Bath & North East Somerset Council		
MEETING:	**Council**	
MEETING DATE	**19th September 2024**	
TITLE:	**Annual Report on the use of the Regulation of Investigatory Powers Act 2000 (RIPA) & Investigatory Powers Act (IPA) 2016**	
WARD:	**All**	
AN OPEN PUBLIC ITEM		
List of attachments to this report: **Appendix 1 Usage Statistics 2023-2024** **Appendix 2 RIPA & IPA training module** **Appendix 3 RIPA & IPA Policy**		

1 THE ISSUE

1.1 This report updates council on the use of Regulation of Investigatory Powers Act and Investigatory Powers Act, Policies, and Procedures.

2 RECOMMENDATION

The Council is asked to:

2.1 Note the summary of statistics on the use of Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 (RIPA/IPA) by the council (Appendix 1);

2.2 Note the RIPA & IPA training module (Appendix 2); and

2.3 Adopt the Home Office Covert Human Intelligence sources code of practice (revised December 2022) set out at paragraph C.1.13 of the Council's Policy on the use of Regulation of Investigatory Powers Act 2000 (RIPA) & Investigatory Powers Act (IPA) 2016 (Appendix 3).

3 THE REPORT

3.1 **T**he Regulation of Investigatory Powers Act 2000 permits Councils to carry out covert (secret) surveillance of alleged offenders for the prevention and detection of

crime and the protection of public health. This is undertaken by either the use of directed surveillance or the use of a covert human intelligence source (CHIS). The Investigatory Powers Act 2016 allows the council to apply to telecommunications providers for data information (but not the contents of communications) about individuals who are suspected of committing crimes. when RIPA & IPA are applied, It ensures that the actions taken by the council comply with the human rights act 1998. resource implications (finance, property, people)

3.2 The Investigatory Powers Commissioner's Office (IPCO) is responsible for the inspection of public authorities with regard to compliance with RIPA & IPA. The council has previously been inspected in May 2014 and June 2017 and in 2020 a 'desk top' inspection was undertaken. the frequency of inspection for local authorities is every 3 years and in all likelihood the council will be inspected in the near future.

3.3 A summary of the Council's Annual Return on its use of RIPA and IPA powers to the IPCO is at Appendix 1.

3.4. The Council is committed to the continued professional development of Officers using RIPA and IPA powers. Officers using RIPA and IPA powers, therefore, are required to undergo annual training. The RIPA and IPA training module has been updated this year and made available through the Council's online 'Learning Zone' portal with a Certificate generated on successful completion of the training module. The Learning Zone is available to all Officers and will be available to the IPCO on inspection. A link to the RIPA and IPA training module is at Appendix 2.

3.5 The Council's Policy on the use of Regulation of Investigatory Powers Act 2000 (RIPA) & Investigatory Powers Act (IPA) 2016 is at Appendix 3 and note that paragraph C.1.13 provides a link to the Home Office Covert Human Intelligence Sources Revised Code of Practice revised December 2022.

4. CHANGES [IPCO] THE INVESTIGATORY POWERS COMMISSIONER'S OFFICE AND THE OFFICE FOR COMMUNICATIONS DATA AUTHORISATIONS (OCDA) HAVE MERGED

4.1 A merger has taken place to combine the [IPCO] the Investigatory Powers Commissioner's Office and the Office for Communications Data Authorisations (OCDA) . The merger has been completed. The combined authorisation will be known as ***"The Investigatory Powers Commissioner's Office (IPCO) With A New Tagline: Authorisation And Oversight***".

4.2 The primary purpose of the merger is to make the business and administration processes of the two organisations more efficient, while protecting the independent decision making and oversight functions of each.

Sir Brian Leveson stated :"I am delighted to announce formally the merger of IPCO and OCDA. I am immensely proud of the work achieved by both organisations to date in overseeing and authorising the use of investigatory powers. IPCO was set up following the Investigatory Powers Act 2016 and OCDA was established some two years later following amendments to the IPA, each with different resources, functions and capability. At that later time, it was right that the organisations were separate and able to establish effective working practices for their different functions. Five years on, however, as IPCO and OCDA have matured and the working practices and support systems of the two organisations have aligned, it had made sense formally to join the two and to develop a

single, unified body. I am confident the merger will make administrative processes more efficient while preserving the independence of our statutory functions."

4.3 The name IPCO has been retained because the organisation's authorisation and oversight functions derive from powers delegated by the Investigatory Powers Commissioner, whose statutory role was created by the Investigatory Powers Act 2016.The merger will drive administrative change while the functions of authorisation and oversight will remain as before.

4.4 Applications to acquire communications data will continue to be considered by authorising officers exercising the delegated powers of the Investigatory Powers Commissioner and compliance with the Act and the Codes of Practice will still be overseen by teams of inspectors reporting back to the Investigatory Powers Commissioner.

5. STATUTORY CONSIDERATIONS

5.1 The revised code on Covert Surveillance and Property Interference recommends that elected members should review the use of RIPA/IPA powers and set the policy annually.

6. RESOURCE IMPLICATIONS (FINANCE, PROPERTY, PEOPLE)

6.1 There are no direct implications arising from this report. Although the Council is an infrequent user of RIPA/IPA powers, the IPCO requires the Council 's procedures to remain in a good state of readiness should these need to be implemented. Consequently, the financial implications are limited to the cost of periodic refresher training for officers in the use of RIPA powers.

7. RISK MANAGEMENT

7.1 A risk assessment related to the issue and recommendations has been undertaken, in compliance with the Council's decision-making risk management guidance.

8. CLIMATE CHANGE

8.1 There are no impacts on climate change arising from this report.

9. OTHER OPTIONS CONSIDERED

9.1 None

10. CONSULTATION

10.1 The Monitoring Officer and Council S.151 Officer have been consulted on the contents of this report.

Contact person	Michael Hewitt tel: 01225 395125
Background papers	None
Please contact the report author if you need to access this report in an alternative format	

APPENDIX 1

Annual Return - Key Statistics 2023-2024

SURVEILLANCE DATA

None

COMMUNICATIONS DATA*

1

REQUEST FOR USE OF COUNCIL CCTV BY PARTNER ENFORCEMENT AGENCIES

None

Key Statistics 2023-24

SURVEILLANCE DATA

None

COMMUNICATIONS DATA

None

REQUEST FOR USE OF COUNCIL CCTV BY PARTNER ENFORCEMENT AGENCIES

None

APPENDIX 2

RIPA TRAINING PLAN

RIPA-IPA TRAINING 2023-2024
(LINK BELOW)

https://www.youtube.com/watch?v=tdhHinlgkUE

APPENDIX 3

BATH AND NORTH EAST SOMERSET COUNCIL

Policy on

Regulation of Investigatory Powers Act 2000 (RIPA)

and

Investigatory Powers Act 2016 (IPA)

Revised August 2024

BATH AND NORTH EAST SOMERSET COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

&

INVESTIGATORY POWERS ACT 2016 (IPA)

POLICY

CONTENTS

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

&

INVESTIGATORY POWERS ACT 2016 (IPA)

A.1 **Purpose**

The purpose of this Policy and accompanying guidance is to explain:

- the scope of RIPA and IPA
- the circumstances where these apply

A.2 **Introduction**

A 2.1 **RIPA** - which came into force in 2000, regulates the use of investigatory powers exercised by various bodies including Local Authorities, and ensures that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and that, judicial approval is obtained before they are carried out.

A 2.2 **IPA** - which came into force in 2019, regulates the acquisition and disclosure of Communications Data (CD) by various bodies including Local Authorities. This is achieved by requiring application for CD to be facilitated by collaboration with the National Anti-Fraud Network (NAFN) and approved by the Investigatory Powers Commissioner's Office(INVESTIGATORY POWERS COMMISSIONER'S OFFICE)

A 2.3 This policy sets out Bath and North East Somerset Council's (the Council) position in relation to RIPA and IPA. Part I deals with RIPA and Part II deals with IPA

A 2.4 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of human rights is justified in the interests of the community as a whole, or whether the information could be obtained in other ways.

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

PART I – RIPA

B 1.0 The investigatory powers, which are relevant to a Local Authority, are directed covert surveillance in respect of specific operations involving criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months imprisonment, or are related to the underage sale of alcohol and tobacco and the use of covert human intelligence sources (CHIS). The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and these can be viewed at

https://www.gov.uk/government/collections/ripa-codes

B 1.1 This policy sets out the practice to be followed before any covert surveillance is undertaken. The Council will only carry out covert surveillance where such action is necessary, proportionate and justified and will endeavour to keep such surveillance to a minimum. The Council recognises its obligation to comply with RIPA when such an investigation is for the purpose of preventing or detecting crime, preventing disorder or the protection of public health and has produced this document as guidance to assist officers. The procedures and guidance set out in this Policy are based on the provisions of RIPA, the Home Office Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources (CHIS), the Home Office guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance and guidance issued by the Investigatory Powers Commissioner. See

B 1.2 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases, investigations carried out by Council officers will not be subject to RIPA, as they involve overt rather than covert surveillance (see below).

B 1.3 RIPA does:

- require prior authorisation and judicial approval of directed covert surveillance
- prohibit the Council from carrying out intrusive surveillance
- require prior authorisation and judicial approval of the conduct and use of CHIS
- require safeguards for the conduct and use of CHIS.

B 1.4 RIPA does not:

- prejudice any existing powers available to the Council to obtain information by any means not involving conduct requiring authorisation under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or from the Land Registry as to the ownership of a property.
- authorise the use of directed covert surveillance unless the crime threshold is met.

B 2.0 **Applications for Authorisations**

B 2.1 All applications for authorisation in accordance with RIPA must be considered by one of the Council's designated authorising officers. Schedule 1 of this Policy identifies the officers authorised to act as the Council's designated persons. Any incomplete or inadequate application forms will be returned to the Applicant Officer for amendment. The Authorising Officer shall in particular ensure that:

- a criminal offence is being investigated;
- there is a satisfactory reason for carrying out the surveillance;
- the crime threshold is met or the offences relate to the underage sale of alcohol or tobacco;
- the covert nature of the investigation is necessary;
- proper consideration has been given to collateral intrusion;
- the proposed length and extent of the surveillance is proportionate to the information being sought;
- the authorisations are reviewed and cancelled;
- records of all authorisations are sent to the Monitoring Officer for entry on the Central Register;
- an analysis of alternative methods, other than directed covert surveillance has been considered as a way of obtaining the necessary information together with reasons why those alternatives are inappropriate. This is to ensure that RIPA powers are used as a last resort;

B 2.2 After authorisation has been obtained from an authorising officer the Applicant Officer must attend the Magistrates' Court in order to obtain Judicial approval for the authorisation.

B 3.0 **Scrutiny and Tribunal**

B 3.1 The Council must obtain an order from a Magistrate approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity be carried out. The Council can only challenge a decision of the Magistrate on a point of law by way of judicial review.

B 3.2 The Investigatory Powers Commissioner (IPC) was set up to oversee and monitor compliance with RIPA operations carried out by public authorities. The IPC has "*a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA",* and the IPC will from time to time inspect and examine the Council's policies, records, operations and procedures for this purpose.

B 3.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g., directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

B 3.4 The Tribunal can order:

B 3.4.1 the quashing or cancellation of any warrant or authorisation;

B 3.4.2 the destruction of any records or information obtained by using a warrant or authorisation;

B 3.4.3 the destruction of records or information held by a public authority in relation to any person.

B 3.5 The Council has a duty to disclose to the Tribunal all documents it requires, if any Council officer has:

B 3.5.1 granted any authorisation under RIPA;

B 3.5.2 engaged in any conduct as a result of such authorisation.

B 4.0 **Benefits of RIPA Authorisations**

B 4.1 RIPA states that if authorisation is given to engage in a certain conduct and the conduct undertaken is in accordance with the authorisation (including judicial approval), then it will be lawful for all purposes. Consequently, RIPA provides a defence to an accusation of an infringement of a human right.

B 4.2 Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

B 5.0 **Statutory Definitions**

B 5.1 'Surveillance' includes:

B 5.1 monitoring, observing, listening to people, watching or following their movements, listening to their conversations and other such activities or communications.

B 5.1.2 recording anything mentioned above in the course of surveillance.

B 5.1.3 surveillance by, or with the assistance of, appropriate surveillance device(s).

Surveillance can be overt or covert.

B 5.2 **Overt surveillance** will include most of the surveillance carried out by the Council – there will be nothing secretive, clandestine or hidden about it. For example, sign posted CCTV cameras normally amount to overt surveillance (but see 6.6 and 7.3 below). In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases carried out by Environmental Health for food hygiene or other purposes), and/or will be going about Council business openly (e.g. a parking attendant walking through a Council car park.

B 5.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that noise will be recorded if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

B 5.4 Overt surveillance does not require any authorisation under RIPA. Neither does **low-level surveillance** consisting of general observations in the course of law enforcement (for example, where a planning officer drives past a site to check whether planning conditions

are being complied with). Repeated visits may amount to systematic surveillance, however, and require authorisation: if in doubt, legal advice should be sought. Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of a *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved.

B 5.5 **Covert surveillance** (S. 26(9)(a)) is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place. RIPA requires the authorisation to two types of covert surveillance (**directed surveillance** and **intrusive surveillance**) plus the use of CHIS.

B 5.6 **Directed surveillance** (s.26(2)) is surveillance which:

B 5.6.1 is covert; and

B 5.6.2 is not intrusive surveillance (see definition below – **the Council is prohibited by law from carrying out any intrusive surveillance**);

B 5.6.3 is not carried out in an immediate response to events where it would not be practicable to obtain authorisation under the Act;

B 5.6.4 is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation).

B 5.6 **Private information** in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact or associates with.

B 5.7 Similarly, although signposted town centre CCTV cameras do not normally require authorisation, this will be required if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular person or place.

B 5.8 Other examples of directed surveillance include:

B 5.8.1 officers following an individual over a period to establish whether s/he is working whilst claiming benefit.

B 5.8.2 test purchases where a hidden camera or other recording device is used.

B 5.9 Surveillance that is unforeseen and undertaken as **an immediate response** to a situation normally falls outside the definition of directed surveillance and, therefore, authorisation is not required. However, if a specific investigation or operation is subsequently to follow, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced.

B 5.10 **Intrusive Surveillance (s. 26(3))** occurs when surveillance:

B 5.10.1 is covert;

B 5.10.2 relates to residential premises and private vehicles; and

B 5.10.3 involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if it were in the premises/vehicle.

Residential premises do not include common areas to which a person has access in connection with their use of occupation for example hotel reception area or communal stairways.

B 5.11 Directed surveillance carried out at the following locations for the purpose of legal consultation shall be treated as intrusive surveillance:

B 5.11.1 Any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;

B 5.11.2 Police stations;

B 5.11.3 Hospitals where psychiatric services are provided;

B 5.11.4 The place of business of any professional legal adviser;

B 5.11.5 Any place used for the sittings and business of any court, tribunal, inquest or enquiry;

B 5.11.6 Any place which persons may be detained under certain circumstances provided by the Immigration Act 1971 or UK Border Act 2007.

Intrusive surveillance can be carried out only by police and other law enforcement agencies. **Council officers must not carry out intrusive surveillance.**

B 5.12 **'Covert human intelligence source'** (CHIS) (s.26(8)) is defined as a person who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or providing access to information to another person or covertly discloses information obtained through the use of such a relationship or as a consequence of the relationship.

B 5.13 **'Authorising Officer'** in the case of Local Authorities these are specified as Assistant Chief Officers (and more senior officers), Assistant Heads of Service, Service Managers or equivalent, responsible for the management of an investigation (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521). The Council's authorising officers are set out in Schedule 1 to this Policy.

B 5.14 **'Applicant Officer'** those council officers who apply for RIPA authorisation.

B 5.15 **'Crime Threshold'** applies to an authorisation for directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences

must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or be an offence under:

7.11.1 S.146 of the Licensing Act 2003 (sale of alcohol to children);

7.11.2 S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);

7.11.3 S.147A of the Licensing Act 2003 (persistently selling alcohol to children);

7.11.4 S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

B 6.0 **When does RIPA apply?**

Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime or of preventing disorder.

B 6.1 The Council can only authorise directed covert surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or be an offence under:

- S.146 of the Licensing Act 2003 (sale of alcohol to children);
- S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
- S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
- S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

B 6.2 CCTV – the normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV to target a specific individual or group of individuals via CCTV recordings.

B 6.3 The use of RIPA powers must be in relation to the performance of a core function of the Council and not 'ordinary functions' such as employment issues or contractual arrangements. It will include criminal misconduct investigations.

B 7.0 **Training**

B 7.1 Each Director shall be responsible for ensuring that relevant members of staff, involved with any aspect of covert surveillance, are aware of the Act's requirements.

B 7.2 The Monitoring Officer shall ensure that refresher training is offered once a year to all services of the Council and also give advice and training on request. Applicant Officers must have received training and bi-annual refresher guidance on RIPA.

B 8.0 **Central Register and Records**

B 8.1 A Central Register of all authorisations including the application for judicial approval, and Order form shall be retained by the Monitoring Officer. The content of the application forms

and authorisations will be monitored to ensure that they comply with the Act. The Monitoring Officer will report any breaches of this Policy or the Act's provisions to the Strategic Management Team of the Council

B 9.0 **Overview and Scrutiny**

B 9.1 The Monitoring Officer shall be the Senior Responsible Officer who will:

- ensure compliance with the Council's policy, relevant RIPA legislation and guidance;
- engage with commissioners and inspectors when the Council's inspection is due (usually every three years);
- oversee any post-inspection action plans recommended or approved by a Commissioner.

B 9.2 This policy shall be reviewed, and where necessary amended, at least once a year and the version control table at Schedule 2 updated accordingly. If requiring amendment, the revised policy shall be presented to and considered by the following:

- The Strategic Management Team
- The relevant Council Committee/Cabinet

B 9.3 The Senior Responsible Officer will report to the relevant Council committee/Cabinet, detailing the Council's use of RIPA powers, annually.

B 9.4 The Council's elected members will not be involved in any decisions made on specific authorisations granted.

B.10 **Internet & Social Media Policy**

B 10.1 In order to prevent and detect crime a social media policy has been introduced to ensure that a lawful process is followed when accessing Social Networking Sites "SNS" and the internet at Schedule 3

B.11.0 **Aerial Surveillance**

B 11.1 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft ('drones'), is planned, consideration must be given as to whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. If these devices are used in a covert and pre-planned manner, as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance.

C 1.0 **Covert Human Intelligence Source**

C 1.1 The RIPA definition (section 26) is anyone who:

C.1.1.1 establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs C 1.1.2 –C 1.1.3;

C 1.1.2 covertly uses such a relationship to obtain information or provide access to any information to another person; or

C 1.1.3 covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

C 1.2 Any reference to the conduct of a CHIS includes the conduct of a source which falls within C1.1.1 - C 1.1.3. or is incidental to it. References to the use of CHIS are references to inducing, asking or assisting a person to engage in such conduct.

C 1.3 Section 26(9) of RIPA goes on to define:

C 1.3.1 a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and

C 1.3.2 a relationship is used covertly, and information obtained as mentioned in section 26 (8)c and is disclosed covertly, if and only if, it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

C 1.4 The Council is only likely to use a CHIS in **very exceptional circumstances**, and advice should be sought from the Monitoring Officer before any authorisation is sought.

C 1.5 If the Monitoring Officer deems that the use of a CHIS is appropriate the application must be authorised and judicial approval obtained.

C 1.6 The provisions of RIPA relating to CHIS do **not** apply;

C .1.61 where members of the public volunteer information to the Council as part of their normal civic duties;
C 1.6.2 where the public contact telephone numbers set up by the Council to specifically receive information;
C.1.6.3 where test purchases are carried out in the normal course of business
C.1.6.4 where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti-social behaviour.

as none of these situations normally require a relationship to be established for the covert purpose of obtaining information.

C 1.7 If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation and judicial approval;

C.1.7.1 conduct – establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information

C.1.7.2 use – inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

C.1.8 One person within the Council will be responsible for tasking the source, dealing with them, directing their day-to-day activities and recording information supplied by them and monitoring their welfare and security. A risk assessment MUST be carried out at the start, during and after the investigation (see Schedule 3 and Section 29(5) of RIPA for the specific requirements that need to be satisfied and for details of the different persons required to undertake separate responsibilities).

C 1.9 Special safeguards exist for the use of individuals who are under the age of 18 years old as a CHIS. The Regulation of Investigatory Powers (Juveniles) Order 2000 details the special provisions that must be satisfied.

C.1.10 Only an Authorising Officer may grant an authorisation for the use of a juvenile as a CHIS. Under no circumstances may a juvenile under the age of 16 be authorised to act as a CHIS against the wishes of his parents or person who has parental responsibility for him/her. The duration of an authorisation for the use of a juvenile as a CHIS is one month.

C.1.11A vulnerable individual is a person who is or may be in need of community care services for reason of mental or other disability, age or illness or is unable to take care of himself or protect himself from significant harm or exploitation. Only in the most exceptional circumstances may an Authorising Officer grant an authorisation for the use of a vulnerable individual as a CHIS.

C.1.12 There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship which is authorised in the 2000 Act, not whether the CHIS is asked to do so by the Council. Where an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on the information from any such informant.

C 2.0 **Directed Surveillance**

C 2.1 All application forms see

https://www.gov.uk/government/collections/ripa-forms--2

must be fully completed by the Applicant Officer with the required details and sufficient information to enable to Authorising Officer to make an informed decision that he is satisfied and believes that RIPA is necessary and proportionate. The application form must also provide all the information required for approval by the Judiciary. No authorisation shall be granted unless the Authorising officer is satisfied that the RIPA authorisation is:

- Necessary for either the purpose of preventing or detecting crime or the prevention of disorder that involves a criminal offence or offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months imprisonment or are related to the underage sale of alcohol and tobacco (see paragraph 7.2 the policy above);

- Proportionate this means that:

  - the method of surveillance proposed is not excessive to the seriousness of the matter under investigation;

  - it must be the method that is least invasive of the individual or individual being observed;

  - the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 2.2 below); and

  - that no other form of investigation would be appropriate.

  The authorisation completed by the Authorising Officer should indicate that full consideration has been given to the above points and a record should be made on the appropriate forms.

  Both the Applicant Officer and Authorising Officer should refer to their training notes regarding the completion of the RIPA forms, with particular attention to necessity and proportionality.

C 2.2 The Authorising Officer must also take into account the risk of **'collateral intrusion'** i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation, particularly where there are special sensitivities e.g. premises used by lawyers, doctors or priests for any form of medical or professional counselling or therapy. The application form must include a detailed assessment of any risk of collateral intrusion for this purpose.

C 2.3 Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion. The Applicant Officer must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

C 2.4 A single authorisation may refer to a number of individuals but relate to a single investigation and are "same fact". However, necessity, proportionality and collateral intrusion should be considered individually. If particular subjects are subsequently ruled out of the investigation, those individuals should be removed at the next review. Such circumstances should prompt an early review.

C 2.5 Special consideration should be given in respect of confidential information. Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material (S98 – 100 Police Act 1997). The Chief Executive, Monitoring Officer or Deputy Monitoring Officer must sign any authorisation before judicial authority is sought.

C 2.6 Legal Privilege

This applies to legal consultation and includes communications or consultation between an individual and his/her legal adviser or a person representing their client in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. This also includes consultations with medical practitioners. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Monitoring Officer should be sought in respect of any issues in this area.

C 2.7 Confidential Personal Information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

C 2.9 Confidential Journalistic Material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered under RIPA may not necessarily be properly regarded as confidential under Section 41 Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Monitoring Officer.

C 3.0 **Judicial Approval of Authorisations**

C 3.1 Once the Authorising Officer has authorised the Directed Surveillance or CHIS the Applicant Officer (who completed the application form) should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Magistrate.

C 3.2 The Applicant Officer will provide the Magistrate with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Magistrate and should contain all the information that is relied upon.

C 3.3 In addition the Applicant Officer will provide the Magistrate with a partially completed judicial application/order form.

C 3.4 The hearing will be in the Magistrates' Court and the Applicant Officer will be sworn in and present the evidence as required by the Magistrate. Any such evidence should be limited to the information in the authorisation.

C 3.5 The Magistrate will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be so. He/she will also consider whether the authorisation was given by the appropriately designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

C 3.6 The Magistrate can:

C 3.6.1 approve the grant of the authorisation which means that the authorisation will then take effect; or

C 3.6.2 refuse to approve the grant of the authorisation which means the authorisation will not take effect but the Council may look at the reasons for the refusal, make amendments and re-apply for judicial approval; or

C 3.6.3 refuse to approve the grant of the authorisation and quash the original authorisation. The Court cannot exercise its power to quash the authorisation unless the Applicant Officer has at least two business days from the date of the refusal in which to make representations.

C 4.0 Notifications to Inspector/Commissioner

C 4.1 The following situations must be brought to the Inspector/Commissioner's attention at the next inspection:

- where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved;
- where a lawyer is the subject of an investigation or operation;
- where confidential personal information or confidential journalistic information has been acquired and retained.

C 5.0 Applications for CHIS

C 5.1 The process is the same as for directed surveillance except that the authorisation must specify the activities and identity of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

All application forms https://www.gov.uk/government/collections/ripa-forms--2

must be fully completed with the required details to enable the Authorising Officer to make an informed decision and to be approved by the Magistrate.

C 6.0 URGENT AUTHORISATIONS

C 6.1 Urgent authorisations should not normally be necessary. However, in exceptional circumstances, if the authorisation cannot be handled on the next working day the Court's out-of-hours service can be contacted. Legal Advice should be sought from the Monitoring Officer about whether it is appropriate to utilise this facility.

C 6.2 If the need for authorisation has been neglected, or if the situation is of the Applicant Officer's own making, this will not amount to an urgent or exceptional circumstance.

C 7.0 Duration and Cancellation

C 7.1 Every authorisation and every renewal (except in the cases of oral authorisations or where the use of a juvenile CHIS is being authorised) must be for the designated statutory period. If the operation is to only last for a short time, this is information which should be considered in the review and/or cancellation.

C 7.2 An authorisation for directed surveillance shall cease to have effect (if not renewed) 3 months less one day from the date of judicial approval but still requires to be cancelled using the appropriate form even if the surveillance is required for less than 3 months.

C 7.3 An authorisation for CHIS shall cease to have effect (unless renewed) 12 months from the date of judicial approval but it is still necessary to cancel the authorisation using the appropriate form.

NOTE:

Authorisations should continue for the minimum period reasonable for the purpose they are given and then cancelled promptly.

C 8.0 **Reviews**

C 8.1 The Authorising Officer should review all authorisations prior to their expiry date and at intervals determined by him/herself. This should be as often as necessary and practicable. Particular attention should be paid to the possibility of obtaining confidential information. The Applicant Officer can do the necessary research and prepare the papers for the review but the actual review is the responsibility of the original Authorising Officer and should be conducted by him. Necessity and proportionality should be reconsidered if the surveillance is to continue.

C 8.2 The Applicant Officer must make the Authorising Officer aware of any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in further or greater intrusion into the private life of any person by means of a review. The Authorising Officer should consider whether the proposed changes are proportionate before approving or rejecting them.

C 8.3 Where authorisation is given for the surveillance of unidentified individuals whose identity is later established, the review should include reference to their identity. A fresh authorisation will not be necessary if the investigation remains the same.

C 8.4 Evidence of the review should be recorded.

C 9.0 **Renewals**

C 9.1 Any Authorising Officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect. This renewal must then be approved by a Magistrate in the same way the original authorisation was approved. The process set out in C 3.0 above should be followed.

C 9.2 A CHIS authorisation must be thoroughly reviewed before any application for renewal is sought. Once the Authorising Officer has approved an application to renew, that application must then be approved by a Magistrate in the same way that the original authorisation was approved. The process set out in C 3.0 above should be followed.

C 10. **Central Register of Authorisations**

C 10.1 The Council must maintain the following documents:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorised Officer;
- a copy of the order made by the Magistrate;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation and order made by the judiciary and supporting documentation submitted when the renewal was requested;

- the date and time when any instruction was given by the Authorising Officer.

C 10.2 To comply with C 10.1 above the Monitoring Officer will hold the central register of all authorisations issued by Authorising Officers of the Council. The original copy of every authorisation, judicial order, review, renewal and cancellation issued should be lodged immediately with Legal Services in an envelope marked 'Private and Confidential'.

C 10.3 The Council must also maintain a centrally retrievable record of the following information for a period of 3 years or until the next IPC inspection whichever is the latter:

- type of authorisation
- date the authorisation was given
- date the Order was made by the Magistrate
- name and rank/grade of the Authorising Officer
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation;
- whether urgency provisions were used, and if so why
- details of renewal
- whether the investigation/operation is likely to result in obtaining confidential information
- whether the authorisation was granted by an individual directly involved in the investigation
- date of cancellation

These records will be retained for at least 3 years and will be available for inspection by the Investigatory Powers Commissioners Office.

C 11. **Retention of Records**

C 11.1 All documents must be treated as strictly confidential and the Authorising Officer must make appropriate arrangements for their retention, security and destruction, in accordance with the Council's Data Protection Policy and the RIPA codes of practice. The retention period of the purposes of this guidance is three years from the ending of the period authorised.

C 11.2 The Council's Records Retention and Disposal Policy should be referred to which sets out how different types of records are created as part of any investigation, their storage, retrieval, maintenance, protection and final disposal. The Council also has a separate Code of Practice which covers these issues specifically for CCTV tapes.

C 12 **Complaints Procedure**

C 12.1 The Council will maintain the standards set out in this guidance and the relevant Codes of Practice. The IPC has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.

C 12.2 A contravention of the General Data Protection Regulations (GDPR) may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of the guidance should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Customer Feedback & Standards Manager, Bath and North East Somerset Council on 01225 477013 or via councilconnect@bathnes.gov.uk

POLICY ON INVESTIGATORY POWERS ACT 2016 (IPA)

PART II - IPA

D 1.0 ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

D 1.1 With effect from 5 February 2019, and in accordance with Part 3 and chapter 2 of Part 6 of the Investigatory Powers Act 2016 ("the IPA"), Local Authorities can obtain' communications data'(CD) provided that the acquisition of such CD is necessary for the applicable crime purpose ; and proportionate to what is sought to be achieved by acquiring such CD.

D 1.2 The applicable crime purpose will depend upon whether the CD being sought is classified as entity data or events data. Where the CD sought is wholly or partly events data the purpose must be for a serious crime. In any other case the CD must be for the purpose of preventing or detecting crime or of preventing disorder.

- *Serious crime"* means crime where-
- (a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 1 year or more, or
- (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose

D. 1.3 The Communications data Code of Practice can be accessed here:

https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

Important: The Council is NOT Permitted to Intercept any Communications

D 1.4 The purpose and effect of the procedure is the same as RIPA i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge.

D 1.5 Applications for CD are subject to independent examination, scrutiny and approval by the IPC through the "Investigatory Powers Commissioner's Office (IPCO). All applications for CD must be undertaken online through NAFN acting as single point of contact SPOC pursuant to the IPA.

D 2.0 What is 'Communications Data'?

D 2.1 The term Communications Data includes the "who", "where", and "how" of a communication but not the content i.e. what was said or written. CD is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services.

D 2.2 The Council may only acquire less intrusive types of CD. These are:

Entity Data – this data describes or identifies the entity. Entities can be individuals and objects (such as mobile phones).

Events Data –for CD this is limited to communications events which identifies any person, apparatus or location to or from which a communication is transmitted

e.g.:

- incoming call records,
- the location of a mobile phone,
- numbers called

D 2.3 CD relating to Events data is more intrusive than data relating to Entities

D 3.0 **Senior Responsible Officer**

D 3.1 The Monitoring Officer shall be appointed as the Council's Senior Responsible Officer and in their absence the Deputy Monitoring Officer

The SRO is responsible for

- the integrity of the process in place within the public authority to acquire communications data;
- engagement with authorising officers in the IPCO (where relevant);
- compliance with Part 3 of the Act and with the code, including responsibility for novel or contentious cases;
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to the Investigatory Powers Commissioner's Office by the public authority;
- engagement with the IPC's inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

D 4.0 **Application Forms**

D 4.1 The Council will maintain a collaboration agreement with the National Anti- Fraud Network (NAFN). All applications must be made online at https://www.nafn.gov.uk/ NAFN will act as a single point of contact (SPOC) between both the communications service providers (CSPs) and the Council concerning the request and provision of CD. This is to ensure a centralised and managed approach in making applications to obtain CD and facilitates lawful acquisition of CD and effective co-operation between the Council and CSPs.

In addition to being considered by a NAFN SPOC, the applicant for CD must ensure that the Council's SRO is aware of the application being made before it is submitted to an authorising officer in the IPCO. The Council's SRO's will be notified to NAFN.

D 5.0 **Duration**

D 5.1 Authorisations to obtain CD are only valid for one month beginning with the date on which the Investigatory Powers Commissioner's Office approval is granted.

D 6.0 **Renewal and Cancellation**

D 6.1 An authorisation may be renewed at any time during the month it is valid using the same procedure as used in the original application (including IPCO approval). A renewal takes effect on the date which the authorisation it is renewing expires.

D 6.2 The code requires that all authorisations must be cancelled by the Council and sent to the IPCO as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The Council must notify the SPOC which must cease the authorised conduct.

D 7.0 **Retention of Records**

D 7.1 Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner. Applications must also be retained to allow the Tribunal (see paragraph D 8.0 to carry out its functions.

D 7.2 A record must be kept of:

- the dates of which the authorisation or notice is started or cancelled;
- any errors that have occurred in the granting of authorisations or giving of notices.

D 7.3 A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable. Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the GDPR must be observed. The Monitoring Officer will maintain a centrally retrievable register.

D 8.0 **Oversight and Complaints**

D 8.1 The Act provides for an Investigatory Powers Commissioner whose remit is to provide independent oversight of the use of the powers contained within the IPA and the code requires any person who uses the powers conferred by the IPA to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions.

D 8.2 The IPC must inform any affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal.

SCHEDULE 1

Designated Persons/Authorising Officers

Chief Executive
Monitoring Officer
Deputy Monitoring Officer

Note: When the above are the Applicant Officer in a matter they may NOT authorise the same application for surveillance.

Senior Responsible Officers for CD

Monitoring Officer
Deputy Monitoring Officer

SPOC for CD

NAFN https://www.nafn.gov.uk/

SCHEDULE 2

VERSION CONTROL TABLE
Since 2014

RIPA POLICY VERSIONS	DATE	STATUS	Approved by Council
Version 1	14 April 2014	Superseded	
Version 2	18 May 2017	Superseded	
Version 3	31 July 2019	Superseded	
Version 4	15 September 2022	Superseded	
Version 5	01 November 2022		
Version 6	30 August 2024	superseded	

SCHEDULE 3

AUTHORISING A CHIS: PROCEDURE

The Council will only authorise a CHIS is exceptional circumstances. Section 29 of RIPA sets out the criteria for authorising a CHIS.

The Authorising Officer

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the Authorising Officer for a local authority can be a Director, Head of Service, Service Manager or equivalent.

Where the surveillance involves the likelihood of obtaining confidential information, the deployment of juveniles or vulnerable people, then authorisation has to be sought from the Head of Paid Service and in their absence, the acting Head of Paid Service.

Time Limits

The current time limits for an authorisation 12 months for a CHIS (1 month if the CHIS is underage).

A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a Magistrate.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but applicants must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application).

Authorising Officer's Consideration

S.29 (2) states:
"A person shall not grant an authorisation for the conduct or the use of a covert human intelligence source unless he believes-
(a) that the authorisation is necessary on grounds falling within subsection (3);
(b) that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use; and
(c) that arrangements exist for the source's case that satisfy the requirements of subsection (5) and such other requirements as may be imposed by order made by the Secretary of State. "

Consequently the following matters must be satisfied before authorising the deployment of a CHIS:

1. Necessity

The deployment of a CHIS has to be necessary on one of the grounds set out within in S.29 (3). Local authorities can only authorise on the following grounds; where it is necessary:

“for the purpose of preventing or detecting crime or of preventing disorder.” (S.29 (3) (b)) or

The matter being investigated must be an identifiable criminal offence, constitute disorder or be for the purpose of protecting public health.

2. Proportionality

Proportionality means ensuring that the deployment of the CHIS is the least intrusive method to obtain the required information having considered all reasonable alternatives. This requires consideration of not only whether a CHIS is appropriate but also the method to be adopted, the duration and the equipment to be used. The CHIS Code Para 3.6 provides guidance on the elements of proportionality:- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1112009/October_2022_Draft_Revised_CHIS_Code_of_Practice__print_.pdf

• balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

• explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

• considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

• evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3. Security and Welfare Arrangements

CHIS’s are often placed in difficult and sometime dangerous situations. Appropriate security and welfare arrangements must also be in place in relation to each CHIS. S.29 (5) requires there to be:

- A person who will have day-to-day responsibility for dealing with the CHIS on behalf of that authority, and for his/her security and welfare; (**CHIS Handler**)
-
- A person who will have general oversight of the use made of the CHIS. (**CHIS Controller**)This person must be different to the one above.
-
- A person who will maintain a record of the use made of the CHIS. This can be one of the above or a separate person.
-
- Proper and secure records to be kept about the use made of the CHIS.

4. Risk Assessment:

An applicant considering deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking.

Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, Court.

The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

• the validity of the risk assessment;

• the conduct of the CHIS; and

• the safety and welfare of the CHIS.

Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

SCHEDULE 4

Bath & North East Somerset Council
Social Media Policy for the
Purposes of
Regulation of Investigatory Powers Act 2000' RIPA'

Bath & North East Somerset Council recognises the benefits and opportunities that the internet and multi-media provide to access and share information using a wide range of on line facilities. This is referred to Social Networking Sites – 'SNS'.

There are however some considerations and standards to apply when using such sites and this policy establishes the Council's position regarding the use of the internet, mobile web browsing and specifically social media websites when undertaking investigations under and in accordance with RIPA.

The Council's ICT Security Policy provides the basis for this policy and associated guidance. This policy should be read in conjunction with the supporting RIPA Policy and any guidance issued by the IPC – Investigatory Powers Commissioner.

This policy covers external investigations, which could also apply to internal staff that may be subject to an investigation. Advice should be taken from HR should an investigation involve a member of staff.

Contents

1. This policy covers the use of social media, including social networking websites such as Twitter, Facebook, LinkedIn, and YouTube, content communities and blogs.

2. The policy and guidance aim to ensure that the council and its employees when undertaking investigations are protected and that a lawful and fair process is followed.

3. This policy closely relates to other council documents but in particular ICT Security policy.

4. The other legislation that may also be impacted by an investigation being carried out is as follows: Human Rights Act 1998, Freedom of Information Act 2000 and the GDPR

Conducting an investigation under the Social Media Policy.

5. The implications of enforcement through monitoring of social media and its human rights implications are difficult areas for law enforcement with complex privacy considerations:

5.1 The three main issues are:

(1) What expectation of privacy a user may reasonably have when posting on the Internet; and
(2) How covert or overt the officer looking at information on the internet is being.

(3) Whether or not a RIPA or CHIS authorisation should be obtained.

Investigatory 'Tools'

There are three main investigatory tools under RIPA that Officers may consider using in an investigation involving SNS. They are:

The use of 'Directed Surveillance, which is essentially covert surveillance carried out in places other than residential premises or private vehicles which is relevant where an investigatory technique might infringe Article 8 rights (e.g. where personal data or sensitive date is likely to be accessed or acquired and where there is an expectation of privacy) and which is subject to a 'crime threshold' when investigating criminal offences.

The use of Covert Human Intelligence Source (CHIS) which includes undercover officers (most significantly included covert profiles), informants and persons making test purchases; and

5.2 Powers to acquire or obtain 'communications data'.

5.3 The Council is seeking to focus on 3 broad categories so as to give an indication of what is and what is not acceptable for it to do. Prior to starting a browsing session an officer should consider what he/she is seeking to achieve and is likely to be doing and be aware of when their actions might cross the boundary from one "level" to another.

Three Broad Categories

6. **Category 1** – Viewing publically available postings or websites where **the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view.** E.g. a typical trader's website.

   - There must be a low expectation of privacy and **no RIPA authorisation would normally** be required to view or record these pages.

   - However, **repeated visits** over time to the extent that you might be perceived as **monitoring** a website, may require authorisation. Private information can remain private information even when posted on such a website and the European Convention on Human Rights has construed that the way a business is run can be private information. If you intend to monitor in this way therefore you may acquire private information and it is recommended that it is done in a **systematic** way with results recorded. Particularly note whether or not you happen to access private information. The fact that on previous visits a lack of private information is found could be good evidence that any subsequent acquisition was incidental and a RIPA authorisation is not required.

   - There is unlikely to be **unfairness** (S78 PACE Act) in presenting the pages viewed as evidence. Pay attention to the requirements in Appendix B of the ACPO Good Practice Guide for Digital Evidence (in Chapter 2 of the D&S enforcement manual). If a test purchase is required, you may use a fictitious name and address without triggering the need for a CHIS (or Directed Surveillance) authorisation, provided no "relationship" is formed.

- As above, the **use of a fictitious identity or "covert" account** is not necessarily the trigger for a need for a RIPA authorisation, be it Directed Surveillance, or the in the case of a test purchase, CHIS. More relevant is the likelihood of acquisition of private information, or how far a "relationship" is formed.

7. **Category 2** – Viewing postings on social networks **where the viewer has had to register a profile but there is not otherwise a restriction on access**. This would include Facebook where there is no need to be accepted as a "friend" to view. E.g.: Trader has a "shop window" on Facebook advertising a business and products.

    - There are differences between this and Category 1. The person who posts information or runs such a website may reasonably expect viewers to work within the terms and conditions of the website.
    - Viewing should therefore normally be conducted in an overt manner i.e. via an account profile which uses your correct name, and email address (which should be a B&NES.gov.uk etc. address) or an officer's Service Sanctioned profile. If this is done there can be no objection to a recording of the visit being made and presented in evidence.

    - If the posting or website contains no private information a viewing would not engage privacy issues and therefore a RIPA authorisation is not needed. However it is possible that a mixture of private and business material is displayed, and the ECHR has construed the way a business is run as being private information. The conditions regarding **repeat visits** in Level 1 are therefore relevant.

    - A "Covert" account at this level should only be used in the context of a RIPA authorisation.

8. **Category 3– Viewing postings on social networks which require a "friend" or similar status to view.**

    - These are **highly** likely to involve viewing private information.

    - Repeated viewings will constitute Surveillance and require a RIPA authorisation. This may apply whether or not a "covert" or "overt" account is used, though this is probably best obtained via a CHIS authorisation with the use of a covert profile and appropriate risk assessments.

    - An "Overt" account which gains "friend" or similar status may **still require a RIPA authorisation.** It may be that such a status may be given by a default on the part of the person posting or website owner. The officer should be especially sure that their access is being granted as a representative of the Service. For example, on Facebook it is stated that only people who know the person who maintains a profile should send a "friend" request to that profile. A person accepting that friend request may believe the person requesting is an acquaintance that they simply do not recall or know by another name. They still have a justifiable expectation of privacy. While requesting access may not comply with a strict interpretation of Facebook terms and conditions, a clearly identifiable **Officer's Service Sanctioned profile** is a way to deal with that expectation of privacy, rather than a more neutral officer based profile.

- A “Covert” account at this level should only be used in the context of a RIPA authorisation.

Covert Facebook Accounts:

9. The use of covert Facebook accounts to access postings need to be covered by a RIPA authorisation. Currently there does not seem to be a mechanism for a Service to operate these on Facebook within the company’s terms and conditions. Any evidence obtained via them can run a risk of being considered “unfair”. It is quite likely that the profiles used will become “blown” at some stage and users need to monitor them to ensure this is identified early. Considerable officer time is required to maintain a covert identity.

10. Obtaining a RIPA authorisation will also present an officer with a defence should there be an allegation that they have breached the Computer Misuse Act 1990 – it is an offence to deliberately access unauthorised material.

Covert surveillance of Social Networking Sites (SNS)

11. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

12. Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). **Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.**

13. Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site’s content).

14. **It is not unlawful for a member of a public authority to set up a false identity but it is not advisable for a member of a public authority to do so for a covert purpose without authorisation.** Using photographs of other persons without their permission to support the false identity infringes other laws.

15. A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is being used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what

is and is not to be done).

Recording Information

16. All information should be recorded on the appropriate form(s) should an authorisation be required.

Training

17. Training should be made available to Officers undertaking any covert or directed surveillance when undertaking investigations.

Related Documents

18. Documents that should be referred to are:
    - RIPA Policy
    - Investigatory Powers Commissioners Codes
    - Council Code of Conduct
    - Council Email and Internet Policies