BCP Council Regulation of Investigatory Powers Act (RIPA) Policy

April 2021

Policy Owner: Susan Zeiss
Author/s: Law & Governance and Policy and Performance
Version: 1.1
Review Date: March 2023

1. Purpose Statement

1.1 This policy ensures compliance with the regulatory framework for the use of covert surveillance techniques by BCP Council as set out in the Regulation of Investigatory Powers Act 2000 (RIPA) and RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (and as amended 2012).

This policy does not cover access to, or the acquisition of, Communications Data covered by the Investigatory Powers Act (IPA) 2016 which came into force on 11 June 2019. See 6.2.

1.2 Surveillance plays a necessary part in modern life. Most of the surveillance carried out by or on behalf of BCP Council will be overt. That is, there will be nothing secretive, clandestine or hidden about it. Overt surveillance is not covered by RIPA.

1.3 Covert surveillance 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. If certain activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

1.4 BCP Council will only use covert surveillance where it is proportionate to do so and where overt measures have been exhausted or are not possible. Covert surveillance will not be undertaken unless absolutely necessary.

2. Who the policy applies to

2.1 Those officers who may conduct or authorise covert surveillance investigations.

2.2 In most cases investigations carried out by council officers will not be subject to RIPA, as they involve overt rather than covert surveillance.

3. This policy replaces

3.1 This policy replaces the legacy policies, procedures and guidance of the three preceding authorities that now make up BCP council.

4. Approval process

4.1 This policy will be approved by the Audit and Governance Committee.

5. Links to Council Strategies

5.1 This policy has been prepared based on Government legislation and requirements laid out under the Regulation of Investigatory Powers Act 2000 (and as amended) and taking into account accompanying guidance and codes of practice.

5.2 This policy links to the following BCP Council policies and strategies:

- Information Security Policy
- Information Governance Policy
- Equality & Diversity Policy
- Safeguarding Strategy

6. The Policy

6.1 In some circumstances, it may be necessary for BCP Council employees or contractors, in the course of their duties, to make observations of a person or person(s) in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy, and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 (`the right to respect for private and family life`).

6.2 RIPA limits local authorities to using three types of covert surveillance techniques, as set out below (see Appendix A for definitions):

- **Directed surveillance**
- **Covert Human Intelligence Source (CHIS)**
- **Access to Communications Data (CD)**

IPA 2016, which commenced on 11 June 2019, is now the main legislation governing the access to or acquisition of Communications data, it does not fully replace all pre-existing RIPA requirements but does introduce some important and significant variations to authorisation and regulatory oversight in particular.

BCP Council is in the process of producing a separate IPA Policy.

6.3 Employees and contractors (where applicable) of BCP Council cannot, according to law, carry out **intrusive surveillance** (see Appendix A for definition) within the meaning of the Regulation of Investigatory Powers Act 2000 nor will they interfere with property or wireless telegraphy.

6.4 BCP Council employees and contractors (where applicable) will adhere to the authorisation procedure (see Appendix B) before conducting any covert surveillance.

6.5 Officers of BCP Council may only seek authorisation to engage in directed surveillance or CHIS surveillance where it meets the statutory tests that it is necessary for the "prevention or detection of crime or disorder" and where it has been demonstrated to be necessary and proportionate in what it seeks to achieve. If in any doubt advice from the RIPA Senior Responsible Officer (SRO) or the RIPA Administrator must be sought (see roles and responsibilities section).

6.6 The Revised Code of Practice which came into effect in August 2018 (further revision imminent) requires the highest levels of authorisation where 'confidential information' is likely to be acquired and at BCP Council this is the Head of Paid Service in consultation with the RIPA SRO. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material, or where information identifies a journalist's source.

6.7 BCP Council will ensure the code of practice is complied with through appropriate training given to officers and annual Audit and Governance oversight of RIPA usage.

6.8 BCP Council is subject to audit and inspection by the Investigatory Powers Commissioner's Office (IPCO) and it is important that compliance with RIPA and accompanying guidance can be demonstrated in every case. BCP Council will hold a central record of RIPA authorisations in line with section 8 of the Code Practice.

6.9 Types of surveillance that can and cannot be carried out by Local Authorities and further information is set out in Appendix A.

7. Authorisation of RIPA application to a Magistrates Court

7.1 Statutory Instrument 2010 No. 521 restricts Authorising Officers in local authorities to be Directors, Heads of Service or Service mangers or equivalent. In BCP Council only certain officers, within these categories of mangers, are designated as Authorising Officers (See section 9).

7.2 All other reasonable and less intrusive options to gain the required information must be considered before an authorisation is applied for and the RIPA application must detail why these options have failed or have been considered not appropriate in the circumstances of the individual investigation.

7.3 The Protection of Freedoms Act 2012 requires that Local Authorities seeking RIPA authorisation are subject to judicial approval in the local Magistrates' Court. If the Authorising Officer authorises an application under RIPA, the application must be presented to a Magistrate for final approval. Authorisation will not take effect until a Magistrate has made an order approving the grant of the authorisation. It is vital that any surveillance for which authorisation has been sought does not start until such a time as it has been approved by a Magistrate.

7.4 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

7.5 When considering an application, the Authorising Officer must:

- Have regard to the contents of this document, the training provided and any other guidance or advice given by the RIPA SRO;
- Satisfy themselves that the RIPA authorisation will be:
    - In accordance with the law
    - Necessary in the circumstances of the particular case; and
    - Proportionate to what it seeks to achieve;
- Assess whether or not the proposed surveillance is proportionate considering the following elements:
    - The custodial sentence applicable to the offence being investigated
    - 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
    - Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result
    - Evidencing, as far as reasonably practicable, what other methods had been considered and why were not implemented;
- Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called 'collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);
- Consider any issues which may arise in relation to the health and safety of council employees and agents and ensure that a risk assessment has been undertaken;
- Ensure that the equality impact of any proposed surveillance is considered through the completion of an Equality Impact Assessment (EIA).

7.6 When authorising the conduct or use of a CHIS, the Authorising Officer must also:

- Be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
- Be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
- Consider the likely degree of intrusion for all those potentially affected;
- Consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained;
- Ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

7.7 If an application is granted, the Authorising Officer must set a date for its review and ensure that it is reviewed on that date. Records must be kept in relation to all RIPA applications and authorisations and, to facilitate this, each investigation or operation should be given a unique reference number (URN) by the RIPA Administrator. Any subsequent forms relating to the same investigation or operation should be identified by the means of the same URN.

7.8 Authorisations will have effect until the date for expiry specified on the relevant form. They will only be granted for the designated period of three months for directed surveillance and twelve months for the use or conduct of a CHIS. No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed. It will be responsibility of the officer in charge of an investigation to ensure that any directed surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, they must be mindful of the date when authorisations and renewals will cease to have effect. The RIPA Administrator will perform an auditing role in this respect but the primary responsibility rest with the officer in charge of the surveillance investigation.

7.9 Authorisations will be reviewed at appropriate intervals to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Reviews should take place on a monthly basis unless the Authorising Officer considers they should take place more regularly. The results of the review should be recorded and retained.

7.10 Authorisations must be 'cancelled' as soon as they become unnecessary. Authorisations should not be allowed to lapse and must be formally cancelled or renewed, whichever is required, before the expiry date. The responsibility for ensuring that authorisations are cancelled rests primarily with the officer in charge of the surveillance investigation who should submit a request for cancellation to the RIPA Administrator.

7.11 If it is required, a renewal must be authorised (by a Magistrate) prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original authorisation period is due to expire. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. Renewals may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be 'cancelled' and new authorisation sought. Any renewal should seek to begin on the day when the original authorisation would otherwise have expired.

7.12 Following the completion of any case involving the use of RIPA a written assessment review should be undertaken by the Authorising Officer in charge of the surveillance. This written assessment should detail the information obtained and how it was used to take the case forward. The written assessment must be passed to the RIPA Administrator and stored with any other URN records for that case be provided as part of any inspection by the IPCO.

7.13 Records must be maintained for a period of at least three years from the cancellation of the authorisation. Following which they shall be securely destroyed in accordance with the guidance from the council's Information Governance team on document retention.

8. How to use this policy and useful documents

8.1 Appendix A: Surveillance that can and cannot be carried out by LA's
8.2 Appendix B: RIPA Authorisation Process
8.3 Appendix C: Does RIPA apply? Directed Surveillance Flowchart
8.4 Appendix D: Covert Human Intelligence Source Flowchart
8.5 Appendix E: Accessing Communications Data Flowchart (interim until specific policy or addendum is in place)
8.6 Appendix F: Equality Impact Assessment for this policy
8.7 Equality Impact Assessment templates (on the BCP Council intranet)
8.8 Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance
8.9 Home Office RIPA Forms

9. Roles and responsibilities

Role	Responsibilities
Senior Responsible Officer (SRO) Director of Law & Governance (and Monitoring Officer) Deputy SRO will be Chief Executive	• The integrity of the process in place within the council for the directed surveillance, management of CHIS and acquisition of communications data • Overall responsibility for the management and oversight of requests and authorisations under RIPA • Ensuring that all authorising officers are trained to an appropriate standard • Ensures compliance with Part 2 of the Act and with the Home Office Codes of Practice • Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors • Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their audits or inspections, where applicable • Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner
Authorising Officer Regulatory Services Manager	• The only officers in BCP Council who can authorise applications (and renewals) under RIPA for onward consideration by a Magistrate • Must 'cancel' authorisations where the case has concluded and undertake reviews in relation to any investigation carried out • Must not delegate their powers in relation to RIPA to any other officers

Director of Communities Chief Executive and Corporate Directors	**Note:** The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, (in the case of illness or has left the Council in the interim only) this can be undertaken by another Authorising Officer. In exceptional circumstances it may be necessary for the Chief Executive or a Corporate Director to act as an Authorising Officer
RIPA Administrator Head of Audit and Management Assurance Deputy RIPA Administrator will be Audit Manager (Deputy Chief Internal Auditor)	• Issue a unique reference number to each authorisation requested under RIPA – reference numbers will be sequential and start at BCP01. • Retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer • Maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice • Review and monitor all forms and documents received to ensure compliance with the relevant law and guidance in consultation with the RIPA Senior Responsible Officer and inform the Authorising Officer of any concerns • Chase failures to submit documents and/or carry out reviews/cancellations
All Staff	• Must not engage in covert surveillance of any type unless authorised to do so, formally by a designated Authorising Officer
Audit and Governance Committee	• Monitor the Council's usage of its powers under RIPA on an annual basis

10. Enforcement and sanctions

10.1 Compliance with the provisions of RIPA, the Home Office Codes of Practice and this policy and procedures should protect the council, its officers and agencies working on its behalf against legal challenge. Section 27 of RIPA states that "conduct… shall be lawful for all purposes if an authorisation…confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation". If correct procedures are not followed, the council could be rendered liable to claims, complaints and significant costs and the use of the information obtained may be disallowed in any subsequent legal proceedings.

10.2 The Investigatory Powers Commissioner's Office (IPCO) conducts audits and inspections of the use of investigatory powers to ensure that public bodies that are authorised to use investigatory powers are doing so lawfully and in line with best practice. They produce thorough and impartial reports which support and inform the work of the IPC and the Judicial Commissioners. The IPCO also carries out ad-hoc investigations into potential non-compliance.

10.3 Any failure to follow this policy will be considered gross misconduct and investigated accordingly.

11. Further information and evidence

11.1 The Home Office has Codes of practice and guidance for making an application under the Regulation of Investigatory Powers Act (2000).

11.2 Individuals who feel that the Local Authority has applied the principles of this policy incorrectly can appeal to the IPCO.

12. Glossary

12.1 The following terms are useful to know in regards to RIPA:

- RIPA - Regulation of Investigatory Powers Act 2000
- CHIS - Covert Human Intelligence Source
- SPoC - Single Point of Contact
- SRO - Senior Responsible Officer
- IPCO - Investigatory Powers Commissioner's Office
- NAFN - National Anti-Fraud Network
- CSP- Communications Service Provider

APPENDIX A –Surveillance that can and cannot be carried out by LA's

Intrusive Surveillance
Intrusive surveillance is a specific form of covert surveillance which local authorities cannot, according to law, carry out within the meaning of the RIPA nor will they interfere with property or wireless telegraphy. The ability to undertake intrusive surveillance is limited to the Police and Security Services who, in certain circumstances and within RIPA requirements, must obtain a High Court order to authorise.
Intrusive surveillance is any form of covert surveillance taking place in any residential premise or any private vehicle.

Directed Surveillance
Directed surveillance is a specific form of covert surveillance and may only be authorised under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.

As the description implies the form of surveillance is 'directed' at a specific individual or business.

Authorised directed surveillance would be needed for example, when using mobile, hidden recording devices or cameras to record what is going on in a shop selling alcohol and tobacco.

Covert Human Intelligence Source (CHIS)
A CHIS is a specific form of covert surveillance and is defined as the use of an individual to create a relationship with a subject, for the purposes of obtaining information, where the purpose of the relationship is not disclosed to the subject. Interaction with the subject of surveillance is therefore required in order for an individual to be regarded as a covert human intelligence source (CHIS).

For example, CHIS would be required for developing a relationship with a person in a shop, to obtain information about the seller's suppliers of an illegal product e.g. illegally imported products.

The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example;

- Where members of the public volunteer information to the council as part of their normal civic duties;
- Where members of the public volunteer to make test purchases on behalf of the Council;
- Where the public contact telephone numbers set up by the council to receive information;
- Where members of the public are asked to keep diaries of incidents in relation to, for example, planning enforcement, anti-social behaviour or noise nuisance. However, in certain circumstances, RIPA authorisation may be required if the criteria in section 26(2) of the Act are met.

Activity not falling within the definition of covert surveillance requiring authorisation
Some covert surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance authorisation is required to be obtained for such activity. Such activity includes:

- Covert surveillance by way of an immediate response to events;

- Covert surveillance as part of general observation activities;
- Covert surveillance not relating to the statutory grounds specified in the 2000 Act;
- Overt use of CCTV and ANPR systems;
- Covert surveillance authorised as part of an equipment interference warrant under the 2016 Act;
- Certain other specific situations of covert surveillance that is not directed surveillance or Covert Human Intelligence Source (CHIS) – such as covert recording of noise where the recording is of decibels only or non-verbal noise (such as machinery, music or an alarm).

Communication Data
Acquisition of Communications data is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written)

Under IPA 2016 a local authority can only obtain authorisation for less intrusive types of communications data acquisition, called Entity Data, to investigate 'applicable crime'. Under no circumstances can local authorities be authorised to obtain traffic data under IPA.

Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

For access to communication data, a Single Point of Contact (SPoC) is required to undertake the practical facilitation with the communications service provider (CSP) in order to obtain the data requested. The SPoC must have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the local authority and CSP. The SPoC does not need to be an officer of the authority, the National Anti-Fraud Network provides a SPoC service to local authorities.

BCP Council is in the process of producing a separate IPA Policy, which will cover communication data acquisition.

Social Networking Sites
The Internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of the local authority is intending to engage with others online without disclosing their identity a CHIS authorisation may be needed.

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where reasonable steps are taken to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not be required.

Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as an investigation. This is regardless of whether the individual has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy.

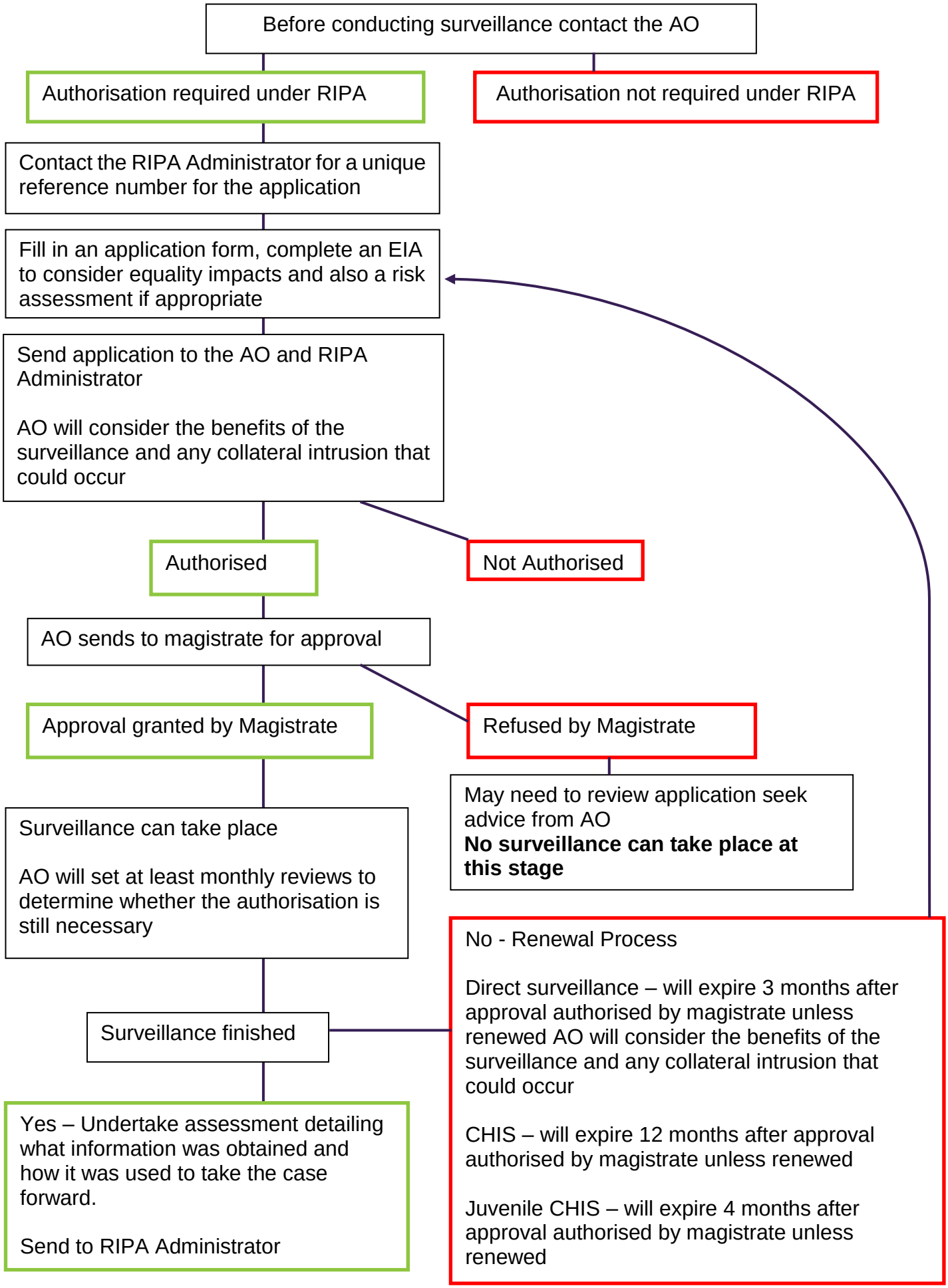
Simple reconnaissance of such sites is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where information is systematically collected or recorded about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

CCTV

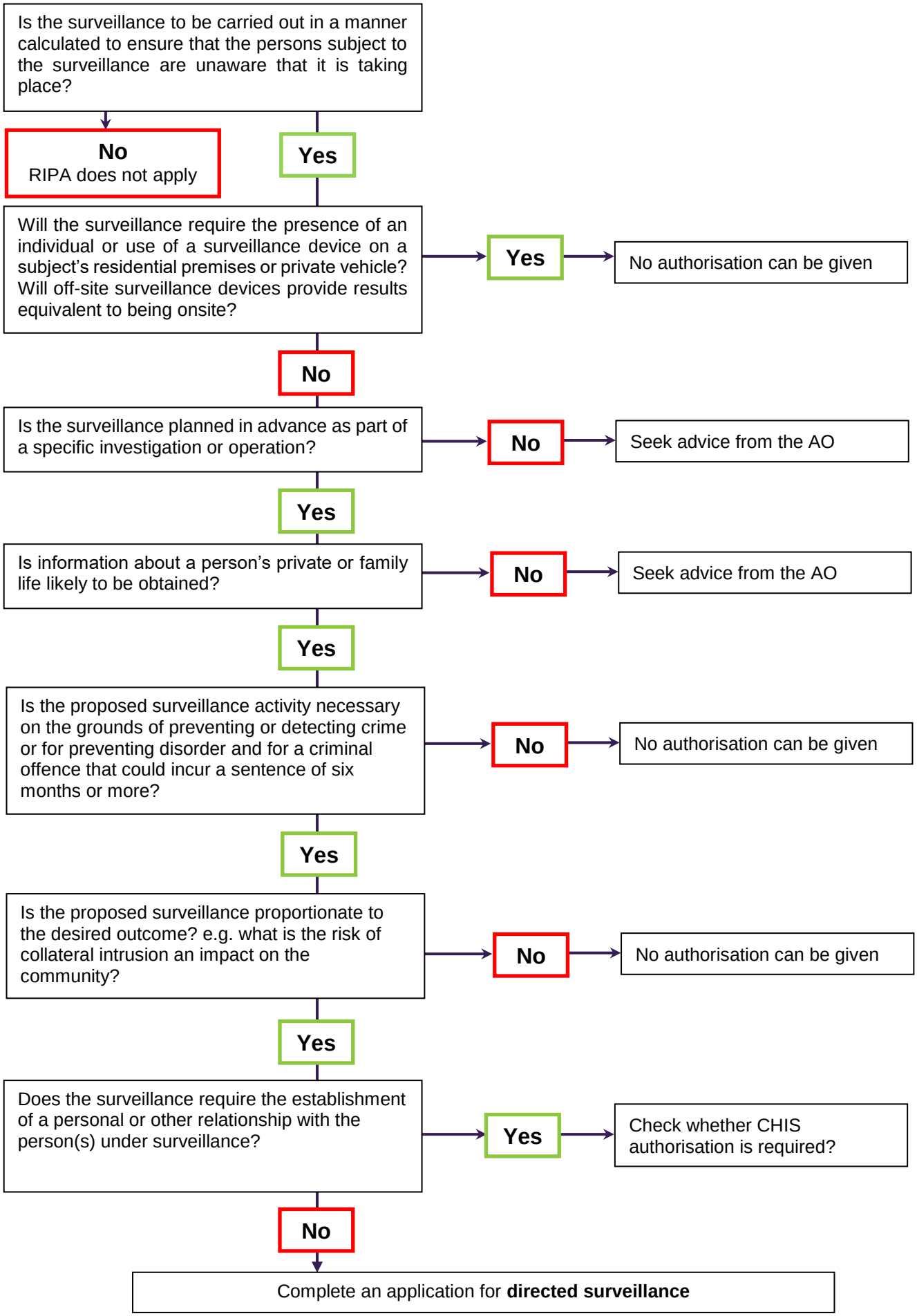
If CCTV is accompanied by clear signage then the monitoring will be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation then RIPA authorisation is likely to be required.

If a law enforcement agency wishes to use BCP Council CCTV for directed surveillance then they must provide the authorisation (redacted if necessary) and only utilise the CCTV equipment in accordance with that authorisation.

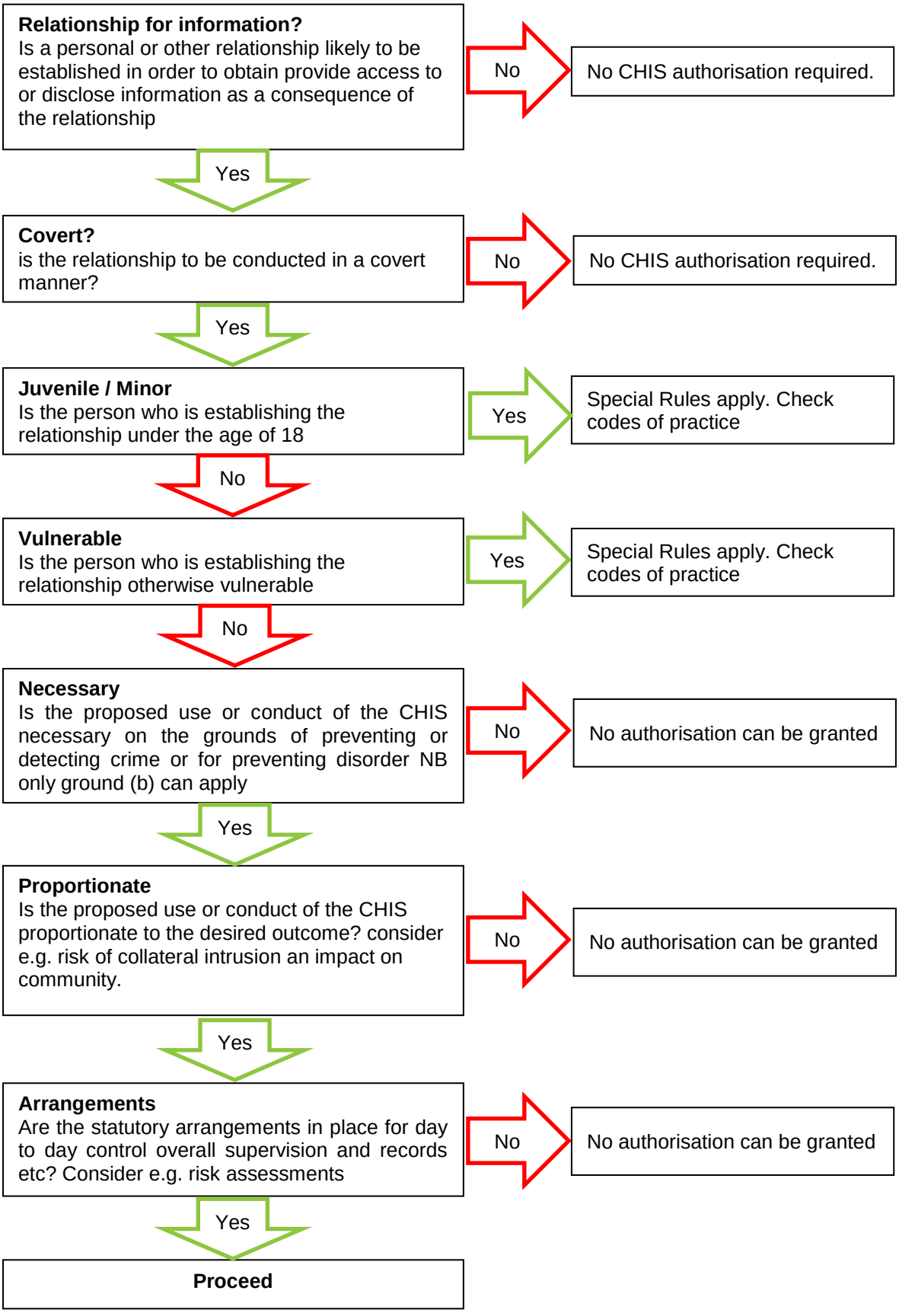
APPENDIX B - RIPA Authorisation Process



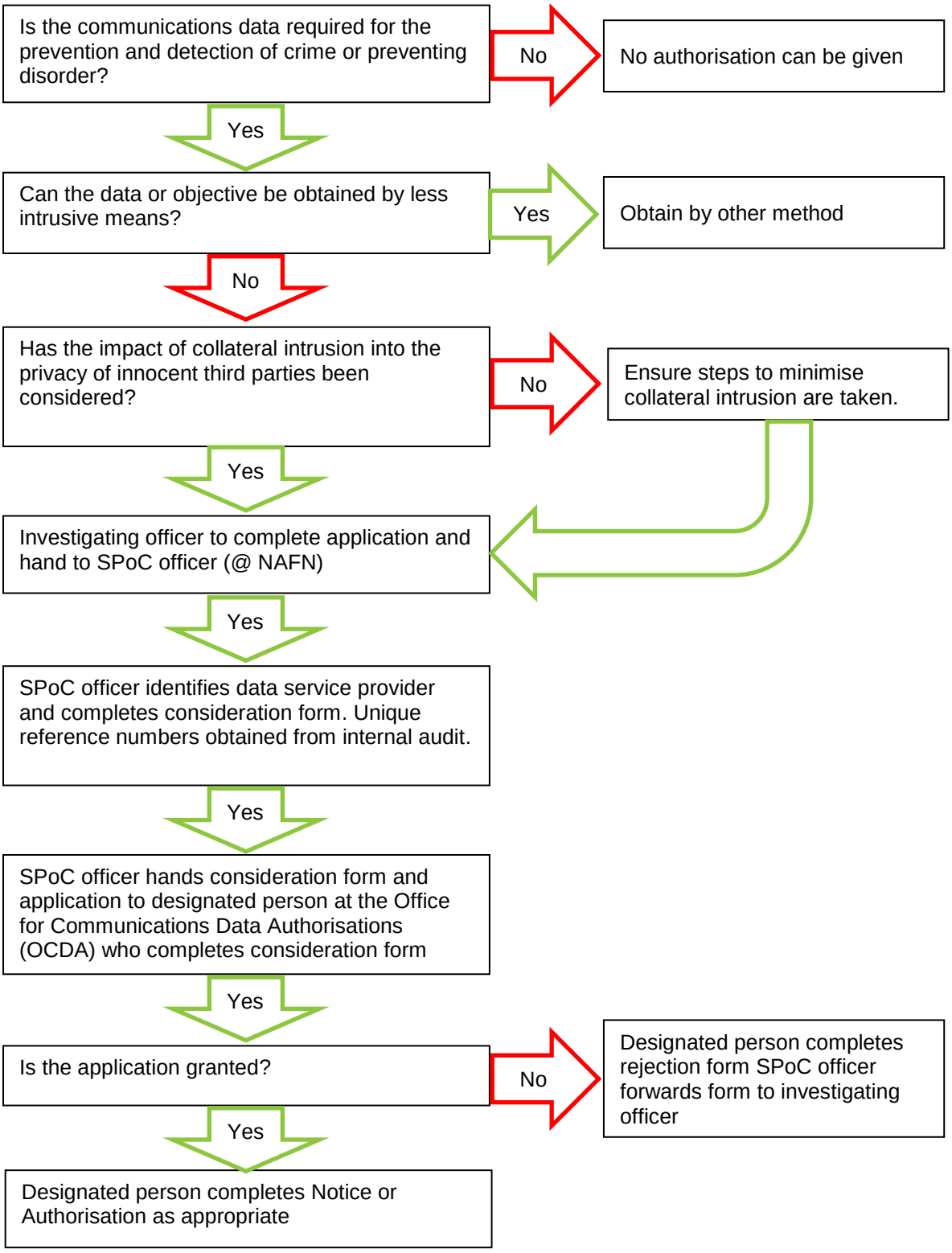
APPENDIX C – Does RIPA apply? Directed Surveillance Flowchart



APPENDIX D - Covert Human Intelligence Source Flowchart



APPENDIX E - Accessing Communications Data Flowchart (Interim until specific policy or addendum is in place)



Note: If at any time during the process, the data is no longer required for any reason. The SPoC officer should be informed and the Designated Person will complete the relevant cancellation notice which is forwarded to the Data service Provider

APPENDIX F

Equality Impact Assessment: conversation screening tool

Policy/Service under development/review:	BCP Council and the Regulation of Investigatory Powers Act 2000
What changes are being made to the policy/service?	New policy being adopted
Service Unit:	Law and Governance
Persons present in the conversation and their role/experience in the service:	Graeme Smith, Policy and Performance Officer Sophie Bradfield, Policy and Performance Officer
Conversation dates:	5/3/21
Do you know your current or potential client base? Who are the key stakeholders?	The client base is anyone the authority may choose to conduct covert surveillance about. This could, therefore, apply to any resident or staff member of BCP. BCP council has not conducted covert surveillance under RIPA since its creation, and the predecessor authorities had not for a number of years prior to that.
Do different groups have different needs or experiences in relation to the policy/service?	BCP Council's aim is that no resident or staff member should have a different experience of the policy because of any protected characteristic. The policy requires an equality impact assessment to be carried out prior to application so a detailed assessment can be made based on the circumstances to ensure any equality implications are taken into consideration.
Will the policy or service change affect any of these service users?	The policy will ensure that there is a rigorous procedure in place for dealing with requests to conduct covert surveillance and ensure uniformity of process.
[If the answer to any of the questions above is 'don't know' then you need to gather more evidence and do a full EIA. The best way to do this is to use the Capturing Evidence form]	
What are the benefits or positive impacts of the policy/service change on current or potential service users?	Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals, but also as a means of protecting the public from harm and preventing crime. The policy implements legal requirements approved by Parliament and is designed to safeguard the human rights of individuals. The policy operates in a neutral way in respect of individuals. To ensure this, the policy asks to applicants to consider the equality impacts of covert surveillance for each individual application.
What are the negative impacts of the policy/service change on current or potential service users?	None
Will the policy or service change affect employees?	Yes, it impacts staff as it sets out the legal parameters within which staff may employ covert surveillance techniques and also how the authority may legally use covert surveillance to monitor staff.
Will the policy or service change affect the wider community?	Yes, the policy will confirm a lawful approach to establishing covert surveillance for the whole community.

What mitigating actions are planned or already in place for those negatively affected by the policy/service change?	None required at this stage
Summary of Equality Implications:	The policy notes that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary. In the few circumstances where the council may use this policy it ensures that any covert surveillance is conducted within the parameters set out by Parliament and, therefore, protects human rights. This policy ensures that an equitable approach is taken towards individuals and requires that assessments are made of the equality impact when authorisations are requested.