

---

<b>Report To:</b>	<b>Policy &amp; Resources Committee</b>	<b>Date:</b>	<b>21 November 2023</b>
<b>Report By:</b>	<b>Head of Legal, Democratic, Digital &amp; Customer Services</b>	<b>Report No:</b>	<b>LS/112/23/IS</b>
<b>Contact Officer:</b>	<b>Iain Strachan</b>	<b>Contact No:</b>	<b>01475 712498</b>
<b>Subject:</b>	<b>Updated Policy and Annual Update on the use of surveillance powers - The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)</b>		

---

## 1.0 PURPOSE AND SUMMARY

1.1  For Decision  For Information/Noting

1.2 The purpose of this report is to seek approval of an updated version of the Council's RIPSA Policy and to provide an overview and update on the use of directed surveillance powers by the Council.

1.3 The Council has also recently been the subject of a regular inspection by the Investigatory Powers Commissioner's Office, and an update on that is also included in this report.

## 2.0 RECOMMENDATIONS

2.1 It is recommended that the Committee notes the contents of this report, including the recent inspection by the Investigatory Powers Commissioner's Office.

2.2 It is recommended that the Committee approves the updated Regulation of Investigatory Powers (Scotland) Act 2000 Policy appended to this report in Appendix 3.

2.3 It is recommended that the Committee note a further annual update, including a review of the Regulation of Investigatory Powers (Scotland) Act 2000 Policy, will be provided in a year's time.

**Iain Strachan**  
**Head of Legal, Democratic, Digital & Customer Services**

### **3.0 BACKGROUND AND CONTEXT**

- 3.1 The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. To ensure that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of unaided surveillance and surveillance devices.
- 3.2 Where this surveillance is covert i.e. the subject of the surveillance is unaware that it is taking place, then it must be authorised in accordance with the relevant regulations 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.
- 3.3 The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) provides a legal framework for the use, deployment, duration and effectiveness of covert surveillance and the use of covert human intelligence sources. The Council must comply with RIPSA and adhere to the authorisation procedures specified in the Council’s RIPSA Policy and related procedures. The Investigatory Powers Commissioner’s Office (IPCO) provides independent oversight of the use of the powers contained within RIPSA. This oversight includes inspection visits by IPCO inspectors on a 3-yearly basis.
- 3.4 Under the Council’s authorisation procedures, applications for directed surveillance are authorised by a restricted number of Authorising Officers at Appendix 4 of the Council’s RIPSA Policy. A central register of authorisations is maintained by the Head of Legal, Democratic, Digital and Customer Services who also carries out a gate-keeping role in connection with draft applications.

### **4.0 PROPOSALS**

#### **Overview of RIPSA**

- 4.1 The Council’s RIPSA Policy and its procedures applies where ‘Directed Surveillance’ is being planned or carried out. Directed Surveillance can only be conducted to achieve one of more of the permitted RIPSA purposes, namely (i) preventing or detecting crime or prevention of disorder, (ii) in the interests of public safety or (iii) protecting public health. Directed surveillance is covert and is undertaken for the purpose of a specific investigation to obtain private information.
- 4.2 All applications for authorisations or renewals of authorisations must be reviewed by one of the Council’s Authorising Officers, with an appropriate form having first been completed by a relevant Council officer. Authorisations should be made in writing but can be made verbally in cases of emergency. Authorising Officers must be satisfied that the authorisation is (i) necessary - where there is no reasonable and alternative way of achieving the objective, and (ii) proportionate - any use of the surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.
- 4.3 Key points in relation to the Authorisation Process are outlined below:-

#### Time Periods

Written authorisations expire after three months in the case of directed surveillance. Oral applications expire after 72 hours.

#### Review

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

### Renewals

If at any time before an authorisation would expire the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed for a further period beginning on the day on which the previous authorisation ceases to have effect.

### Cancellation

The Authorising Officer must cancel an authorisation if satisfied that the directed surveillance no longer satisfies the criteria for authorisation, the use or conduct of the source no longer satisfies the criteria for authorisation or procedures for the management of the source are no longer in place.

- 4.4 Appendix 2 of the RIPSAs Policy gives guidance on information that should be included by those that complete RIPSAs authorisations and is for the benefit of Authorising Officers in reviewing the application. Appendix 3 also gives guidance for officers to consider on the potential application of RIPSAs when using the internet or social media sites for Council purposes. Whilst this guidance is of a more operational nature it is felt appropriate to include in the Policy, given the developments in this area, and the need to ensure any such covert surveillance is appropriate. The Council also advised IPCO that this additional guidance would be included.
- 4.5 The Committee was last updated on the Council's RIPSAs activity in September 2022, and it is important that elected members receive regular updates on the Council's use of its surveillance powers, given their potentially intrusive nature. Since the last report to the Committee in September 2022, there has been no further use of surveillance which was authorised under RIPSAs. Training sessions have been held with Authorising Officers and those officers that are most likely to make use of RIPSAs. It should also be noted that the Council has not made any use of covert human intelligence sources in the period since the September 2022 report, and any such use is considered highly unlikely. A link to the report to the Committee in 2022 is included here <https://www.inverclyde.gov.uk/meetings/meeting/2482>. An updated version of the Policy will assist with the Council's compliance.

### **IPCO Inspection**

- 4.6 As was anticipated, and reported to the Committee in September 2022, the Council has also recently been the subject of a regular inspection by IPCO. This inspection took the form of the Council providing a written update on its compliance with RIPSAs. A copy of IPCO's correspondence with the Council, which includes an explanation for the reason why IPCO is now carrying out an alternative approach to oversight of local authorities, is included in Appendix 1 to this report, comprising letters of 2 May, 15 June and 16 June 2023. It is to be noted that IPCO confirmed it is satisfied that the Council provided assurance that ongoing compliance with RIPSAs will be maintained and a further inspection this year will not be required. The next inspection will be 2026.

### **Review of the Council's RIPSAs Policy**

- 4.7 As is set out in the Council's correspondence with IPCO, going forward the Council will be conducting an annual review of its RIPSAs Policy, in order to meet IPCO's expectations and to also ensure the Policy and the Council's practices remain up to date with good awareness across the Council.

- 4.8 The proposed changes to the RIPSAs Policy are mainly minor in nature, with the only ones of note being the inclusion of additional guidance around the potential application of RIPSAs to Council activity being conducted on social media sites. The Policy has, however, had removed from it aspects that were much more operational in nature, for instance details of the forms to be used and the Standard Operating Procedure for the use of technical equipment for directed surveillance, which will be made available separately to staff and on ICON. Appendix 2 to this report does, however, include a table which summarises the proposed changes to the Policy, with the updated Policy being included in Appendix 3 to this report.
- 4.9 The Council's cross-service Information Governance Steering Group has been consulted on these changes to the RIPSAs Policy.

## 5.0 IMPLICATIONS

- 5.1 The table below shows whether risks and implications apply if the recommendation(s) is(are) agreed:

SUBJECT	YES	NO
Financial		X
Legal/Risk	X	
Human Resources		X
Strategic (Partnership Plan/Council Plan)		X
Equalities, Fairer Scotland Duty & Children/Young People's Rights & Wellbeing	X	
Environmental & Sustainability		X
Data Protection		X

### 5.2 Finance

One off Costs

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

Annually Recurring Costs/ (Savings)

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

### 5.3 Legal/Risk

RIPSA provides a legal framework for authorising covert surveillance by public authorities and an independent inspection regime to monitor these activities within the United Kingdom. If RIPSAs has been complied with, then any interference with an individual's privacy will be in accordance with the law. Failure to act in accordance with RIPSAs could result in a complaint being raised with the Investigatory Powers Tribunal. There are clear risks to the Council if unlawful surveillance

was to be undertaken, and keeping the RIPSA Policy under regular review, with appropriate support and training to staff, will mitigate against this,

**5.4 Human Resources**

There are no direct Human Resources implications arising from this report.

**5.5 Strategic**

There are no strategic implications directly arising from this report.

**5.6 Equalities, Fairer Scotland Duty & Children/Young People**

(a) Equalities

This report has been considered under the Corporate Equalities Impact Assessment (EqIA) process with the following outcome:

X	YES – Assessed as relevant, an EqIA is required and is available on the Council’s website.
	NO – This report does not introduce a new policy, function or strategy or recommend a substantive change to an existing policy, function or strategy. Therefore, assessed as not relevant and no EqIA is required. Provide any other relevant reasons why an EqIA is not necessary/screening statement.

(b) Fairer Scotland Duty

If this report affects or proposes any major strategic decision:-

Has there been active consideration of how this report’s recommendations reduce inequalities of outcome?

	YES – A written statement showing how this report’s recommendations reduce inequalities of outcome caused by socio-economic disadvantage has been completed.
X	NO – Assessed as not relevant under the Fairer Scotland Duty for the following reasons: Provide reasons why the report has been assessed as not relevant.

(c) Children and Young People

Has a Children’s Rights and Wellbeing Impact Assessment been carried out?

	YES – Assessed as relevant and a CRWIA is required.
X	NO – Assessed as not relevant as this report does not involve a new policy, function or strategy or recommends a substantive change to an existing policy, function or strategy which will have an impact on children’s rights.

## **6.0 CONSULTATION**

6.1 The Information Governance Steering Group and the Corporate Management Team have been consulted on the updated RIPSA Policy.

## **7.0 BACKGROUND PAPERS**

7.1 None

# IPCO

Investigatory Powers  
Commissioner's Office

PO Box 29105, London  
SW1V 1ZU

02 May 2023

Ms. Louise Long  
Chief Executive  
Inverclyde Council  
24 Clyde Square  
Greenock  
PA15 1LY



Dear Chief Executive,

During 2023, your Council is due its usual three-yearly inspection by IPCO, regarding its compliance with RIPSAs 2000 and the Investigatory Powers Act 2016. Your local authority was last inspected in June 2020.

Following a review of how IPCO conducts its oversight of local authorities, we shall no longer undertake routinely an inspection as has previously been the case. Instead, the Investigatory Powers Commissioner (IPC) has agreed that each local authority should provide a written update, in the first instance, on its compliance with the legislation. This will enable us to assess whether or not a remote, or in some cases, in-person inspection is required. This approach takes cognisance of the general decline in the use of covert powers by many local authorities, and seems the right approach for now, based upon our assessment of risk and where our limited resources are best directed for the coming year.

It is, of course, the responsibility of your authority to ensure that any covert activity is conducted in accordance with the legislation. The IPC expects early notification of any Errors in the use of the powers, which will then be investigated fully. However, generally speaking, if you have not used the powers since your last inspection, and your responses to the questions below assure us of having maintained good levels of compliance, we shall probably require no further engagement. Where the powers have been used, or you are planning to use them in the near future, an appropriate discussion with an Inspector will be arranged in order to help us form a view of the approach you are taking.

In addition, we will conduct a dip sample of in-person inspections during the coming year. This might include your authority, even if you have not used the powers for some time. You will be given sufficient prior notice if this is the case.

I have been allocated your Council to inspect this year. If you wish to discuss anything in advance of sending me your response, please feel free to get in touch.

I should be grateful if you would provide me with the following details through a return email. Please ensure that your contact details or those of your Senior Responsible Officer, through whom you might wish to respond, are provided in that reply.

The IPC expects you to have paid ongoing, due regard to the requirements of the legislation and associated Codes of Practice and seeks your written confirmation of the following:

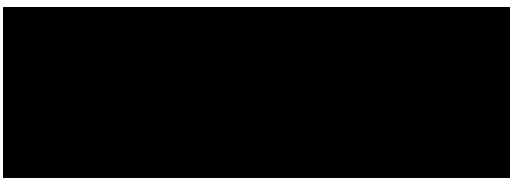
1. Any Areas of Non-Compliance identified at your last inspection have been remedied
2. Your RIPSAs Policy is subject to annual review and submitted to your Elected Members for approval (please advise when this was most recently revised and shared with Members)
3. Training, both initial and ongoing for key officers, plus awareness training for all staff, is provided (please provide dates since the last inspection)
4. A Central Record that meets the requirements of the relevant Codes of Practice is in place
5. You have a named SRO in place, as well as designated Authorising Officers
6. You have policies and training that appropriately cover the potential or actual use of social media as part of investigations/enforcement activities
7. The potential (for inadvertent, unauthorised) use of such media is actively monitored by managers
8. If you own/manage a town centre CCTV system, that this is operated and appropriately managed in line with RIPA considerations, including when used by third parties such as the local police.
9. Your Council has recognised and adheres to the Safeguards outlined in the relevant Codes of Practice in relation to its retention, review and destruction of material obtained through the use of covert powers.

Finally, in relation to use of the covert powers available to you, can you please confirm whether you have:

- Used the powers since the last inspection, or plan to use them imminently (or can envisage doing so following the formation of a new investigative/enforcement team or strategy)
- If you have used the powers, please provide an electronic copy of the relevant applications and authorisations for my review when you reply to this letter.

I look forward to hearing from you,

Yours faithfully,



**John Coull**  
**Oversight Inspector**  
**Investigatory Powers Commissioner's Office**  
Tel: [REDACTED] Email: [REDACTED]  
Check out our website at <https://www.ipco.org.uk>



Our Ref: LL/JMcL

Date: 15<sup>th</sup> June 2023

**Louise Long**  
**Chief Executive**  
Municipal Buildings  
Clyde Square  
Greenock  
PA15 1LY

Tel: [REDACTED]

Mr John Coull  
Oversight Inspector  
IPCO

Dear Sir

I write further to your letter of 2<sup>nd</sup> May 2023, and apologies for the delay in responding. The Council would respond to the points raised in your letter, as set out below.

**1. Any Areas of Non-Compliance identified at your last inspection have been remedied**

Whilst there were a number of observations and recommendations at the time of the last inspection, in June 2020, the Council does not believe that any areas of non-compliance were identified.

**2. Your RIPSAs Policy is subject to annual review and submitted to your Elected Members for approval (please advise when this was most recently revised and shared with Members)**

The Council's [RIPSA Policy](#) is not currently the subject of an annual review. The Council's Policy & Resources Committee did, however, receive an update on the Council's RIPSAs activity in September 2022. A copy of the report can be found [here](#), which (as noted in paragraph 4.4 of the report) will be an annual report going forward.

The annual report which will be submitted to Committee later in 2023 will also include a review of the RIPSAs Policy, which will likewise be undertaken annually going forward.

**3. Training, both initial and ongoing for key officers, plus awareness training for all staff, is provided (please provide dates since the last inspection)**

The Council instructed an external training provider, Act Now, to provide RIPSAs training in April and May 2022 to its five RIPSAs Authorising Officers and to another 12 officers who are most likely to make RIPSAs applications. The latter are mostly officers within the Council's Public Protection Service.

The Council will carry out internal refresher training sessions for its RIPSAs work in Summer 2023, which will again be primarily aimed at those officers described above.

In addition, the Council has a cross-service working group, the Information Governance Group (IGSG), whose purpose, as set out in its Terms of Reference (ToRs), is to:-

- support and drive the broader information governance agenda across the Council;
- ensure the effective management of all information governance risks; and
- provide assurance to the Council's Corporate Management Team that appropriate frameworks, work-streams and initiatives are in place to support, co-ordinate, promote, monitor, and assure the development and delivery of effective information governance.

RIPSA is a standing agenda item on the monthly meetings of the IGSG, and for 2023 one of its key tasks set out in its Terms of Reference is to oversee the “preparation and management of the Council’s external RIPSA inspection by the Office of the Investigatory Powers Commissioner”.

**4. A Central Record that meets the requirements of the relevant Codes of Practice is in place**

The Council holds a Central Register of RIPSA applications that meets the requirements of the relevant Codes of Practice.

**5. You have a named SRO in place, as well as designated Authorising Officers**

Senior Responsible Officer – Iain Strachan, Head of Legal, Democratic, Digital and Customer Services.

Designated Authorising Officers

Louise Long - Chief Executive

Ruth Binks - Corporate Director, Education, Communities & Organisational Development

Alan Puckrin - Chief Financial Officer

Stuart Jamieson - Director, Environment and Regeneration

Kate Rocks - Chief Officer, Inverclyde Health and Social Care Partnership

The Council’s Head of Legal, Democratic, Digital and Customer Services is also a Designated Authorising Officer. However, given his role as Senior Responsible Officer he would only consider authorising an application where (i) the application was urgent and, for whatever reason, no other authorising officer was available and (ii) another Council solicitor with sufficient knowledge of RIPSA was available to conduct a separate peer review on the application.

**6. You have policies and training that appropriately cover the potential or actual use of social media as part of investigations/enforcement activities**

The Council has covered off this area in the external training sessions delivered by Act Now in relation to the use of social media as part of investigations/enforcement activities. A copy of the presentation delivered by Act Now is enclosed with this letter.

The Council will again cover this in the training to be delivered this summer and will update its Policy later this year to also include additional guidance around such use of social media.

**7. The potential (for inadvertent, unauthorised) use of such media is actively monitored by managers**

As noted above, such use of social media for investigations/enforcement was included in the training delivered by Act Now, and the Council’s Policy will be updated to also include additional guidance around this. The Council is content that relevant managers know they need to undertake such active monitoring.

**8. If you own/manage a town centre CCTV system, that this is operated and appropriately managed in line with RIPA considerations, including when used by third parties such as the local police.**

Inverclyde Council operates its own Public Space CCTV system. We refer to our Covert Use of Public Space CCTV Guidance and Protocol with Police Scotland. In general, the system is used for general observation duties which do not require authorisation under RIPSA.

Public Space CCTV, including mobile CCTV, is also used for both planned and spontaneous events e.g. youth gatherings, unauthorised firework displays, marches and demonstrations and the like. RIPSAs authorisations are required where Police Scotland wish to carry out directed surveillance on individuals or groups using the system.

The use of the Public Space CCTV system is overt rather than covert.

**9. Your Council has recognised and adheres to the Safeguards outlined in the relevant Codes of Practice in relation to its retention, review and destruction of material obtained through the use of covert powers.**

The Council continues to adhere to the Security and Retention of Documents section of its RIPSA Policy. We have recently been revisiting our position on data assurance and as advised above this area will be addressed in our Policy renewal later this year.

In relation to retention/disposal of RIPSAs authorisations and associated records we can confirm the following.

The Council has a retention period of five years for RIPSAs Registers and Authorisations as well as associated records (correspondence, emails and the like).

The Council has a retention period of six months for RIPSAs Authorisations and associated records that are not approved.

Training records and Learning materials will be kept indefinitely for training purposes. However, no personal data or any Authorisations will be held as part of that.

**Finally, in relation to use of the covert powers available to you, can you please confirm whether you have:**

- Used the powers since the last inspection, or plan to use them imminently (or can envisage doing so following the formation of a new investigative/enforcement team or strategy)

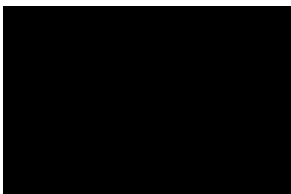
Please find attached electronic copies of our 2020 and 2021 Authorisations, one in each year.

- If you have used the powers, please provide an electronic copy of the relevant applications and authorisations for my review when you reply to this letter.

As above

Should you wish to discuss anything contained in this letter, then please feel free to contact myself, or my colleagues Iain Strachan, or Martin Hughes.

Yours sincerely



**Louise Long**  
**Chief Executive**

OFFICIAL

# IPCO

Investigatory Powers  
Commissioner's Office

PO Box 29105, London  
SW1V 1ZU

Ms. Louise Long  
Chief Executive  
Inverclyde Council  
24 Clyde Square  
Greenock  
PA15 1LY

16 June 2023

Dear Chief Executive,

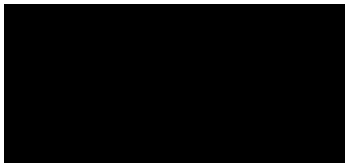
Thank you for providing IPCO with your response to the matters identified at points 1 to 9 of my Inspector's letter dated 2 May 2023.


I am satisfied that your reply provides your assurance that ongoing compliance with RIP(S)A 2000 and the Investigatory Powers Act 2016 will be maintained. As such, your Council will not require further inspection this year.

I would ask that you ensure that the key compliance issues continue to receive the necessary internal governance and oversight through yourself and your Senior Responsible Officer: policy refreshes; annual updates to your Elected Members; ongoing training and awareness raising; internal compliance monitoring by lead managers within their business areas; and the retention, review and destruction (RRD) of any product obtained through the use of covert powers (Records and Product Management in accordance with the Safeguards Chapters of the relevant Codes of Practice).

Your Council will be due its next inspection in 2026, but please do not hesitate to contact my Office if IPCO can be of assistance in the intervening period.

Yours sincerely,

  
**The Rt. Hon. Sir Brian Leveson**  
The Investigatory Powers Commissioner

 0207 389 8900

 [info@ipco.org.uk](mailto:info@ipco.org.uk)

 @IPCOOffice

 [www.ipco.org.uk](http://www.ipco.org.uk)

OFFICIAL

## SUMMARY OF PROPOSED REVISIONS TO RIPSA POLICY – NOVEMBER 2023

PAGE	TITLE	SECTION	PROPOSED CHANGE
1	Title Page	n/a	New Title Page
2	Document Control Page	n/a	New Document Control Section
3/4	Policy Statement	3	Minor deletion, and here and elsewhere changes to make clear is a policy and not a procedure
4	Objective of the Policy	3	Minor deletion
4	Scope of the Policy	5	Minor deletion and change of service name. Inclusion of reference to new Pre RIPSA Authorisation Review Form.
4/5	Principles of Directed Surveillance and the Use or Conduct of Covert Human Intelligence Sources	6	Minor amendments of roles
5/6	The Authorisation Process	7	Minor amendment for change of service name
7	Security and Retention of Documents	11/12	Minor amendments for changes of service name
8	Oversight and Complaints	12	Inclusion of IPCO website details
10	Appendix 1 - Definitions	n/a	Inclusion of text to make clear references to statute etc are to such provisions as amended from time to time
12/3	Appendix 3 – Internet & Social Media	n/a	Minor amendments and new sections inserted to give guidance on use of social media by officers carrying out surveillance which may involve RIPSA considerations, including in relation to online social media research carried out for child/adult protection work and test purchasing.
14	Appendix 4 – Authorising Officers	n/a	Changes to reflect changes in officers and job titles
-	Appendices 2 and 4 in previous Policy removed	n/a	Removed as more operational in nature, and will be made available separately to staff, including on ICON.

# Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Policy

Version 2.2

*Produced by:*  
*Information Governance Steering Group*  
*Inverclyde Council*  
*Municipal Buildings*  
*GREENOCK*  
*PA15 1LX*



**INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER  
THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE,  
OR COMPUTER DISC**

**DOCUMENT CONTROL**

<b>Document Responsibility</b>		
<b>Name</b>	<b>Title</b>	<b>Service</b>
Information Governance Steering Group	RIPSA Policy	Information Governance Steering Group
<b>Change History</b>		
<b>Version</b>	<b>Date</b>	<b>Comments</b>
1.0	August 2020	RIPSA Policy Review
2.0	August 2023	Revisions made by Information Governance (Solicitor)
2.1	October 2023	Revisions made by Head of Legal, Democratic, Digital & Customer Services
2.2	October 2023	Revisions made by Head of Legal, Democratic, Digital & Customer Services following CMT review
<b>Distribution</b>		
<b>Name/ Title</b>	<b>Date</b>	<b>Comments</b>
Information Governance Steering Group	August 2023	Minor amendments to Policy and new insertions at Appendix 3
Information Governance Steering Group	October 2023	Minor amendments
CMT	October 2023	Deletions of more operational/procedural aspects not required for a policy

*Distribution may be made to others on request*

<b>Policy Review</b>			
<b>Updating Frequency</b>	<b>Review Date</b>	<b>Person Responsible</b>	<b>Service</b>
Annually unless required earlier	November 2024	Information Governance Steering Group	Legal, Democratic, Digital and Customer Services

**Copyright**

***All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise without the prior permission of Inverclyde Council.***

## **1 Introduction**

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 policy 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.

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".

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**

Appendix 1 contains definitions of the terms used within this policy.

## **3 Policy Statement**

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").

The Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) together provide 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.

Inverclyde Council employees must adhere to the authorisation framework specified in this policy, and the associated procedures, before conducting any covert surveillance or using a source or allowing or conducting an undercover operation.



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 Policy**

The objective of this policy, and the associated 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 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". This policy, and the associated procedures, should be read in conjunction with RIPSA and the Scottish Government's Codes of Practice on covert surveillance and the use of covert human intelligence sources.

#### **5 Scope of the Policy**

This policy, and the associated 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 media sites (see Appendix 3).

This policy, and the associated 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.

In all cases of doubt, legal advice should be sought from the Head of Legal, Democratic, Digital and Customer Services.

Officers might also find it helpful to consider the Pre RIPSA Authorisation Review Form that is available from Legal, Democratic, Digital & Customer Services, to assist them in deciding whether or not a RIPSA authorisation is required in terms of this policy, and the associated procedures.

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

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

##### Lawful purposes

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

- for the purposes of preventing or detecting crime or the prevention of disorder
- in the interests of public safety
- for the purpose of protecting public health

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

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 legal limits in regard to this principle risks prosecution.

#### Confidential Material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of an Authorising Officer.

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

#### Vulnerable Individuals

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 Authorising Officer shall be required.

#### Juvenile Sources

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).

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

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.

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; and
- the Authorising Officer has satisfied himself/herself that any identified risks will be suitably managed

Deployment of juvenile sources will only be authorised by an Authorising Officer.

## **7 The Authorisation Process**

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 is attached at Appendix 4.

Authorising Officers within the meaning of this policy, and the associated procedures, 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.

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 Authorising Officer was available to grant the authorisation would, in the judgement of the Authorising Officer, be likely to endanger life or jeopardise the investigation or operation for which authorisation is being given.

All applications for authorisations or renewals of authorisations shall be made on the appropriate form, details of which can be obtained from Legal, Democratic, Digital & Customer Services. 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.

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.

All forms, codes of practice and supplementary material are available from the Head of Legal, Democratic, Digital and Customer Services.

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; and
- in the case of source work that satisfactory arrangements exist for the management of the source.

#### Necessity

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

#### Effectiveness

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

The Standard Operating Procedure (SOP) shall be followed when technical equipment is used in any directed surveillance operation. The SOP is available from the Head of Legal, Democratic, Digital and Customer Services.

#### Proportionality

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.

### Authorisations

Oral applications expire after 72 hours. 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.

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

### Review

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.

### Renewals

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.

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.

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

## **9 Cancellation**

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.

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 Scottish Government's Covert Surveillance Code of Practice). The IPCO preferred form of cancellation should always be used.

## **10 Monitoring**

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 2 for the matters that must be included in the record.

## **11 Security and Retention of Documents**

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 2018/the General Data Protection Regulation and Inverclyde Council's relevant policies and procedures.

The Head of Legal, Democratic, Digital and Customer 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.

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, Democratic, Digital and Customer Services with the authorising officer retaining a copy.

The Authorising Officer shall retain the copy forms for at least one year after cancellation. The Head of Legal, Democratic, Digital and Customer 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.

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.

## **12 Oversight and Complaints**

The Investigatory Powers Commissioner's Office (IPCO) provides an independent review of the use of the powers contained within RIPA. This review includes inspection visits by inspectors appointed by the IPCO. An independent tribunal, the Investigatory Powers Tribunal has full powers to investigate cases for use of surveillance. The website for the Investigatory Powers Tribunal has more information on its role and its work, including details of how a person can make a complaint to the Tribunal. <https://investigatorypowerstribunal.org.uk/>

## APPENDIX 1

**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.

References to any legislation, regulation, statutory instrument or the like is to the same as it may be varied, supplemented or replaced from time to time.

## APPENDIX 2

### 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 3

### THE INTERNET AND SOCIAL MEDIA 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 RIPSA 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.

Council officers may be called upon in the course of their duties to undertake surveillance by accessing website or social media content. Online activity applies equally to activities that are offline/in person operations.

Surveillance activities needing authorisation might include:

- visiting a third-party website or accessing social media posts, profiles or groups
- visiting/viewing websites, posts, profiles and/or groups regularly over a period of time
- entering into a personal relationship with a third party or parties via online or social media platforms.

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 seeking 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 requisite 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 written consent of the person whose identity is used.

#### Online Social Media Research in Child Protection cases

In relation to child protection work, social workers carrying out research online on social networking sites in the interests of the child may still engage an individual’s rights under Article 8 of the European Convention of Human Rights.

A documented decision trail will ensure that parameters are set, both to avoid any interference with Convention rights which is or may be disproportionate to the legitimate aim pursued, and for the protection of individual employees.

Applications to conduct online research in child protection cases will need to be authorised by the Authorising Officer for Inverclyde Health & Social Care Partnership or failing this, the Chief Executive or Head of Legal, Democratic, Digital and Customer Services.

The same approach will also apply to the carrying out of such research in adult protection cases too.

#### Test Purchases

The criteria for directed surveillance should be applied on a case by case basis. Council officers making undisclosed site visits or test purchases do not count as ‘covert human intelligence sources’ and such activities generally do not require formal authorization. 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. However, CHIS authorisation may be required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed.

#### **APPENDIX 4**

##### **AUTHORISING OFFICERS**

1. Louise Long, Chief Executive
2. Ruth Binks, Corporate Director, Education, Communities & Organisational Development
3. Alan Puckrin, Chief Financial Officer
4. Stuart Jamieson, Director, Environment and Regeneration
5. Kate Rocks, Chief Officer, Inverclyde Health and Social Care Partnership
6. Iain Strachan, Head of Legal, Democratic, Digital & Customer Services (but only (i) where the RIPSAs application is urgent and no other Authorising Officer is available and (ii) another Council solicitor with sufficient knowledge of RIPSAs is available to conduct a separate peer review of the application, given the Head of Legal, Democratic, Digital & Customer Services is also the RIPSAs Senior Responsible Officer)

(As at November 2023)

##### **SENIOR RESPONSIBLE OFFICER**

Iain Strachan, Head of Legal, Democratic, Digital and Customer Services