BURNLEY BOROUGH COUNCIL

CORPORATE POLICY

FOR THE USE OF

COVERT SURVEILLANCE

AND

COVERT HUMAN INTELLIGENCE SOURCES

TO COMPLY WITH THE PROVISIONS OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

REVISED February 2021

CONTENTS

1.0 INTRODUCTION

1.1 This Corporate Policy is intended for use by persons involved in the use of covert surveillance or a covert human intelligence source under the Regulation of Investigatory Powers Act 2000 ("the Act"). Part II of the Act deals with surveillance and covert human intelligence sources ("CHIS"). In addition, in 2018 the Secretary of State issued revised Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources ("the Codes of Practice") pursuant to Section 71 of the Act. The Council should have regard to the Codes of Practice when exercising its powers under Part II of the Act. This Corporate Policy is based on the Codes of Practice.

1.2 Conduct to which Part II of the Act applies is lawful for all purposes if it is conduct which is authorised under the Act and the conduct is in accordance with or pursuant to the authorisation. In addition, any officer will not be subject to any civil liability in respect of any conduct of his which is incidental to any lawful conduct. It is therefore important that any officer seeking to use powers under Part II of the Act has regard to the Codes of Practice and the contents of this Corporate Policy.

1.3 This Corporate Policy, along with the Codes of Practice published by the Secretary of State, must be readily available at Burnley Borough Council for consultation and reference. Copies of this Corporate Policy can be obtained from the Head of Legal and Democratic Services, Town Hall, Manchester Road, Burnley BB11 9SA. It is also available on the Council's intranet.

2.0 DEFINITIONS

The following definitions are used in this Corporate Policy.

2.1. Directed Surveillance

2.1.1 Part II of the Act relates to directed surveillance. Surveillance is directed surveillance if all the following are true:-

(a) It is covert but not intrusive surveillance.

(b) It is conducted for the purposes of a specific investigation or operation.

(c) It is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

(d) It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought.

2.2.0 **Covert Surveillance**

2.2.1 Surveillance is covert only if it is carried out in a manner that is calculated to ensure that persons who are subject to it are unaware that it is or may be taking place.

2.3.0 **Intrusive Surveillance**

2.3.1 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device. A surveillance device is any apparatus designed or adapted for use in surveillance. Whether something is intrusive surveillance depends on the location of the surveillance and not to any consideration of the nature of the information that is expected to be obtained. **Local authorities are not permitted to undertake intrusive surveillance.**

2.4.0 **Private Information**

2.4.1 Private information is any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. It includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. It also includes information about any person, not just the subject of an investigation. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy, even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Private information may include personal data such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

2.5.0 **Collateral Intrusion**

2.5.1 Collateral intrusion is where there is any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation for which surveillance authorisation is being sought. It is important that consideration is given to collateral intrusion when seeking an authorisation and appropriate measures should be taken to minimise the likelihood of collateral intrusion.

2.6.0 **Confidential Information**

2.6.1 Confidential information is defined in the Codes of Practice and consists of the following categories:

- communications subject to legal privilege;
- communications between a Member of Parliament and another person on constituency matters;

- confidential personal information;
- confidential journalistic material.

Further advice on confidential information is contained at paragraph 4.5.

2.7.0 **Residential Premises**

2.7.1 Residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. However, common areas (such as a communal area in a block of flats) to which a person has access in connection with their use or occupation of the accommodation are specifically excluded from the definition of residential premises. "Premises" includes any place whatsoever, including any vehicle or movable structure whether or not occupied as land.

2.8.0 **Covert Human Intelligence Source (CHIS)**

2.8.1 A person is a CHIS if

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2.8.2 A relationship is established or maintained for a covert purpose only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. A relationship is used covertly and information obtained is disclosed covertly only if the relationship is used or the information is 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.

2.9.0 **Authorising Officer**

2.9.1 An authorising officer is a person within the Council who is entitled to grant authorisations under the Act. An authorising officer must be a person who is a Director, Head of Service, Service Manager or equivalent. In addition to the Council's Chief Executive, the following are Authorising Officers for the Council:

Chief Operating Officer
Head of Legal & Democratic Services
Head of Finance & Property
Head of Housing & Development Control
Head of Streetscene

2.10.0 **Senior Responsible Officer**

2.10.1 The Senior Responsible Officer is responsible for the integrity of the Council's procedures to authorise directed surveillance or the use of a CHIS. She is also responsible for ensuring compliance with the Act and the Codes of Practice and engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner. The Council's Senior Responsible Officer is the Head of Legal & Democratic Services.

2.11.0 **RIPA Monitoring Officer**

2.11.1 This is an internal role performed by the Principal Legal Officer(Litigation & Regulation). This role involves maintaining policies and procedures, providing training and keeping a central record of all applications and liaising with the Office of the Surveillance Commissioner. From November 2012 the RIPA Monitoring Officer is also responsible for making application for approval of authorisations to a Justice of the Peace.

2.12.0 **Investigatory Powers Commissioner's Office (IPCO)**

2.12.1 The IPCO is the statutory body responsible for inspection and regulation of the public authorities which make use of the powers under Part II of the Act. The Council is inspected by the IPCOon a regular basis and is required to provide annual statistics to the IPCOof the Council's use of the powers under the Act.

3.0 **HUMAN RIGHTS CONSIDERATIONS**

3.1 Under Article 8 of the European Convention on Human Rights contained in Schedule 1 of the Human Rights Act 1998, the Council must respect an individual's right to respect for his private and family life, his home and his correspondence. However, this right is not absolute, and is qualified thus: -

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

3.2 Any such interference must be lawful, necessary and appropriate. The Act is one of the means by which such interference can be undertaken lawfully.

3.3 Covert surveillance or the use of a CHIS can be only be undertaken if it is necessary for one of the purposes set out in the Act. In relation to local authorities the only purpose for which covert surveillance or the use of a CHIS can be undertaken is for the purpose of preventing or detecting crime or of preventing disorder.

3.4 The officer authorising the covert surveillance or use of a CHIS must believe that the authorisation is necessary and that the conduct is proportionate to what is sought to be achieved by undertaking the authorised activity.

3.5.0 **Necessity**

3.5.1 The covert surveillance/use of a CHIS must be necessary for the purpose of preventing or detecting crime or preventing disorder. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any criminal proceedings and the apprehension of the person or persons by whom any crime was committed.

3.6.0 **Proportionality**

3.6.1 The authorising officer must believe that the conduct required by the authorisation is proportionate to what is sought to be achieved by undertaking the surveillance or use of a CHIS. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by the Council in the public interest. Covert surveillance/use of a CHIS should be the most appropriate method of advancing the investigation. Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. Efforts should be made to minimise the amount of collateral intrusion (see paragraph 4.3.7 – 4.3.9 and the Codes of Practice for further details). The applicant should draw attention to any circumstances that give rise to a meaningful degree of collateral intrusion.

3.7 An interference with the right to respect of individual privacy may not be justified because the adverse impact on the privacy of an individual or group of individuals is too severe. Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation or is in any way arbitrary will not be proportionate and should therefore be refused.

4.0 THE AUTHORISATION PROCESS

In response to a recommendation from the IPCO the Council has amended its authorisation process to cover situations where strictly speaking the RIPA framework does not apply, the Non – RIPA situation. Certain types of surveillance do not technically fall within the RIPA regime because they are not 'strictly' covert under the definition. One example is where premises have been forewarned that there will be a test purchase. Other cases that fall outside RIPA are those where the surveillance is covert under the definition but the surveillance is not done for the purposes of a criminal investigation. In those circumstances officers are advised to follow the Non-RIPA process referred to below to ensure that it is lawful, necessary and proportionate. This is to enable the Council to avoid a breach of Article 8 of the Human Rights Act 1998 - the right to respect for one's private and family life. Examples include employee monitoring or surveillance in connection with civil court claims. If employee monitoring is to take place Officers should follow the guidance in the Council's Investigations – Code of Practice document as well as the Employment Practices Data Protected Code issued by the Information Commissioner.

4.1 **Authorisation**

4.1.1 An authorisation must be given by an authorising officer in writing.

4.1.2 Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable.

4.2.0 **Completion of Application Form**

4.2.1 For a RIPA authorisation the applicant should complete an application form available on the Council's intranet under Regulation of Investigatory Powers Act - Documents - All Documents (sharepoint.com) either in writing or electronically, setting out for consideration of the authorising officer the necessity and proportionality of a specific application. The application completed by the applicant must also include:

- the reasons why the authorisation is necessary in the particular case for the purpose of preventing or detecting crime or of preventing disorder;
- the nature of the surveillance;
- the identities (where known) of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where appropriate;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authority required for the surveillance; and
- a subsequent record of whether the authorisation was given or refused, by whom and the time and date this happened.

A copy of the Non- RIPA authorisation is available under the Regulation of Investigatory Powers Act - Documents - All Documents (sharepoint.com)

4.3 **Necessity, Proportionality and Collateral Intrusion Considerations**

4.3.1 Applicants must consider the issues of necessity, proportionality and collateral intrusion on the application form.

4.3.2 Necessity should be a short explanation of the crime or disorder which is the subject of the proposed surveillance and why it is necessary to use the covert techniques requested. **From 1st November 2012, an authorisation can only be granted on the grounds of crime prevention or detection or prevention of disorder where the crime under investigation is one that carries a maximum term of imprisonment of at least 6 months (whether at Magistrates' Court or Crown Court) or is an offence under:**

(a) Section 146 of the Licensing Act 2003 (sale of alcohol to children);
(b) Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
(c) Section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or
(d) Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under 18)

4.3.3 Although the applicant should provide facts and evidence in order to assist the authorising officer's assessment, it is not the role of the applicant to assert that it is necessary; that is the statutory responsibility of the authorising officer.

4.3.4 In the proportionality section of the application form, applicants should outline what they expect to achieve from the surveillance and explain how the level of intrusion is justified when taking into consideration the benefit the information will give to the investigation. The applicant must believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not of itself render intrusive actions proportionate. It will not be appropriate to use covert techniques for minor offences such as dog fouling. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.3.5 The following elements of proportionality should therefore be considered:

- 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 have been considered and why they were not implemented.

4.3.6. Although the applicant should provide facts and evidence in order to assist the authorising officer's assessment, it is not the role of the applicant to assert that it is proportionate; that is the statutory responsibility of the authorising officer.

4.3.7 Collateral intrusion should also be addressed. Measures should be taken wherever practicable to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subject of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised provided the intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

4.3.8 In order to give proper consideration to collateral intrusion, and to comply with *R v Sutherland*, the authorising officer must fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed. An application which does not assist the authorising officer in this respect should be returned for clarification.

4.3.9 Some specialist equipment extracts automatically more data than can be justified as necessary or proportionate and may give rise to collateral intrusion. The inability of technology to restrict capability should not dictate the terms of an authorisation. If data is obtained that exceeds the parameters of an authorisation, the authorising officer should immediately review it and make arrangements for its disposal.

4.3.10 Notes to assist applicants and authorising officers in completing forms are contained at Appendices 1 and 2. Further guidance on the completion of application forms and necessity and proportionality considerations is contained in the Codes of Practice.

4.3.11 The application of the legal principles of covert surveillance to particular facts is, ultimately, a matter of judgment: the extent to which judgment can be prescribed is limited; there is not a one-size-fits all catalogue of principles.

4.3.12 The authorisation should clearly demonstrate how an authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve. An authorisation should, in particular, make clear that the following elements of proportionality have been fully considered:

(a) balancing the size and scope of the operation against the gravity and extent of the perceived mischief;

(b) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

(c) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and

(d) providing evidence of other methods considered and why they were not implemented.

4.4 Demonstrating Satisfaction with the Intelligence on which an application is made

4.4.1 To assist an authorising to reach a proper judgment, the provenance of the data, information or intelligence on which the application has been made should be clear. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the internet or social networks.

4.5 Confidential Information

4.5.1 The Codes of Practice require particular care to be taken in cases where the subject of the investigation or operation is likely to result in the obtaining of confidential information. Any application where confidential information is likely to be obtained can only be authorised by the Chief Executive. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner

or Inspector during his next inspection. The following categories of information are regarded as confidential information.

4.5.2 **Matters Subject to Legal Privilege**

This means information such as confidential written/oral communications between a professional legal adviser and his client or any person representing his client in connection with the giving of legal advice to the client and in connection with or contemplation of and for the purpose of legal proceedings. "Professional legal advisor" would not normally apply to a Trade Union representative but would normally apply to a Barrister, Solicitor, Legal Executive or Solicitor's Clerk. An application for surveillance likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Further guidance on authorisations in respect of legally privileged information is contained in the Codes of Practice.

4.5.3 **Communications between a Member of Parliament and Another Person on Constituency Matters**

This means information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. A Member of Parliament includes Members of both Houses of Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.5.4 **Confidential Personal Information**

This means information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Spiritual counselling means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.5.5 **Confidential Journalistic Material**

This includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.6 **Judicial Approval of Authorisations**

4.6.1 **An authorisation is not to take effect until such time (if any) as a justice of the peace has made an order approving the grant of the authorisation.**

4.6.2 All applications for approval under paragraph 4.6.1 must be made by submitting the application for authorisation and the authorisation forthwith to the RIPA Monitoring Officer who shall make arrangements to obtain an order approving the authorisation by a justice of the peace as soon as practicable.

4.6.3 In no circumstances must any activity authorised by an authorisation be carried out unless and until the RIPA Monitoring Officer has confirmed that an order approving the authorisation has been granted by a justice of the peace.

5.0 REVIEWS OF AUTHORISATIONS

5.1 Authorisations for Directed Surveillance and CHIS last for three months and twelve months respectively from the date on which they are granted by the authorising officer. Authorisations should be subject to a monthly review to assess the need for the surveillance to continue. The review date should be noted on the application form by the authorising officer. Reviews should normally be carried out by the authorising officer who granted the authorisation but if he or she is unavailable, the review can be conducted by another authorising officer.

5.2 Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further or greater intrusion into the private life of any person should be brought to the attention of the authorising officer by means of a review. The authorising officer should then consider whether the proposed changes are proportionate (bearing in mind any extra intrusion into privacy or collateral intrusion) before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed. During a review, the authorising officer may amend specific aspects of the authorisation e.g. to cease surveillance of a particular suspect.

5.3 Except in complex cases where it is foreseen that additional tactics may be required as the operation develops, reviews and renewals should not broaden the scope of the investigation but can reduce its terms. Where other subjects may unexpectedly come under surveillance, and providing it is justified by intelligence, authorisations can anticipate it by using words such as “suspected of”, “believed to be” or “this authorisation is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known but are believed to be involved in the “criminality”. When the identities of other criminal associates and vehicle details become known, they should be identified at review and in the renewal authorisation, so long as this is consistent with the terms of the original authorisation. Otherwise, fresh authorisations are required.

5.4 When an authorisation includes a phrase such as “…other criminal associates…” a review or renewal can only include those associates who are acting in concert with a named subject within the authorisation (a direct associate) and who are believed to be engaged in a crime. It does not enable “associates of associates” to be included, for whom a fresh authorisation is required.

5.5 It is acceptable to authorise surveillance against a group or entity involving more than one individual (for example an organised criminal group where only some identities are known) providing that it is possible to link the individual to the common criminal

purpose being investigated. It is essential to make explicit the reasons why it is necessary and proportionate to include persons, vehicles or other details that are unknown at the time of authorisation but once identified they should be added at review. The authorising officers should set parameters to limit surveillance and use review to avoid “mission creep”.

6.0 RENEWAL OF AUTHORISATIONS

6.1 As mentioned in paragraph 5.1, authorisations last for three months. However, before they cease to have effect, authorisations can be renewed for a further period of three months, using the renewal form available on the intranet. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Authorisations should be renewed by the officer who granted the original authorisation but in his or her absence any authorising officer may authorise a renewal. The authorising officer for the renewal must consider it necessary for the authorisation to continue for the purpose for which it was given. The renewals last for three months and take effect on the day the existing authorisation would have expired. Authorisations can be renewed more than once provided they continue to meet the criteria for authorisation.

6.2 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously
- any significant changes to the information in the initial application
- the reasons why the authorisation for directed surveillance should continue
- the content and value to the investigation or operation of the information so far obtained by the surveillance
- the results of regular reviews of the investigation or operation

6.2.1 A renewal of an authorisation is not to take effect until such time (if any) as a justice of the peace has made an order approving the grant of the renewal.

6.2.2 All applications for approval under paragraph 6.2.1 must be made by submitting the application for renewal forthwith to the RIPA Monitoring Officer who shall make arrangements to obtain an order approving the renewal by a justice of the peace as soon as practicable.

6.2.3 In no circumstances must any activity authorised by an authorisation be carried out after the expiry of 3 months following the initial authorisation unless and until the RIPA Monitoring Officer has confirmed that an order approving the renewal of the authorising has been granted by a justice of the peace.

7.0 CANCELLATION OF AUTHORISATIONS

7.1 An authorisation must be cancelled by an authorising officer if he is satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. The authorising officer must complete a cancellation form which is

available on the intranet. If the original authorising officer is no longer available, the cancellation can be performed by another authorising officer. As soon as the decision is taken that the directed surveillance should be discontinued, the instruction must be given to all those involved to stop all surveillance of the subject.

8.0 SURVEILLANCE OF COUNCIL EMPLOYEES

8.1 Following the decision of the Investigatory Powers Tribunal in the case of *C v The Police and the Secretary of State for the Home Office – IPT/03/32/H* dated 14 November 2006, Councils may only engage the Act when in performance of their "core functions". These are the specific public functions undertaken by local authorities e.g. dealing with fly tipping, in contrast to the ordinary functions which are undertaken by all authorities e.g. employment issues, contractual arrangements, etc. The disciplining of an employee is not a core function, although related criminal investigations may be. The protection of the Act may therefore be available in relation to associated criminal investigations so long as the activity is deemed to be necessary and proportionate.

8.2 Surveillance which falls outside the Act should be dealt with in accordance with Data Protection legislation and the Employment Practices Code issued by the Information Commissioner's Office. Regard should also be had to the Council's Investigations Code of Practice document. Use of the Non- RIPA process should be considered. For further guidance on this matter you should refer to the Council's Legal Department

9.0 MAINTENANCE OF RECORDS

9.1 The RIPA Monitoring Officer maintains a central record of applications. The original of all application, review, renewal and cancellation forms should be forwarded to the RIPA Monitoring Officer for inclusion on the central record. The forms should be sent in sealed envelopes to protect confidentiality. All these records are made available for inspection by the IPCO.

9.2 Copies of all forms should be kept for a period of three years after the conclusion of any court proceedings the authorisations related to or until the next visit by the IPCO, whichever is the later.

10.0 CORRECTIVE ACTION FORMS

10.1 The RIPA Monitoring Officer will review all completed applications, review, renewal and cancellation forms when they are received by her and where necessary she will send a corrective action form to the authorising officer for completion. This will highlight errors on the completed application, review, renewal or cancellation form and notify him of action for future reference. If an authorising officer receives a corrective action form, it is his/her responsibility to consider the issues notified and respond to the RIPA Monitoring Officer with regard to remedial action to prevent recurrence of the problem highlighted on the form.

11.0 AUTHORISATION OF A CHIS

11.1 There must be arrangements in place for ensuring that at all times a designated Council Officer has responsibility for maintaining a record of the use made of the CHIS and that records that disclose the identity of the CHIS will only be disclosed to persons who have a need for access to them.

11.2 Arrangements must also be in place for ensuring that at all times a designated Council officer has day to day responsibility for dealing with the CHIS on behalf of the Council and the CHIS's security and welfare. This officer will be known as a handler and will usually be of a rank or position below that of the authorising officer. The handler will have day to day responsibility for:

- dealing with the CHIS on behalf of the Council
- directing the day to day activities of the CHIS
- recording the information supplied by the CHIS
- monitoring the CHIS's security and welfare

11.3 At all times another designated Council officer must have general oversight of the use made of the CHIS. This officer will be known as the controller and will normally be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

11.4 The authorisation of a CHIS lasts for 12 months, but should be subject to monthly review by an authorising officer.

11.5 Burnley Borough Council does not generally use a CHIS and any request to do so should be referred to the RIPA Monitoring Officer in the first instance for guidance and advice. Further guidance is contained in the relevant Code of Practice.

12.0 THE USE OF EXTERNAL PARTNERS

12.1 When a person who is not an employee of the Council is authorised to conduct covert surveillance, he is an agent of the Council. This applies to private contractors or members of another public authority. It is unwise to assume competence and, where there is doubt, an authorising officer should check it and record that he has done so. It is wise, if no collaboration agreement exists, to obtain written acknowledgment that they are an agent of the Council and will comply with the authorisation.

13.0 THE USE OF THE INTERNET AND SOCIAL MEDIASITES

13.1 ~~Viewing of open source material does not require authorisation unless and until it is repeated or systematic, at which stage directed surveillance authorisation should be considered.~~

~~13.2 Passing an 'access control' so as to look deeper into the site, for example by making a "friend request", requires at least directed surveillance authorisation. If the investigator is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member of the public, this requires CHIS authorisation.~~

13.1 It should not be assumed that all monitoring of open social media sites are automatically immune from the need for an authorisation of some sort whether RIPA applies or not. See Section 14 below for the 'Non RIPA' process to apply in cases where RIPA does not apply. Use of open media, in circumstances where there is a reasonable expectation of privacy, is likely to require an authorisation, particularly if the monitoring is intensive or for a prolonged period of time i.e. more than a week or so. The creation of fake or anonymous websites for investigation purposes is likely to require an authorisation. Entry onto chat rooms or closed groups for investigatory purposes is also likely to require authorisation unless the officer identifies himself as working for the Council and is carrying out surveillance. Use of a 3rd party's identity requires both an authorisation and express written permission from that person. Whilst overt working in this way might avoid the need for a surveillance authorisation officers should be aware that a CHIS situation could inadvertently arise. It is expected that social media sites will generate significant amounts of sensitive information. Sensitive material that is not relevant to an investigation should be quickly and safely disposed of. Any interaction between an investigator and the public via social media could inadvertently give rise to a CHIS situation. Investigators should generally avoid interaction whilst monitoring social media sites and take advice should any uncertainty arise. The use of internet and social media may require a RIPA Authorisation in the following circumstances:

13.2 Any Communications which are made with 3rd parties for the purpose of gathering evidence or intelligence about an offence in circumstances where the third party is not aware that the officer is working for the Council and that he is carrying out surveillance.

13.3 Accessing private pages of social media for the purpose of gathering evidence or intelligence about an offence or other matter subject to potential litigation.

13.4 Communication between an officer and a 3rd party for the purpose of using that person to gather evidence or intelligence about a suspect. This could be relevant in complaints against members under the Code of Conduct which include postings on social media.

13.5. Intensive monitoring of a suspect using social media over a sustained period of time particularly when this is used in connection with other methods of investigation.

13.6 Creation of a false personae or use of a third party's identity for investigation purposes.

13.7 Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, if they are not explicit that they are working for the Council and carrying out surveillance.

13.8 Repeated entry to social media sites and copying material for the purpose of an investigation is likely to engage the RIPA regime. As a rule of thumb access to Facebook and other social media sites should be made via the Council's Facebook account as opposed to a private account. If there is any doubt the officer who is conducting this activity is advised to take legal advice.

14. NON-RIPA AUTHORISATIONS

14.1 There are some types of surveillance which require Non-RIPA authorisations where the circumstances fall outside of RIPA either because the activity falls short of the technical definition of ‘covert’ or because the surveillance is covert but is not done for the purposes of prevention or detection of crime.

14.2 If the activity is not covered by RIPA it means that it is not possible to take advantage of the extra legal protection RIPA offers against being in breach of the Human Rights Act notably Article 8 and such activity is still a risk.

14.3 Therefore it is best practice to apply the principles in Article 8 by showing that you can justify the action in law and confirm its necessity and proportionality. This enables you to state that the public interest in undertaking the action outweighs the public interest in maintaining the right to privacy that the activity will intrude upon.

14.4 The best way to show that you have done this is to go through a very similar authorisation process known as ‘Non RIPA’ Process.

Where the Surveillance is Not Covert

14.5 The Non RIPA process should be used in cases where the surveillance is not ‘covert’ but would otherwise be subject to the RIPA authorisation requirements. The definition of covert see paragraph 2.2.1 in the definitions section and repeated here for ease of reference is:- 'Surveillance is covert if and only if it is carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place'.

14.6 For example, in relation to underage sales – if the premises being targeted for surveillance and test purchases (e.g. because they have been complained about or have poor records for compliance) have been warned by a letter that within a specified period of time – e.g. for the next 3 months, they are likely to be visited by a mystery shopper who is under-age and doing an observed test purchase (by hidden camera or officer whichever may be specified), this means that they are forewarned. Therefore the local authority is entitled to treat it as ‘overt’ and not to need an authorisation under RIPA. However, to be entirely sure that the process will be upheld to be lawful, the Non RIPA forms must be completed and Non RIPA authorisation obtained. This could apply in other situations where the investigating officer and ultimately the Authorising Officer believes that there is a high likelihood that private information or even sensitive private or personal data is being gathered whether collaterally or directly. (See the definition of ‘covert’ at paragraph 2.2.1 to enable you to decide whether any given situation falls outside the definition of ‘covert’.)

14.7 When an investigating officer is faced with deciding whether or not to obtain any kind of authorisation in a situation involving surveillance of an individual whether it is by investigative observation techniques or simply online or using social media, and is in doubt as to what action to take, he/she ought to seek advice from an Authorising Officer or the Legal department.

14.8 The completion of the application form will ensure that the investigating officer follows the correct decision-making process and considers the right criteria prior to taking the action. It will mitigate the risk of a breach of Article 8 human right to respect for his private and family life.

14.9 The form is very similar to the RIPA form and a copy is attached at Appendix 3 to this Policy.

14.10 The same process relating to who should be an authorising officer will apply. RIPA or Non RIPA process for Social media.

14.11 Very often the access to social media considered to be 'open source' will require a Non RIPA approval in cases where the statutory requirements of RIPA do not apply. See section 13. Usually this is because it falls outside the definition of 'covert'. See paragraph 14.5 above. However, where a sustained course of observations take place this is questionable and a RIPA authorisation will be required.

14.12 The IPCO view is that the fact that it is 'open source' does not mean that the individual's public information is 'fair game' and can be accessed, read and recorded on a file as a matter of course. If you will not be informing that person that you are observing them or conducting a surveillance operation, they will be 'unaware that it is taking place' and it is 'calculated to ensure' that the person is so unaware. So actually you need to analyse what the activity is and decide whether it should fall within the RIPA regime or not.

14.13 It is necessary to consider the subject/target's reasonable expectations of privacy from their point of view. It is reasonable to expect people to take a passing interest in what they publish for different reasons. So an individual could be aware that they can be seen publicly but not that observations for a specific investigation over a period of time are taking place. So as a general rule of thumb it is reasonable to expect that if the observations are being carried on over a period over four weeks or more a RIPA form will be needed as then it would cease to be overt in the true spirit of the definition whether it is public or not.

14.14 Non –RIPA forms are likely to be required if the proposed activity does not fall within RIPA but can be considered to be likely to breach a person's right to respect for his private and family life. So if you are going to spend over three weeks googling or otherwise monitoring a person's name on various dates during that time then that should trigger a Non- RIPA form at the very least. It may depend upon how many hits you may click on during those weeks and the type of information uncovered. Consider whether what you are seeing really is intended to be 'open source' even if you do find it on an open source site.

Scenario.

Consider the type of social media and internet surveillance you are doing. One example is a simple company director search. You can find the name and address of the Director online to find out if they are the Director of a company that you have had complaints about and consider may be committing consumer offences. Once you have that name you may google it – and receive a list of 'hits'. From just looking at

the list of those hits you may already have enough information to go and interview the person under PACE for example. So at that point you may stop and asses and decide that no further clicking and opening of sites is necessary. At that stage you have not interfered with anyone's privacy so apart from your own file notes as to what you accessed and why there are no privacy implications. If you then go on to click on all the hits and find out more information that is the point at which you need to decide whether or not you need a non-RIPA Authorisation form.

14.15 Investigating officers should use a process of monitoring what they do on social media right from the start of any investigation. This will assist them with the process of deciding whether or not they will need to complete a RIPA or Non RIPA form. It should be noted that during a Non RIPA process it may become apparent that directed surveillance is likely to take place and a fresh RIPA form should then be completed.

14.16. Investigating Officers should as soon as they are tasked with any type of online investigation, complete an internal log for their own use initially on which they record the following:- – Reason/justification for the viewing; – Assessment of the likelihood of accessing private information about individuals whether they are the target or other individuals; – Date of viewing – Pages viewed – Pages saved and where saved to – Private information gathered i.e. any information about an individual's private and family life. see Section 13 headed The use of the internet and Social Media.

14.17 At that stage the investigating officer can then review the log and decide whether more investigation is required and whether it will be likely to intrude into someone's private life requiring a Non RIPA form or a full directed surveillance operation. It is a matter of fact and degree. It is impossible to guess what such investigations may amount to as each case has its own very particular merits. If in doubt seek legal advice. **APPENDIX 1**

NOTES FOR APPLICANTS

Officers seeking an authorisation to undertake directed surveillance should:

1. Familiarise themselves with the Act and read the Council's Corporate Policy and the Home Office Code of Practice on Covert Surveillance and Property Interference. The Council's Corporate Policy and the Home Office Code of Practice can be accessed via the Council's intranet site by entering 'RIPA' into the search facility.

2. Obtain the appropriate forms from the Council's intranet site on each and every occasion. Do not alter the forms**.** There are separate forms for directed surveillance and covert human intelligence sources.

3. Obtain a unique reference number for use on applications etc relating to a particular investigation from the RIPA Monitoring Officer.

4. Complete, sign and date the relevant form (application, review, renewal or cancellation) and submit to an authorising officer for authorisation. Details of the Council's authorising officers are available on the Council's intranet site.

5. When the applicant receives an authorisation, he should keep a copy and ensure the original signed authorisation is sent to the Council's RIPA Monitoring Officer.

6. Authorisations run from the date and time they are given and not from the commencement of the surveillance.

7. No surveillance should be commenced unless and until the RIPA Monitoring Officer has confirmed that a justice of the peace has made an order approving the authorisation.

8. Authorisations always last for 3 months e.g. an authorisation granted on 29th April expires on 28th July. If the applicant only expects to undertake surveillance over a few days or weeks, he should ensure that a cancellation form is completed as soon as the surveillance has ended, rather than waiting until the end of the 3 month authorisation period to expire.

9. Ensure that review forms are completed and authorised by an authorising officer every month while the authorisation remains in force.

10. If authorisation of the surveillance is needed beyond the expiry date given on the form (which will be 3 months from the date of authorisation), the applicant should be aware of the authorising officer's need to complete a renewal form and put this into place before the end of the authorised period.

11. A renewal form should not be completed by the applicant until shortly before the existing authorisation period is due to expire. A copy of the signed renewal form should be retained by the applicant and the original signed form should be sent to the Council's RIPA Monitoring Officer.

12. If the surveillance is no longer needed the applicant should immediately complete a cancellation form which should be signed by an authorising officer. A copy of this form should be retained by the applicant and the original signed form should be sent to the Council's RIPA Monitoring Officer.

13. If the surveillance has been carried out in accordance with a written authorisation, i.e. if the paperwork is in order, the surveillance is lawful for all purposes.

APPENDIX 2

NOTES FOR AUTHORISING OFFICERS

Authorising Officers should:

1. Familiarise themselves with the Act and read the Council's Corporate Policy and the Home Office Code of Practice on Covert Surveillance and Property Interference. The Council's Corporate Policy and the Home Office Code of Practice can be accessed via the Council's intranet site by entering 'RIPA' into the search facility.

2. Read and carefully assess all applications for the use of surveillance (and renewals if the surveillance is expected to go on for longer than the statutory 3 months).

3. Ensure that a unique reference number given by the RIPA Monitoring Officer appears in the box at the top of the form.

4. Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially where it is necessary to act urgently. Where an authorising officer authorises such an investigation or operation, the central record of authorisations should record this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

5. Authorising officers should grant an authorisation only if it is necessary for the purpose of preventing or detecting crime or of preventing disorder and it is proportionate, bearing in mind the risks of collateral intrusion and the obtaining of confidential material.

6. When completing an authorisation, authorising officers must ensure that they put onto the authorisation where indicated, details of the activity and activity they are authorising in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorisation process. Whilst it is not always possible, at the outset of an investigation, to foresee how it will progress, this should not provide a reason for applicants to request a wide number of tactics just in case they are needed later.

7. Authorising officers must enter monthly review dates on any application or renewal form they are asked to authorise.

8. All application, review, renewal or cancellation forms should be signed, dated and timed by the authorising officer e.g. 29th April 2010 at 15.00.

9. Authorisations run from the date and time they are given and not from the commencement of the surveillance.

10. Authorisations always last for 3 months. Authorising officers must enter a cancellation date and time (which should be 23.59) on the application form e.g. an authorisation granted on 29th April expires on 28th July at 23.59.

11. Authorising officers should keep a note in their diary of the date upon which the authorisation was granted and a date no later than one month ahead for a review to be carried out.

12. Authorising officers must complete a review form a month after the granting of authorisation or (if required) complete the form to comply with an earlier review date of his /her own choosing. Some Service Units may wish to review authorisations after one or two weeks depending on the expected length of the particular investigation. However reviews should not be left for longer than a month.

13. Review, renewal and cancellation forms should be authorised by the authorising officer who granted the original authorisation. If for whatever reason the original authorising officer is not available, any authorising officer can sign the review, renewal or cancellation form.

14. A renewal form must be completed if the surveillance is to continue beyond the date given on the application form for the surveillance to end. Authorising officers should check the original application form if they are unsure. A renewal form must be completed before the expiry date on the application form so as to leave no gaps. If a gap is found to have been left between expiry of the authorisation and renewal, a renewal form cannot be used and a new application form must be completed immediately. Note that any surveillance activity carried out during the gap between authorisations is not covered under the Act. Officers should be prepared for an argument in court about a breach of Article 8 of the European Convention on Human Rights should they decide they must still use the evidence.

15. A renewal form should not be authorised until shortly before the existing authorisation period is due to expire. The renewal form should be dated and timed by the authorising officer from midnight on the day the previous authorisation expires e.g. 00.00 on 28th July.

16. A cancellation form must be completed as soon as the surveillance is no longer necessary or proportionate, and at any rate before the expiry of the authorisation, which could be anytime before the expiry of 3 months from the date of authorisation. Authorising officers should check the expiry date given on the form. The applicant will normally ask for the cancellation but if he does not and the authorising officer thinks it should be cancelled he/she must do so immediately. The date and time of the cancellation must be recorded on the form by the authorising officer.

17. Authorising officers should send the original signed application, review, renewal or cancellation forms to the RIPA Monitoring Officer in a sealed envelope and provide the applicant with a copy

18. If the RIPA Monitoring Officer issues a corrective action form highlighting issues on an application, review, renewal or cancellation form, it is the responsibility of the authorising officer to communicate these to the applicant, or consider his or her own part in the issues, and put in place measures to ensure that these are not repeated. The corrective action form should be returned to the Monitoring Officer with appropriate action/comments recorded by the authorising officer.

19. Authorising officers should be aware that their action in completing these forms could come under judicial scrutiny in the event of a dispute and that they may find themselves giving evidence in Court and/or being cross-examined about one of their authorisations or the Council's systems and procedures.

20. If you cease to be an authorising officer, then the RIPA Monitoring Officer should be informed. Each new appointment of an authorising officer needs to be communicated to the RIPA Monitoring Officer.