POLICY AND PROCEDURE ON COVERT SURVEILLANCE

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. INTRODUCTION

The Regulation of Investigatory Powers Act 2000 ("The UK Act") and the Regulation of Investigatory Powers (Scotland) Act 2000 ("The Act") provide a legal framework for covert surveillance by public authorities and prescribe procedures to ensure proper authorisation of surveillance activities.

These Acts are augmented by the following;

Scottish Governments Covert Surveillance and Property Interference Code of Practice 2017 https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/

Scottish Governments Covert Human Intelligence Sources Code of Practice 2017 https://www.gov.scot/publications/covert-human-intelligence-sources-code-practice/

OSC Procedures and Guidance 2016 https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

The Regulation of Investigatory Powers (Juveniles) (Scotland) Regulations 2002

The Regulation of Investigatory Powers (Cancellation of Authorisations) (Scotland) Regulations 2002

The Regulation of Investigatory Powers (Source Records) (Scotland) Regulations 2002

The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2000

The Act provides that "Directed Covert Surveillance" and the use of "Covert Human Intelligence Sources" shall be lawful for all purposes where

1) an authorisation provided in terms of the Act confers an entitlement to engage in the conduct in question and
2) the conduct is in accordance with the terms of the authorisation.

The objective of this Policy and Procedure is to ensure that all work involving the use of "direct surveillance" or the use of a "covert human intelligence source" is carried out effectively and in accordance with law.

Local authorities are permitted in terms of the Act to undertake "direct surveillance" and to use "covert human intelligence sources". Local Authorities are **not** permitted to carry out what is defined as "Intrusive Surveillance".

1. **"Directed surveillance"** is surveillance undertaken if it is covert and for:

(a) The purposes of a specific investigation or operation.

(b) In such a manner as is likely to result in the obtaining of private information about a person and;

(c) Otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation to be obtained for carrying out such surveillance.

2. **"Covert human intelligence source"** is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

(a) Uses such a relationship to obtain information or provide information or access to information to another person or;

(b) Discloses information obtained by the use of such a relationship or as a consequence of such a relationship.

3. **"Intrusive surveillance"** is:

(a) Carried out in relation to anything taking place in residential premises or in any private vehicle and;

(b) Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Intrusive surveillance requires authorisation by a Chief Constable. Employees of Argyll and Bute Council shall **not** authorise or carry out this form of surveillance.

2. PRINCIPLES OF SURVEILLANCE

2.1 Directed Covert Surveillance and the use of a Covert Human Intelligence Source (CHIS) shall be carried out only where necessary to achieve one or more of the permissive purposes as defined in the Act i.e.

(a) For the purpose of preventing or detecting crime or the prevention of disorder;

(b) In the interests of public safety
(c) For the purpose of protecting public health.

2.2 When considering whether directed covert surveillance or use of a CHIS is appropriate and necessary regard must be had to the following;

(a) Necessity – does it satisfy one of the grounds in the act.

(b) Proportionality – the use and extent of the directed surveillance must be in proportionate to what is sought to be achieved by carrying it out.

This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms.

It will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by less intrusive means.

(c) Intrusive Surveillance – no surveillance shall be undertaken where it falls within the definition of intrusive surveillance.

2.3 Collateral Intrusion - Consideration shall be given to the reasonable steps to be taken to minimise or avoid gathering information in regard to the subject or third parties that is not directly necessary for the purposes of the investigation being carried out.

2.4 Risk to Staff/Public – Consideration shall be given by authorising Officers in regard to the possible risks to staff or anyone else likely to be affected.

2.5 **<u>This Policy and Procedure does not apply to</u>**:

(a) 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).

An example would be 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.

(b) Tasks given to persons (whether that person is an employee of the Council or not) to ascertain purely factual information (for example the location of cigarette vending machines in licensed premises).

(c) Observations that are not carried out covertly or not your intention but based on your knowledge of the person subject to the surveillance.

(d) Unplanned observations made as an immediate response to events occurring at any time.

In cases of doubt the Application and Authorisation Process below should be followed.

3. APPLICATIONS AND AUTHORISATION PROCESS

3.1 Applications for Directed Surveillance or the use of Covert Human Intelligence Sources, or any application for renewal of authorisation, shall be authorised by the Regulatory Services and Building Standards Manager, Revenues and Benefits Manager or Operations Manager respectively but only following consultation with the Governance, Risk and Safety Manager or the Head of Legal and Regulatory Support on the merits of the application or the renewal.

Authorisations granted by a person shall be reviewed, renewed and cancelled by that same person unless that person is no longer available (eg, no longer employed), or it is impracticable for them to do so (eg, on holiday), in which case they may be reviewed, renewed and cancelled by any other officer with the power to authorise in terms of this paragraph.

3.2 **Consideration of Applications**

In considering applications authorising Officers shall have regard to the Principles of Surveillance as detailed above, the Act and regulations thereunder and the relevant guidance issued from time to time by the Scottish Executive.

Applications for Directed Surveillance shall be submitted in writing on form RIPSA Form 1. Applications for use of a CHIS shall be submitted in writing on Form RIPSA Form 4. Authorising Officers shall not authorise their own activities.

All authorisations for directed surveillance, other than emergency authorisations, **must be cancelled** after a period of 3 months beginning on the day from which they took effect.

All authorisations for use of a CHIS, other than emergency authorisations, **must be cancelled** after a period of 12 months beginning on the day from which they took effect.

Oral authorisations shall expire after a period of 72 hours from when they take effect. In urgent cases emergency application may be made and authorised orally.

In such emergency cases the applicant shall complete a RIPSA Form 1 in regard to Directed Surveillance and a RIPSA form 4 in regard to use of a CHIS and the authorising Officer shall record the authorisation in writing as soon as reasonably practicable thereafter.

3.3 **Acquisition of Confidential Material**

It is not envisaged that there shall be any directed surveillance where the purpose of such surveillance is to obtain information subject to legal privilege or confidential personal information i.e. information held in confidence relating to physical or mental health.

However where it is proposed to carry out directed surveillance for such a purpose then this **must** be authorised by the **Chief Executive or, in their absence, the Executive Director with responsibility for Legal and Regulatory Support** by way of application made in the first instance to the Governance, Risk and Safety Manager.

Where confidential material has been obtained then this must be clearly identified

as being confidential and care must be taken to avoid inappropriate disclosure.

Such material must not be copied, retained or disseminated unless it is of essential significance to the investigation.

All confidential material must be destroyed as soon as it is no longer essential to the investigation

3.4 Cancellation of Authorisation

Where an authorising Officer concludes that any authorisation granted by them has ceased to be either necessary or appropriate they shall cancel the authorisation and advise the applicant.

Cancellation of Directed Surveillance authorisation shall be recorded using form RIPSA Form 3. Cancellation of a CHIS authorisation shall be recorded using RIPSA Form 6.

3.5 Renewal of Authorisation

An authorisation may be renewed. All applications for renewal shall be made on the form RIPSA form 2 for Directed Surveillance and RIPSA form 5 for CHIS.

Applications should only be made shortly before the then existing authorisation is due to expire.

3.6 Review of Authorisations

Authorising officers will review authorisations at intervals of not more than one month.

Authorising officers shall review an authorisation following any significant occurrence or where the surveillance has resulted in the obtaining of confidential or sensitive personal information.

Review (form 2A) should be attached to the original application.

3.7 Matters Specific to Use of a CHIS

a) Authorisation for use of a Covert Human Intelligence Source can only be granted if sufficient arrangements are in place for handling the source's case.

The arrangements are those contained at Appendix 1 hereof.

b) 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.

Authorisation for the use of that covert human intelligence source shall be obtained in the usual way.

c) In relation to the use of Covert Human Intelligence Sources;

The use of vulnerable adults (i.e. mentally impaired) and children under 18 as a Covert Human Intelligence Source **shall not be authorised** without reference to the

relevant Head of Service considering the application.

Authorisation in such a case must ultimately be granted by the Chief Executive or, in her absence, the Executive Director with responsibility for Legal and Regulatory Support.

The use or conduct of any source under 18 years of age living with their parents cannot be authorised to give information about their parents.

Such sources can give information about other members of their immediate family in exceptional cases. A parent, guardian or other 'appropriate adult' should be present at meetings with a source under the age of 18 years.

The authorisation should not be granted unless or until:

The safety and welfare of the juvenile has been fully considered;

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

A risk assessment 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 or her deployment.

4. RECORDING AND PRESERVATION OF DOCUMENTATION

4.1 Each service will maintain a record of all applications and authorisations to include refusals, renewals, reviews and cancellations of authorisations.

All such documents must be treated as strictly confidential and services must make appropriate arrangements for their retention in accordance with the Data Protection Act and the RIPSA code of practice.

4.2 Each service will maintain a Progress Record Sheet in form RIPSA form 9.

4.3 Legal and Regulatory Support will maintain a central register of authorisations.

Authorising Officers will provide the original of any documentation relating to authorisations, refusals, renewals, reviews and cancellations of authorisations to the Executive Director with responsibility for Legal and Regulatory Support as soon as reasonably practicable after their authorisation by the authorising Officer.

4.4 Documentation in relation to authorisations to include refusals, renewals, reviews and cancellations of authorisations shall be reviewed by each service and by the Executive Director with responsibility for Legal and Regulatory Support at such times as to them may seem appropriate and, in any event, at intervals not exceeding three months.

4.5 All documentation held by each service and by the Executive Director with responsibility for Legal and Regulatory Support in the central register shall be retained for a period of 5 years after the cancellation of the authorisation to which it relates.

After the period of 5 years the Head of the appropriate service and the Executive Director with responsibility for Legal and Regulatory Support shall supervise their

destruction, except where the documentation may be relevant to any ongoing or future civil or criminal proceedings in which case these shall be retained for such further period as may be deemed appropriate.

Thereafter each service and the Executive Director with responsibility for Legal and Regulatory Support shall annually review all documentation and shall each authorise and supervise their destruction when appropriate.

Further information is available at Chapter 8 in each of the codes of practice previously mentioned.

5. ONLINE SURVEILLANCE

As part of any investigation Council Officers can request access to Facebook in order to obtain 'open source data' and must follow the Protocol for requesting Access to Facebook as detailed at Appendix 2.

Useful guidance around the use of social media for investigative purposes is contained in paras 3.11 to 3.16 of the SG code on covert surveillance and property interference and paras 4.7 to 4.14 of the SG code on covert human intelligence sources detailed in the introduction.

6. OVERSIGHT

The Investigatory Powers Commissioners Office (IPCO) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers (Scotland) Act 2000. This oversight includes inspection visits by Inspectors appointed by the IPCO.

7. COMPLAINTS

The Regulation of Investigatory Powers Act 2000 (the 'UK Act) establishes an independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction. Details of the complaint procedure may be obtained from;

Investigatory Powers Tribunal
PO Box 33220
London, SW1H 92Q tele: 0207 273 4514

APPENDIX 1

Arrangements for handling a CHIS.

There will at all times be a person holding the requisite office, rank or position within 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. If the CHIS is an employee their line manager will be the best person to act as the Handler.

There will at all times be another person holding the requisite office, rank or position within 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 would be the handler with oversight by the Controller and the Authorising Officer.

The record relating to the use of that source are maintained by Argyll and Bute Council which will always contain particulars of such matters as may be specified in regulations and codes of practice made by the Scottish Ministers (see below).

The records maintained by Argyll and Bute Council that discloses 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.

There must always be consideration of the following;

Necessity - does it satisfy one of the grounds in the act.

Effectiveness - Planned undercover operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

Proportionality - the use and extent of the CHIS must be in proportionate to what is sought to be achieved by carrying it out.

This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms.

It will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by less intrusive means.

- Examples of when a CHIS may be necessary can be found at paragraphs 2.18, 2.23 and 2.25 of the SG code of practice on covert human intelligence sources detailed in the introduction.

APPENDIX 2

Protocol for requesting Access to Facebook for purposes of an investigation

This protocol is to regulate the procedure where any Council Officer involved in an investigation considers it necessary that they access Facebook in order to obtain 'open source' information which will assist them in the investigation.

1. (Name of Service) has set up a Facebook account (Name of account) for the purpose of allowing any authorised Officer involved in an investigation to access Facebook in order to obtain 'open source' information.

2. In order to access this page on Facebook the investigating Officer must email the authorising officer or their nominated representative to obtain authorisation to access the Facebook account.

3. If at any point the investigating is restricted from accessing information from the targeted account then they must log out immediately not must attempt to obtain or obtain information from that account.

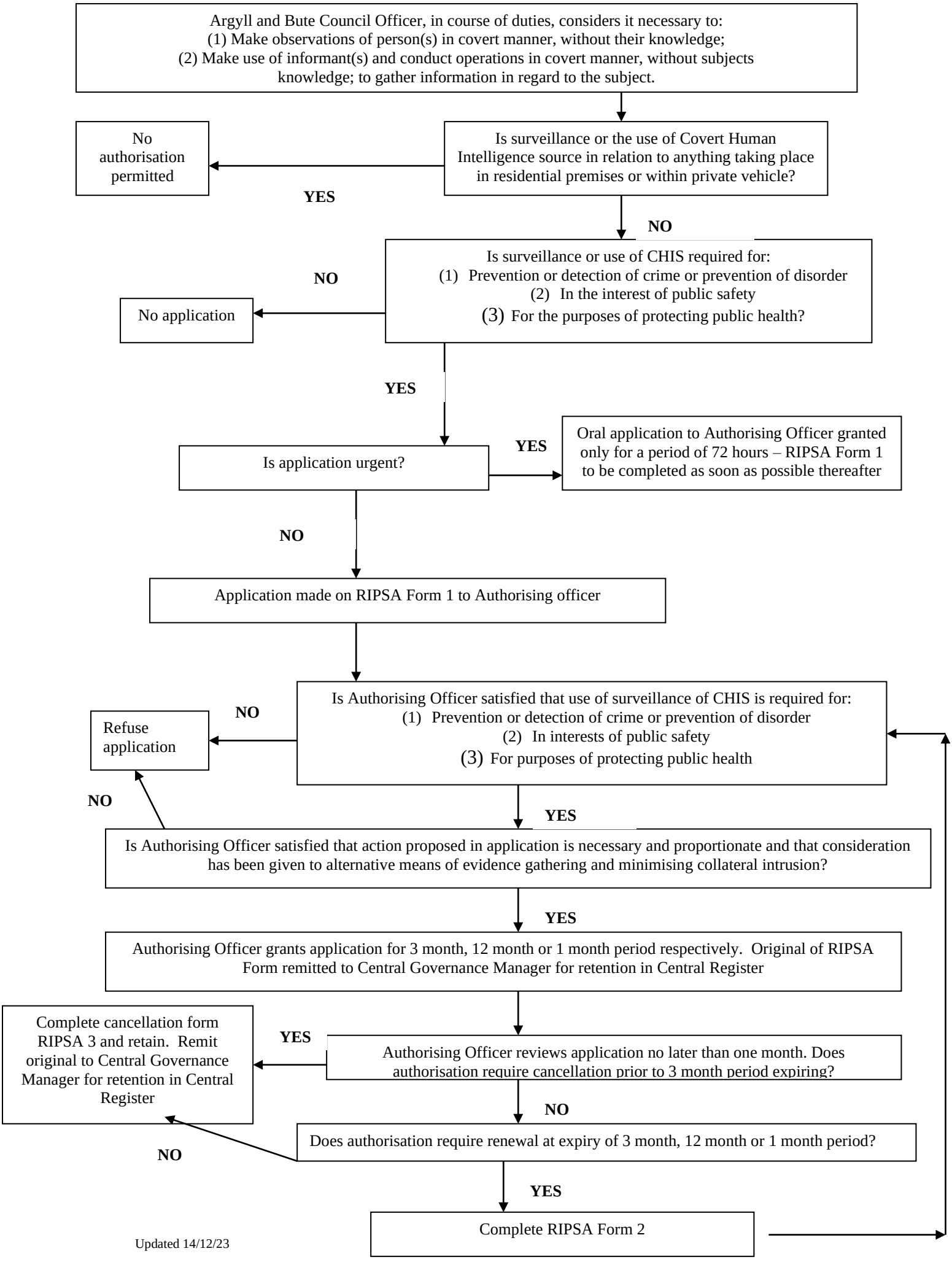
4. The password for the Facebook account is confidential and must not be shared with any other party. The password will be changed every two months.

5. A central log of all authorisations must be kept by the Authorising Officer and a report submitted to their Departmental Management Team (DMT) annually.

6. An annual report on the use of this protocol must also be submitted to the Council as part of the annual report on the use of RIP(S)A.

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

INDEX OF FORMS



Updated 14/12/23