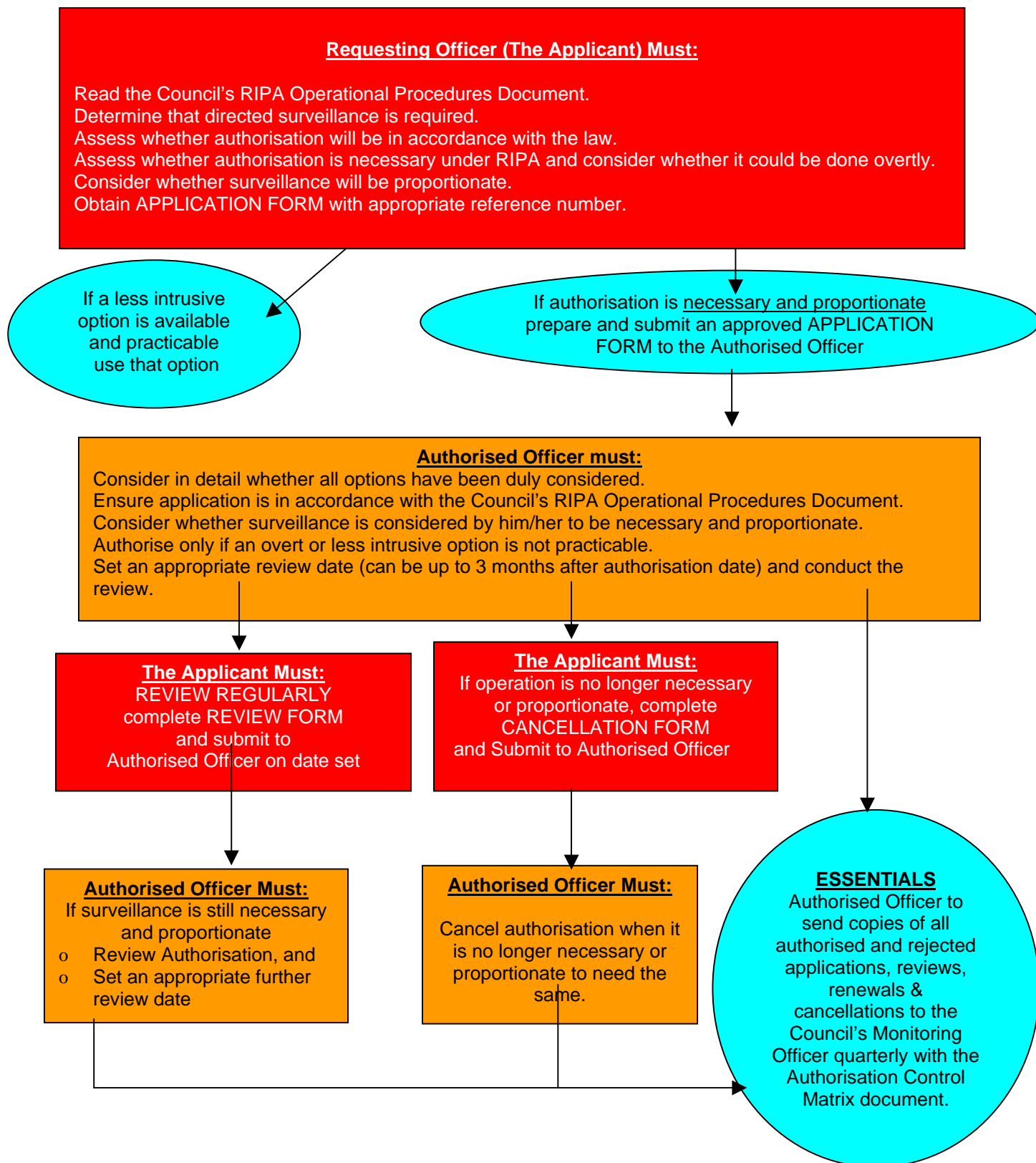
PROCEDURE FOR COMPLETION OF AUTHORISATION FORMS

- 1 The forms that are required for the different stages of authorisation to undertake a covert surveillance investigation operation are to be maintained by the Council's Monitoring Officer.
- 2 Each form will need to be referenced in the following manner:
 - an example reference for the Service Team Benefits would be B, followed by
 - (i) the Authorising Officer's initials i.e. AD for Adrian Dyer, followed by
 - (ii) the date e.g. 01/11/2005, followed by
 - (iii) a sequential number i.e. 001 which would be for the first authorisation.Therefore the form reference in this case would be **B/AD/01/11/2005/001**
- 3 This will ensure an essential record of all authorisations by having a sequence of numbering automatically allocated and therefore ensuring that no documents are lost or duplicated.
- 4 Each time an application is made to an Authorisation Officer (AO) to carry out covert surveillance, once the AO has received the relevant form, the AO will either authorise or deny the application this should be done within **five** working days.
- 5 The application form must be submitted to the AO. The AO retains the original form. Immediately upon signing, a copy of the form will be sent by the AO to the Council's Monitoring Officer. The Investigating Officer will retain a copy, and a copy is retained in the Service Team's own RIPA records
- 6 All forms must be completed fully with the appropriate signatures and dates inserted where necessary.
- 7 In cases of urgent/oral applications, the written authorisation must be obtained as soon as reasonably practical. The authorisation form must indicate the date on when the original date of the authorisation was obtained.

Flowchart

DIRECTED SURVEILLANCE

Authorisation under the Regulation of Investigatory Powers Act 2000



Unique Reference Number

APPENDIX 4

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority <i>(including full address)</i>			
Name of Applicant		Unit/Branch /Division	
Full Address			
Contact Details	Specimen Form		
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number

DETAILS OF APPLICATION	
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171.¹	
2. Describe the purpose of the specific operation or investigation.	
3. 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.	
<h1>Specimen Form</h1>	
4. The identities, where known, of those to be subject of the directed surveillance.	
<ul style="list-style-type: none">• Name:• Address:• DOB:• Other information as appropriate:	
5. Explain the information that it is desired to obtain as a result of the directed surveillance.	

¹ For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)
<ul style="list-style-type: none">• In the interests of national security;• For the purpose of preventing or detecting crime or of preventing disorder;• In the interests of the economic well-being of the United Kingdom;• In the interests of public safety;• for the purpose of protecting public health;• for the purpose of assessing or collecting any tax, duty, tax credit, national insurance contribution or charge payable to a government department;
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.] Describe precautions you will take to minimise collateral intrusion

Specimen Form

Unique Reference Number

9. Explain why this directed 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? [Code paragraph 2.5]

Specimen Form

10. Confidential information. [Code paragraphs 3.1 to 3.12]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	
-------------------------	--

11. Applicant's Details.			
Name (print)		Tel No:	
Grade/Rank		Date	
Signature			
12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW- in this and the following box.]			
<p>I hereby authorise directed surveillance defined as follows: [<i>Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?</i>]</p> <p style="text-align: center;">Specimen Form</p>			
13. Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 2.4] Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]			

Unique Reference Number

--

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12

--

Specimen Form

Date of first review

Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

--

Name (Print)		Grade / Rank	
Signature		Date and time	
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]			

Unique Reference Number	
-------------------------	--

15. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

--

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

--

Name (Print)		Grade/ Rank	
Signature		Date and Time	
Urgent authorisation Expiry date:		Expiry time:	
<i>Remember the 72 hour rule for urgent authorities – check Code of Practice.</i>	e.g. authorisation granted at 5pm on June 1 st expires 4.59pm on 4 th June		

Specir Form

Unique Reference Number	
-------------------------	--

APPENDIX 5

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority <i>(including full address)</i>	Specimen Form		
Name of Applicant			
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

Unique Reference Number	
-------------------------	--

--

3. Detail the reasons why it is necessary to continue with the directed surveillance.

--

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

--

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

--

6. Give details of the results of the regular reviews of the investigation or operation.

--

7. Applicant's Details

Name (Print)		Tel No	
---------------------	--	---------------	--

Unique Reference Number	
-------------------------	--

Grade/Rank		Date	
Signature			

8. Authorising Officer's Comments. This box must be completed.

Specimen Form

9. Authorising Officer's Statement.

I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing.

This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (Print) **Grade / Rank**

Signature **Date**

Renewal From: **Time:** **Date:**

Date of first review.	
Date of subsequent reviews of this authorisation.	

Unique Reference Number

APPENDIX 6

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Specimen Form

Public Authority <i>(including full address)</i>			
Name of Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

--

Unique Reference Number	
-------------------------	--

2. Explain the value of surveillance in the operation:

Specimen Form

3. Authorising officer's statement.

I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.

Name (Print)	Grade
Signature	Date

4. Time and Date of when the authorising officer instructed the surveillance to cease.

Date:		Time:	
--------------	--	--------------	--

5. Authorisation cancelled.	Date:	Time:
------------------------------------	--------------	--------------

Unique Reference Number

APPENDIX 7

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Specimen Form

Public Authority <i>(including address)</i>			
Applicant		Unit/Branch / Division	
Full Address			
Contact Details			
Operation Name		Operation Number* <small>*Filing Ref</small>	
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.
--

Unique Reference Number

--

3. Detail the reasons why it is necessary to continue with the directed surveillance.

<h1>Specimen Form</h1>

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

--

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

--

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

--

7. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	

Unique Reference Number

Signature

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

Specimen Form

9. Authorising Officer's Statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Name (Print) Grade / Rank

Signature Date

10. Date of next review.