Inverclyde council

AGENDA ITEM NO: 17

Report To:	**Policy & Resources Committee**	**Date:**	**21 March 2017**
Report By:	**Corporate Director Environment, Regeneration & Resources**	**Report No:**	**FJ/LP/023/17**
Contact Officer:	**Fraser Jarvie**	**Contact No:**	**01475 712121**
Subject:	**Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Inspection by the Office of Surveillance Commissioners**		

1.0 PURPOSE

1.1 The purpose of this report is to update Members on surveillance carried out by Inverclyde Council employees under the above Act and advise on the inspection visit by Sir David Clarke, Assistant Surveillance Commissioner, the Inspector appointed by the Office of Surveillance Commissioners (OSC), on 16 November 2016.

2.0 SUMMARY

2.1 Until October 2000 the use of covert surveillance and covert human intelligence sources was not subject to statutory control in the UK. From that date arising from the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) there has been a legal framework which ensures that the use, deployment, duration and effectiveness of covert surveillance and the use of covert human intelligence sources is subject to an authorisation, review and cancellation procedure.

2.2 Inverclyde Council employees must comply with the Act and adhere to the authorisation procedures specified in the Council's policy and procedures for authorisation of covert surveillance and covert human intelligence sources approved by the Council following the introduction of the legislation.

2.3 Under the Council's authorisation process, applications for directed surveillance or the use or conduct of a source are authorised by a restricted number of authorising officers at a senior level. A central register of authorisations is maintained by the Head of Legal & Property Services who also carries out a gate-keeping role in connection with draft applications.

2.4 The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within RIPSA. This oversight includes inspection visits by inspectors appointed by the OSC on a 3-yearly basis. The Chief Surveillance Commissioner reports directly to the Prime Minister and the Scottish Ministers. The Council received a visit in this connection on 16 November 2016. The Inspecting Officer, Sir David Clarke, Assistant Surveillance Commissioner met with senior Officers of the Council as well as the Legal Services Manager responsible for the maintenance of the Central Record of Authorisations. He considered previous recommendations from the last inspection on 27 February 2014. He examined the five authorisations made since the last inspection and the Central Register. Finally at the conclusion of his visit he met with the Chief Executive.

2.5 A copy of the inspection report and letter dated 29 November 2016 from the Chief Surveillance Commissioner, Lord Judge, is attached (See Appendix 1). Generally the Chief Surveillance Commissioner, in his covering letter, noted the Inspector's view that the arrangements for dealing with the statutory responsibilities vested in the Council are "sound and fit for purpose".

2.6 The two recommendations from the previous inspection report in 2014 were both discharged. It was noted that the policy and guidance document had been updated to take account of the use of the internet and social networking sites and there had been an improved quality in the authorisations of directed surveillance.

2.7 Three new recommendations were made by the Inspector and appropriate steps have been taken to ensure that these are complied with. To address the first recommendation the Committee is asked to designate the Head of Legal & Property Services, Gerard Malone, as the RIPSA Senior Responsible Officer (SRO) and to approve the Head of Education, Ruth Binks and the Acting Head of Safer & Inclusive Communities, Martin McNab as Authorising Officers also. Secondly the present practice of carrying out juvenile test purchase operations without the protection of RIPSA authorisations is being kept under review by the Council's Trading Standards Officer and thirdly, to ensure that formal reviews of all future authorisations are appropriately conducted at specified intervals, the standard review form will require to be used. The Central Register will also be amended to include a section which records the date of review and the outcome. Lastly it is proposed that an annual report will be submitted to the CMT on the use of RIPSA authorisations and in addition a report will be submitted every three years to the Policy & Resources Committee following the inspection of the Council.

2.8 A copy of the Council's revised RISPA Policy and Procedures are attached (See Appendix 2), and Members are asked to approve the amendments made in response to the Inspector's suggestions.

3.0 RECOMMENDATIONS

3.1 That the Committee note the Inspection Report (Appendix 1) and the positive outcome of the recent inspection in November 2016.

3.2 That the Committee agree that reports on the application of and compliance with the Act are submitted on an annual basis to the CMT and once every three years following the inspection by the OSC, to the Committee.

3.3 That the Committee approve the amended RISPA Policy and Procedures (Appendix 2).

3.4 That the Committee approve the appointment of Gerard Malone, Head of Legal & Property Services as its RIPSA Senior Responsible Officer (SRO), and the appointment of Ruth Binks, Head of Education and Martin McNab, Acting Head of Safer & Inclusive Communities, as Authorising Officers along with the Chief Executive.

3.5 That the Committee note the steps taken to meet the recommendations made by the Inspecting Officer.

Gerard Malone
Legal & Property Services

4.0 BACKGROUND

4.1 The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of unaided surveillance and surveillance devices. Where this surveillance is covert i.e. the subject of the surveillance is unaware that it is taking place, then it must be authorised to ensure that it is lawful. CCTV systems in the main will not be subject to this procedure as they are "overt" forms of surveillance. However, where CCTV is used as part of a pre-planned operation of covert surveillance, then authorisation must be obtained.

4.2 The use of human beings to provide information (informants) is a valuable resource also for the protection of the public in the maintenance of law and order. These are generally described as "Covert Human Intelligence Sources" (CHIS). It should be noted however that the Council has not so far carried out surveillance in this manner since the introduction of the legislation. There are no immediate plans to make use of this provision.

4.3 Currently the following officers have been trained to authorise surveillance under the Act (RIPSA):-

Aubrey Fawcett, Chief Executive
Gerard Malone, Head of Legal & Property Services
Ruth Binks, Head of Education
Martin McNab, Acting Head of Safer Communities

4.4 The two recommendations made by the previous inspecting officer have now been met and three further recommendations have been made following the inspection. Appropriate steps have been taken to respond to these recommendations.

4.5 With reference to Paragraph 18 of the Inspection Report, a training session for Social Work staff will take place before 21 March 2017.

5.0 IMPLICATIONS

Finance

5.1 None.

Financial Implications:

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report	Virement From	Other Comments
N/A	N/A	N/A	N/A	N/A	N/A

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact	Virement From (If Applicable)	Other Comments
N/A	N/A	N/A	N/A	N/A	N/A

Legal

5.2 None

Human Resources

5.3 None

Equalities

5.4 None

Repopulation

5.5 None

APPENDIX 2

INVERCLYDE COUNCIL

POLICY AND PROCEDURES FOR AUTHORISATION OF COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

TABLE OF CONTENTS

1. Introduction

1.1 The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of unaided surveillance and surveillance devices. Where this surveillance is covert i.e. the subject of the surveillance is unaware that it is taking place, then it must be authorised to ensure that it is lawful. CCTV systems in the main will not be subject to this procedure as they are "overt" forms of surveillance. However, where CCTV is used as part of a pre-planned operation of covert surveillance, then authorisation should be obtained.

1.2 The use of human beings to provide information ("informants") is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is sometimes made of "undercover" officers and informants. These will be referred to in this document as "covert human intelligence sources" ("CHIS") and the area of work of undercover officers and informants to whom this procedure applies will be referred to as "CHIS work".

1.3 Until October 2000 the use of covert surveillance and covert human intelligence sources was not subject to statutory control in the UK. From that date a legal framework ensures that the use, deployment, duration and effectiveness of covert surveillance and the use of covert human intelligence sources is subject to an authorisation, review and cancellation procedure.

2. Definitions

2.1 Appendix 1 contains definitions of the terms used within this document.

3. Policy Statement

3.1 In some circumstances it may be necessary for Inverclyde Council employees in the course of their duties to make observations of a person in a covert manner and to make use of informants and to conduct undercover operations in a covert manner. By their nature such actions constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ("the right to respect for private and family life").

3.2 The Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) ("the Acts") together provide for the first time a legal framework for covert surveillance and the use of covert human intelligence sources by public authorities (including local authorities) and an independent oversight regime to monitor these activities.

3.3 Inverclyde Council employees must adhere to the authorisation procedures specified in this document before conducting any covert surveillance or using a source or allowing or conducting an undercover operation.

3.4 Employees of Inverclyde Council will **not** carry out intrusive surveillance within the meaning of RIPSA. This is covert surveillance of anything taking place on residential premises or in a private vehicle that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

4. Objective of the Procedures

4.1 The objective of these procedures is to ensure that all work involving directed surveillance by Inverclyde Council employees is carried out effectively while remaining in accordance with the law. Directed surveillance is defined in the code of practice as covert surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person". These procedures should be read in conjunction with RIPSA and the Scottish Executive's Codes of Practice on covert surveillance and the use of covert human intelligence sources.

5. Scope of the Procedures

5.1 These procedures apply in all cases where "directed surveillance" is being planned or carried out and in all cases where the use of an undercover officer or source is being planned or carried out. This includes the use of media such as the internet or Social Networking Sites (SNS) (see Appendix 5).

5.2 These procedures do not apply to:-

- Ad hoc covert observations that do not involve the systematic surveillance of a specific person.

- Observations that are not carried out covertly.

- Unplanned observations made as an immediate response to events.

- Covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated (see definition of a covert human intelligence source). As an example, the purchase of a music CD for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where he buys suspected fakes, when he takes delivery etc, then authorisation should be sought beforehand.

- Tasks given to persons (whether those persons are employees of the Council or not) to ascertain information which is not private e.g. the location of cigarette vending machines in licensed premises.

5.3 In all cases of doubt, legal advice should be sought from the Head of Legal and Property Services.

6. Principles of Directed Surveillance and the Use or Conduct of Covert Human Intelligence Sources

6.1 In planning and carrying out directed surveillance or CHIS work, Inverclyde Council employees shall comply with the following principles.

6.2 Lawful Purposes

6.2.1 Directed surveillance and source work shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Act) namely:-

- For the purpose of preventing or detecting crime or the prevention of disorder.
- In the interests of public safety.
- For the purpose of protecting public health.

6.2.2 Employees carrying out surveillance shall not interfere with any property or harass any person.

6.2.3 Employees carrying out CHIS work or using sources must be aware that a source has no licence to commit crime. Any source that acts beyond the acceptable limits of case law in regard to this principle risks prosecution.

6.3 Confidential Material

6.3.1 Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of a Corporate Director or the Chief Executive.

6.3.2 Confidential material consists of:

- Matters subject to legal privilege (for example between professional legal adviser and client).
- Confidential personal information (for example relating to a person's physical or mental health).

- Confidential journalistic material.

6.4 Vulnerable Individuals

6.4.1 Vulnerable individuals (such as the mentally impaired) will only be authorised to act as a source in the most exceptional circumstances and the authorisation of the Chief Executive or a Corporate Director shall be required.

6.5 Juvenile Sources

6.5.1 The use or conduct of any source under 16 years of age living with their parents (or any person having parental responsibilities for them) cannot be authorised in relation to giving information about their parents (or any person having parental responsibilities for them).

6.5.2 Sources under the age of 16 can give information about other members of their immediate family in exceptional cases.

6.5.3 A parent, guardian or other appropriate adult must be present at meetings with the juvenile source. There must always be an officer with responsibility for ensuring compliance with this requirement.

6.5.4 An authorisation for any source under the age of 18 shall not be granted or renewed unless or until:

- The safety and welfare of the juvenile have been fully considered.

- A risk assessment, or an updated risk assessment as appropriate, has been undertaken as part of the application to deploy a juvenile source, covering the physical dangers and the moral and psychological aspects of his/her deployment.

- The authorising officer has considered the risk assessment, or an updated risk assessment as appropriate, and is satisfied that any identified risks are justified.

- The authorising officer has satisfied himself/herself that any risk has been properly explained and understood by the juvenile.

6.5.5 Deployment of juvenile sources will only be authorised by the Chief Executive or a Corporate Director.

7. The Authorisation Process

7.1 Applications for directed surveillance or the use or conduct of a source will be authorised at level of "Investigations Manager" or "Assistant Head of Service" as prescribed in the Regulation of Investigatory Powers (Prescription of Offices etc. and Specification of Public Authorities)(Scotland) Order 2010. For the purposes of Inverclyde Council, the person granting authorisation shall be no lower than Head of Service or its equivalent. For public authorities such as Inverclyde Council, there are no substitutes of lower grade prescribed to authorise "urgent" cases. A list of the current Authorising Officers (AO's) is attached at Appendix 6.

7.2 Authorising officers within the meaning of this procedure shall avoid authorising their own activities wherever possible and only do so in exceptional circumstances. An authorising officer should not also act as a controller or handler of a source. These roles should be separate.

7.3 Authorisations shall be in writing. However, in urgent cases the authorising officer **may approve** applications orally. A case may be regarded as urgent if the time that would elapse before the AO was available to grant the authorisation would, in the judgement of the AO, be likely to endanger life or jeopardise the investigation or operation for which authorisation is being given.

7.4 All applications for authorisations or renewals of authorisations shall be made on the appropriate form (see Appendix 2). The applicant in all cases should complete the form. In urgent cases an oral approval may be given by the authorising officer and in such a case a statement that the authorising officer has expressly granted the authorisation should be recorded on the application form or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the

authorising officer spoke (normally the applicant) and must later be endorsed by the authorising officer. A written authorisation shall be issued as soon as practicable.

7.5 Where an authorisation ceases to be either necessary or appropriate, the authorising officer or an appropriate deputy shall cancel the authorisation on the appropriate form.

7.6 Forms, codes of practice and supplementary material will be available from the Head of Legal and Property Services.

7.7 Any person giving an authorisation must be satisfied that:

- Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ("collateral intrusion"). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.

- The authorisation is necessary.

- The authorised surveillance is proportionate.

- In the case of source work that satisfactory arrangements exist for the management of the source.

7.8 **Necessity**

7.8.1 Surveillance operations and CHIS work shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objectives.

7.9 **Effectiveness**

7.9.1 Surveillance operations and CHIS work shall be undertaken only by suitably trained or experienced employees or under their direct supervision.

7.9.2 The Standard Operating Procedure (SOP) detailed in Appendix 4 shall be followed when technical equipment is used in any directed surveillance operation.

7.10 **Proportionality**

7.10.1 The use of surveillance and sources shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated. A balance requires to be struck between the degree of intrusion into a person's privacy against the necessity of the surveillance.

7.11 **Arrangements for Handling Sources**

7.11.1 Authorisation for use of a covert human intelligence source shall only be granted if sufficient arrangements are in place for handling the source. The arrangements that are considered necessary are as follows:-

- There will be at all times a person holding the requisite office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority and for the source's security and welfare - this should be the source's line manager ("the handler"). There will be at all times another person holding the requisite office, rank or position with the relevant investigating authority who will have general oversight of the use made of that source - this should be the handler's line manager ("the controller").

- There will be at all times a person holding the requisite office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of that source - this should be the authorising officer. That record must contain the particulars detailed in Appendix 3.

- The record relating to the use of that source shall be maintained by Inverclyde Council and will always contain particulars of such matters as may be specified in regulations made by Scottish Ministers.

- The records maintained by Inverclyde Council which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

- The authorising officer must make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

7.12 All authorisations for directed surveillance and use of a source shall be in accordance with these procedures.

7.13 **Use of a Covert Human Intelligence Source with Technical Equipment**

7.13.1 A covert human intelligence source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require special authorisation to record activity taking place inside the premises or vehicle where the recording takes place in his presence. Authorisation for the use of that covert human intelligence source may be obtained in the usual way.

7.13.2 Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.

7.13.3 Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by Inverclyde Council; all authorisations must remain within the scope of the Scottish Executive's guidance on authorising grades.

8. **Time Periods - Authorisations**

8.1 Oral applications expire after 72 hours.

8.2 If required, authorisations can be renewed for a further period (three months in the case of directed surveillance and 12 months in the case of the use of a covert human intelligence source) if renewed in writing.

8.3 Written authorisations expire after three months in the case of directed surveillance and 12 months in the case of the use of a covert human intelligence source; these periods begin on the day from which the authorisation took effect.

8.4 Authorisations expire after a period of one month in relation to a source under the age of 18.

9. Time Periods - Review

9.1 The authorising officer shall review all authorisations at intervals of not more than one month. The appropriate review form should always be used. Details of the review and the decision reached shall be noted on the original application. The results of the review should be recorded on the central register of authorisations.

10. Time Periods - Renewals

10.1 If at any time before an authorisation would expire (including oral authorisations) the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period beginning on the day on which the previous authorisation ceases to have effect; the renewal periods are three months in the case of directed surveillance and 12 months in the case of the use of a covert human intelligence source. Applications should only be made shortly before the authorisation is due to expire.

10.2 Any person entitled to authorise may renew authorisations. Authorisations may be renewed more than once, provided that they continue to meet the criteria for authorisation.

10.3 Authorisations for the deployment of a juvenile source are renewable for one further period of one month.

11. Cancellation

11.1 The authorising officer or appropriate deputy (or a substitute of the same or more senior rank to that of the authorising officer) must cancel an authorisation if he/she is satisfied that the directed surveillance no longer satisfies the criteria for authorisation or the use or conduct of the source no longer satisfied the criteria for authorisation or that procedures for the management of the source are no longer in place. Where possible a source must be informed that the authorisation has been cancelled.

11.2 Records should be kept of the use that was made of an authorisation and in particular what material was acquired. This should contain detail of the covert activity conducted under the authorisation, what had been achieved by that covert

activity and what surveillance material, if any, had been acquired. If material has been acquired, then the authorising officer must be satisfied that it is being properly handled, stored or destroyed (for reference see ~The Covert Surveillance Code of Practice, paragraphs 3.16 and 3.17). The OSC preferred form of cancellation should always be used.

12. Monitoring

12.1 Each service or discrete location within services must maintain a record of all applications for authorisation (including its users), renewals, reviews and cancellations. The most senior authoriser in that service or at that location shall maintain the monitoring form. (See Appendix 3 for the matters that must be included in the record.)

13. Security and Retention of Documents

13.1 Documents created under these procedures are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and Inverclyde Council's Code of Practice.

13.2 The Head of Legal and Property Services shall maintain the central register of authorisations. Authorising officers shall notify him/her of the grant, renewal or cancellation of any authorisations and the name of the authorising officer within one working day to ensure the accuracy of the central register.

13.3 The authorising officer shall retain the original authorisation and all renewal forms until cancelled. On cancellation, the original application, renewal and cancellation forms shall be forwarded to the Head of Legal and Property Services with the authorising officer retaining a copy.

13.4 The authorising officer shall retain the copy forms for at least one year after cancellation. The Head of Legal and Property Services shall retain the original forms for at least five years after cancellation. In both cases, these will not be destroyed without the authority of the authorising officer if practicable.

13.5 All information recovered through the use of a source which is relevant to the investigation shall be retained by the authorising officer for at least five years after the cancellation of the authorisation or the completion of any court proceeding in which said information was used or referred to. All other information shall be destroyed as soon as the operation is cancelled.

14. Oversight

14.1 The Office of Surveillance Commissioners ("OSC") provides an independent review of the use of the powers contained within RIPSA. This review includes inspection visits by inspectors appointed by the OSC.

15. Complaints

15.1 RIPA established an independent tribunal. This has full powers to investigate and decide any cases within its jurisdiction. A leaflet entitled "Investigatory Powers Tribunal: Regulation of Investigatory Powers Act 2000" sets out the complaints procedure. This is available from the Head of Safer Communities and includes a form for a person to complain to the tribunal.

APPENDIX 1

DEFINITIONS

Covert Human Intelligence Source ("source" or "CHIS") means a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

- covertly uses such a relationship to obtain information or to provide information or to provide access to information to another person, or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

Directed Surveillance is surveillance that is covert but not intrusive and is undertaken

- for the purpose of a specific investigation or a specific operation, 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
- 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 to be sought for the carrying out of the surveillance.

Intrusive Surveillance is covert surveillance that:

- is carried out in relation to anything taking place on residential premises or in a 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 capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Authorising Officer is the person who is entitled to give an authorisation for the use or conduct of a source in accordance with Section 5 of the Regulation of Investigatory Powers (Scotland) Act 2000.

Private Information includes information about a person relating to that person's private or family life.

Residential Premises means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

Private Vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use a vehicle derives only from having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

Handler means the person referred to in Section 4(6)(a) of the Regulation of Investigatory Powers (Scotland) Act 2000 holding an office or position with the Local Authority and who will have day to day responsibility for:-

- dealing with the source on behalf of the Local Authority;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

Controller means the person/the designated managerial Officer within the Local Authority referred to in Section 4(6)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000 responsible for the general oversight of the use of the source.

The conduct of a source is action of that source falling within the terms of the Regulation of Investigatory Powers (Scotland) Act 2000 or action incidental to it.

The use of a source is any action to induce, ask or assist a person to engage in the conduct of a source or to obtain information by means of an action of the source.

APPENDIX 2

FORMS FOR AUTHORISATION

Directed Surveillance

DS1 - Application for Authority for Directed Surveillance

DS2 - Application for Renewal of Directed Surveillance Authority

DS3 - Cancellation of Directed Surveillance

Authorisation of the Use of Conduct of a Covert Human Intelligence Source (CHIS)

CHIS1 - Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source

CHIS2 - Application for Renewal of the Use or Conduct of a Covert Human Intelligence Source

CHIS3 - Cancellation of the Use or Conduct of a Covert Human Intelligence Source

APPENDIX 3

PARTICULARS TO BE CONTAINED IN RECORDS

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other than the authority maintaining the records;
(d) the means by which the source 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 a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (e) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
(g) the date when, and the circumstances in which, the source was recruited;
(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 7(6)(a) to (c) of the 2000 Act or in any order made by the Scottish Ministers under section 7(2)(c);
(i) the periods during which those persons have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him or her in relation to their activities as a source;
(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
(l) the information obtained by each relevant investigating authority by the conduct or use of the source;
(m) any dissemination by that authority of information obtained in that way; and
(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

APPENDIX 4

STANDARD OPERATING PROCEDURE

Regulation of Investigatory Powers (Scotland) Act 2000
Standard Operating Procedures on the use of Technical Equipment for Directed Surveillance

1.0 Introduction

1.1 The aim of this document is to set out standard operating procedures on the use of technical equipment where it becomes necessary for Inverclyde Council to undertake Covert Directed Surveillance in compliance with the Regulation of Investigatory Powers (Scotland) Act 2000.

1.2 Surveillance falls into three categories: Directed Surveillance: Intrusive Surveillance: Covert Human Intelligence Sources. Councils must not conduct intrusive surveillance.

2.0 Office of Surveillance Commissioners: Procedures & Guidance

2.1 Officers whose duties require them to consider the question of Covert Directed Surveillance are to make themselves familiar with the Regulation of Investigatory Powers (Scotland) Act 2000 and the attendant Procedures & Guidance issued by the Office of Surveillance Commissioners (OSC). The Procedures and Guidance is a protected document and is not to be made available to any member of the public in any form without the written permission of the OSC.

2.2 Officers will adhere to the Council's Policy and Procedures as well as the requirements of the Act and Guidance.

3.0 Operational Considerations

3.1 Each investigation will be different and needs to be considered on its own merits. Where it has been deemed necessary and proportionate to conduct Directed Surveillance (see guidance) an assessment will be carried out in respect of the location to be placed under surveillance.

3.2 The assessment will take account of the nature of the operation, and the evidence to be obtained. Consideration will be given to the safety of the public in general, the safety of any person who is to accommodate investigating officers and/or specialist equipment. Consideration will be given to the question of collateral intrusion including the likelihood of obtaining confidential information in the course of the operation. Officers will consider the capability of any equipment to be deployed, and ensure that intrusive surveillance is avoided. Intrusive surveillance involves information of a quality that would have been obtained if a person or device were placed in a property, vehicle or vessel, even if the person or equipment was outwith that place.

4.0 Application for Directed Surveillance

4.1 Officers will complete an application for Directed Surveillance, ensuring that an up-to-date form is used. Forms are amended by the OSC from time to time.

5.0 Surveillance Equipment

5.1 A master record of all technical equipment held for the purposes of surveillance will be kept in a RIP(S)A folder in a secure location with the equipment. Make, model and serial numbers will be recorded on the record.

5.2 When the use of technical equipment has been authorised for the purposes of covert directed surveillance, the equipment issued will be signed for by the officer installing the equipment at the host location. The time and date of issue will be recorded along with the location concerned. A note will be taken of the Unique Reference Number allocated to the authorisation in the Central Register of Authorisations. This information will be replicated on the Form of Council RIP(S)A records for transfer to the Registry Keeper when the operation has been completed.

5.3 A surveillance equipment mandate will be presented to, and signed by the responsible person at the host location where equipment is installed. The Investigator will also sign the mandate which is an agreement regarding the care of the equipment and its safe return to Inverclyde Council when required.

6.0 Review and Cancellation

6.1 The Regulation of Investigatory Powers (Scotland) Act 2000 requires Authorising Officers to set review dates for each operation. Authority to conduct directed surveillance ceases automatically after three months (unless renewed).Operational officers should note that both review and cancellation must be completed by 2359hrs on the day preceding the set dates. Accordingly, operational officers will make a note of the dates set for review and cancellation on the Form of Council RIP(S)A Records and will conduct their own review of the situation to meet with, or exceed the nominated date.

6.2 When authority to cancel the operation has been given, the case officer will recover the equipment and complete the Form of Council RIP(S)A Records accordingly. The equipment will be 'signed in' on the record of equipment issued and returned. A note is to be made on this record in the event that equipment has to go elsewhere to be tested or repaired.

Attachments: Register of Equipment
Surveillance Equipment: Guidelines & Mandate

Inverclyde Council

Social Protection Team

A.S.I.S.T.

Surveillance Equipment Guidelines For Clients

1. **Do not tamper with equipment.**

2. **In the event of an incident taking place, contact A.S.I.S.T immediately.**

3. **Confidentiality:**

Please ensure you inform no one that there is surveillance equipment installed within your property. This may put you, your premises, the equipment, and the surveillance operation at risk.

4. **Confirmation**

I have read the aforementioned guidelines and rules regarding the installation of surveillance equipment in my property and I agree to abide by them.

I will return the surveillance equipment to the Council's representative when I am requested to do so. I understand that if any of the equipment placed within my property is willfully damaged whilst in my possession, then I may be responsible for the cost of its repair or replacement.

Signed…… Witnessed……

DATE:……..

REGISTER OF EQUIPMENT

ASIST - CAMERA SERIAL NUMBERS

New Wireless System

Name	Serial Number	Description
Camera 1	AFU00402	Bullet Camera 1
Camera 2	CAM321	Bullet Camera 2
Camera 3	411343	PTZ
Removable Hard Drive 1	2050	
Removable Hard Drive 2	1797	
Pelicase	110	

Older System

Name	Serial Number	Description
Camera 4	AP04032073	Standard Camera
Camera 5	AP04032071	Standard Camera
Camera 6	C043309	Bullet Camera
Camera 7	D018657	Spy Hole Camera
Hard Drive 3	A1X041458003	Silver hard drive
Hard Drive 4	A1X041051003	Silver hard drive
Monitor 1	CIU00342	Small Monitor
Monitor 2	KDC12893	Large Monitor

Pinhole Camera System

Computer	PC018667	Standard Computer
Monitor	50L8002741	17” Monitor

New RACAM

The following equipment will be used -

Digital Camera Samsung Serial no: C5556V2C9010483
Bullet camera: Serial No C043309
Time Space Digital Recorder: Serial No 115176 Time space removable Hard Drive 115176
Time Space Monitor: Serial No: 115726

APPENDIX 5

THE INTERNET AND SOCIAL NETWORKING SITES

Circumstances that Might Give Rise to an Authorisation of Directed Surveillance

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. It is important to note that individual social networking sites vary in their operation and care should be taken to understand how they work.

If there is any covert use (i.e. the other party does not realise the enquirer is a Council employee) made of these media in support of a specific investigation or operation and any privacy settings are passed, then there are good grounds to consider granting an authorisation for directed surveillance.

Where privacy settings are available but not applied the data may be considered “open source” and an authorisation is not usually required. However, repeat viewing of “open source” sites may constitute directed surveillance and this has to be considered on a case by case basis. It is not unlawful for a Council Officer to set up a false identity but it is inadvisable to do so for covert purposes without authorisation.

CHIS

If a relationship is likely to be established or maintained (i.e. the activity is more than mere reading of the site’s content) then a CHIS authorisation should be considered.

The identity of a person likely to be known to the subject of interest should not be adopted without authorisation and explicit consent of the person whose identity is used.

With regard to test purchases the criteria for directed surveillance should be applied on a case by case basis. However, CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage.

The guidance at note 288 of the OSC Procedures and Guidance (Dec 2014) should be followed in relation to these issues.

APPENDIX 6

AUTHORISING OFFICERS

1. The Chief Executive – Aubrey Fawcett
2. The Head of Education – Ruth Binks
3. The Head of Legal & Property Services – Gerard Malone
4. The Head of Safer & Inclusive Communities – current Acting Head, Martin McNab

(As at 1 March 2017)