Public Document Pack

EXECUTIVE

Tuesday, 20th April, 2021
6.30 pm

EXECUTIVE

REMOTE MEETINGS - LIVESTREAM ON YOUTUBE

Tuesday, 20th April, 2021 at 6.30 pm

This agenda gives notice of items to be considered in private as required by Regulations (4) and (5) of The Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012.

Members are reminded that if they have detailed questions on individual reports, they are advised to contact the report authors in advance of the meeting.

Members of the public may ask a question, make a statement, or present a petition relating to any agenda item or any matter falling within the remit of the committee.

Notice in writing of the subject matter must be given to the Head of Legal & Democracy by 5.00pm on the day before the meeting.
Forms can be obtained for this purpose from the reception desk at Burnley Town Hall, Manchester Road or from the web at:
http://burnley.moderngov.co.uk/ecCatDisplay.aspx?sch=doc&cat=13234 . You can also register to speak via the online agenda. Requests will be dealt with in the order in which they are received.

All meetings are currently being held remotely. Members of the public wishing to address the meeting should submit their request in the usual way, and will then be invited either to join the meeting by video conference or to make a submission in writing which will be shared with the Committee.

All public meetings are being livestreamed on the Council`s Youtube Channel

AGENDA

1) *Apologies*

To receive any apologies for absence

2) *Minutes* 5 - 10

To approve as a correct record the Minutes of the previous remote meeting held on Tuesday, 23rd March 2021.

3) *Noting of Individual Executive Member Decisions - 25th March 2021* 11 - 14

To note the following Individual Executive Member Decisions made since the previous remote meeting:

Minute 5 - Beat the Streets - 250321
(Executive Member for Health and Wellbeing)

Minute 6 - Sale of Residential Freehold at Holbeck Park, Burnley - 250321 (Executive Member for Resources and Performance)

4) *Additional Items of Business*

To determine whether there are any additional items of business which, by reason of special circumstances, the Chair decides should be considered at the meeting as a matter of urgency.

5) *Declaration of Interest*

In accordance with the Regulations, Members are required to declare any personal or personal and prejudicial interests they may have and the nature of those interests in respect of items on this agenda and/or indicate if S106 of the Local Government Finance Act 1992 applies to them.

6) *Exclusion of the Public*

To determine during which items, if any, the public are to be excluded from the meeting.

7) *Right To Speak*

To consider questions, statements or petitions from Members of the Public

8) *Climate Change Working Group - Woodlands and Commemorative Trees* 15 - 16

That the cross party Climate Change Working Group (CCWG) seeks approval to allocate funds from the Climate Change budget for Woodlands and Commemorative Tree Planting.

9) *Regulation of Investigatory Powers Act (RIPA) - Corporate Policy* 17 - 48

To consider a revised corporate policy for covert surveillance and covert human intelligence sources under the Regulation of Investigatory Powers Act 2000 (RIPA).

MEMBERSHIP OF COMMITTEE

Councillor Mark Townsend	Councillor Sue Graham
Councillor Lian Pate	Councillor John Harbour
Councillor Afrasiab Anwar	Councillor Asif Raja

PUBLISHED Monday, 12 April 2021

This page is intentionally left blank

EXECUTIVE

BURNLEY TOWN HALL

Tuesday, 23rd March, 2021 at 6.30 pm

PRESENT

MEMBERS

Councillors M Townsend, L Pate, A Anwar, S Graham, J Harbour and A Raja

OFFICERS

Lukman Patel	–	Chief Operating Officer
Paul Gatrell	–	Head of Housing & Development Control
Joanne Swift	–	Head of Streetscene
Eric Dickinson	–	Democracy Officer
Alison McEwan	–	Democracy Officer
Mark Hindman	–	Graphic Designer

ALSO IN ATTENDANCE -Councillor A Hosker and Councillor M Lishman

81. Minutes

That the Minutes of the last meeting held on the 15th February 2021 were approved.

82. Minutes of Individual Decisions

That the following Individual Executive Member Decision made since the last meeting by the Executive Member for Resources and performance be noted;
Minute 4-Kickstart-230221

83. Declaration of Interest

Councillor Mark Townsend declared a Disclosable Pecuniary Interest in the item on the agenda regarding the Homelessness and Rough Sleeping Strategy 2021-2026.

84. Urgent Executive Delegated Officer Decision-Cyber Resilience Grant Funding

Decision
That the Constitutional Reporting of the Urgent Executive Delegated Officer Decision made by the Chief Executive on 040321 be noted regarding the Report and Minute relating to Cyber Resilience Grant Funding.

85. Homelessness and Rough Sleeping Strategy 2021-2026

Councillor Mark Townsend left the meeting and took no part in this item, and Councillor Lian Pate then took the Chair for this item.

Purpose
To seek approval from Members for the Homelessness and Rough Sleeping Strategy 2021-2026.

Reason For Decision
To ensure that the Council meets its statutory duty to publish a Homelessness and Rough Sleeping Strategy to cover the period 2021-2026.

To ensure that the Borough has a comprehensive strategy to effectively prevent and relieve homelessness and rough sleeping across the Borough.

Decision

(1) That the document included at Appendix 1 be approved as Burnley's Homelessness and Rough Sleeping Strategy 2021 – 2026;

(2) That the document included as Appendix 2 be approved as Burnley's Homelessness and Rough Sleeping Strategy 2021 – 2026 Action Plan; and

(3) That the document included at Appendix 3 be approved as Burnley`s Homelessness Review.

86. Homelessness Prevention Grant 2021-22

Purpose
To seek approval for the allocation of the Homelessness Prevention Grant 2021-22

Reason For Decision
To ensure that the resources allocated to this local authority under the Homelessness Prevention Grant 2021-22 are aligned with service priorities and utilized effectively to deliver the priorities of the Homelessness and Rough Sleeping Strategy.

Decision

(1) That the allocation of resources from the Homelessness Prevention Grant 2021 – 22 be approved as set out in this report; and

(2) That the Head of Housing and Development Control in consultation with the Executive Member for Housing be authorised to amend the budget allocation where necessary to align with services priorities.

87. Food Safety Delivery Plan (reviewed 2020/21)

Purpose
In order to meet statutory requirements, the Council's Environmental Health and Licensing Team is responsible for Food Safety enforcement and must have in place approved plans. In line with the Constitution, approval of the Food Safety Delivery Plan will be sought from Full Council.

Reason For Decision
To formally review past performance and agree a framework for the future delivery of effective, risk based, proportionate and consistent food safety services.

Decision
That Full Council be recommended to approve the Food Safety Delivery Plan (reviewed 2020/2021), detailed at Appendix 1 to the report.

88. Health and Safety Intervention Plan (reviewed 2020/21)

Purpose
The regulatory team responsible for Health & Safety at Work enforcement must have in in place an intervention plan to meet the requirements of statutory guidance. This report formally consults the Committee on the plans prior to their approval at Full Council.

Reason For Decision
Section 18 of the Health & Safety at Work Act 1974 and the subsequent National Local Authority Enforcement Code for Health and Safety (The Code) provide frameworks within which the Environmental Health & Licensing Team must operate when carrying out its public protection duties within workplaces. The frameworks require the Council to have plans in place to control these activities, and mechanisms for review. The intervention plan appended to this report has been prepared to satisfy the statutory requirements.

Decision
That Full Council be recommended to approve the Health and Safety Intervention Plan (reviewed 2020/2021), detailed at Appendix 1 to the report.

89. Tree Management Policy

Purpose
To seek approval to adopt the updated Tree Management Policy

Reason For Decision
The update of the Tree Management Policy is a key decision, as it will determine how the Council will manage and maintain trees on the 550 hectares of green space that it owns across the Borough.

Decision
That the Tree Management Policy (Appendix 1) be approved.

90. Bulky Waste Price Reduction Extension

Purpose
To seek approval to extend the price reduction for the Bulky Waste collection service for a further 6 months.

Reason For Decision
The initial trial period for the price reduction for the Bulky Waste Collection service was from January to March 2021. The trial has been extremely successful and very well utilised by residents. The number of requests for the Bulky Waste collection service have significantly increased during the trial period. By extending the price reduction for an additional 6 months, this will allow a longer-term assessment to be made in relation to the price and the demand for the service.

The extension of the price reduction will support local residents through the Covid recovery period and encourage continued use of the Bulky Waste collection service. This approach will support social distancing measures by encouraging residents to continue to use the service, whilst avoiding an increased impact upon Lancashire County Councils Household Waste Recycling Centres (HWRCs), which are currently operating under restrictive operational measures.

Decision

(1) That subject to recommendations (2) and (3) to keep the Bulky Waste collection service charge at the reduced price of £6.90 for a further 6 months from the expiry of the current trial;

(2) That Full Council be recommended to carry forward the unspent waste contingency budget from 2020/21 into the next financial year; and

(3) That Full Council be recommended to approve any shortfall in income during the 6-month trial to be met from the unspent waste contingency for 2020/21 and/or Covid Reserve.

91. Thanks to Retiring and Long Serving Officer

Members thanked Michael Darbyshire, a retiring Officer currently working in the Streetscene Service Unit, for 43 years of service to the Borough including working on many projects both in Padiham and in Burnley.
Members highlighted his can-do attitude and that he was an exemplar of fantastic service, and stated their best wishes for his well-deserved retirement.

92. Exclusion of the Public

That the public be excluded from the meeting before discussion takes place related to Minute 93 on the grounds that in view of the nature of the business to be transacted if the public were present there would be a disclosure to them of exempt information within the meaning of Part VA of the Local Government Act 1972 relating to the financial or business affairs of any particular person (including the authority holding that information).

93. Stairlift Procurement

Purpose
To seek approval from Members to enter into a contract with Stannah Stairlifts through a procurement framework with Procurement For Housing.

Reason For Decision
To ensure the Council continues to deliver stairlifts to disabled people through the disabled facilities grants programme. The continued installation of the stairlifts helps people to remain living independently in their own home.

Decision

(1) That authority be delegated to the Head of Legal and Democratic services to sign the procurement framework contract; and

(2) That authority be delegated to the Head of Housing and Development Control to amend any terms of the contract.

This page is intentionally left blank

INDIVIDUAL DECISION BY THE EXECUTIVE MEMBER FOR HEALTH AND WELLBEING

BURNLEY TOWN HALL

PRESENT

OFFICERS Eric Dickinson - Democracy Officer

5. Beat The Streets

Purpose	The seek approval to allocate £20,000 from the Community Recovery Fund to the Beat the Street Project.
Reason For Decision	Beat the Street is an innovative means to encourage more people to become active. Maintaining an active lifestyle and a healthy weight is one of the key ways of reducing the adverse impacts of CoVid19 as well as protecting against many other illnesses such as diabetes, heart disease and depression.
Decision	That the Executive Member for Health and Wellbeing approves the allocation of £20,000 to the Beat the Street Project from the CoVid19 Recovery Fund.

Decision made by: Councillor Lian Pate
Executive Member for Health and Well Being

Date: 24/03/2021
Decision Published on: 25/03/2021

This page is intentionally left blank

INDIVIDUAL DECISION BY THE EXECUTIVE MEMBER FOR RESOURCES AND PERFORMANCE

BURNLEY TOWN HALL

PRESENT

OFFICERS Eric Dickinson - Democracy Officer

6. Sale of Residential Freeholds-Holbeck Park, Burnley

Purpose	To seek approval of the sale of residential freeholds at Holbeck Park, Burnley
Reason For Decision	To enable new home buyers to access Government "help to buy" when purchasing new homes
Decision	That the following be authorised by the Executive Member for Resources and Performance;

(1) The sale of freehold interest in completed houses on the development at Holbeck Park and on other similar developments elsewhere.

(2) The Head of Finance and Property to approve the final terms of sale,

(3) The Head of Legal & Democracy to complete the legal documentation necessary to give effect to the decision.

Decision made by: Councillor Sue Graham
Executive Member for Resources and Performance

Date: 24/03/2021
Decision Published on: 25/03/2021

This page is intentionally left blank

ITEM NO	

REPORT TO THE EXECUTIVE

DATE	**20th April 2021**
PORTFOLIO	
REPORT AUTHOR	**Climate Change Working Group**
TEL NO	
EMAIL	**sgoff@burnley.gov.uk** **pgatrell@burnley.gov.uk**

Cross-party Climate Change Working Group Recommendations on Woodlands and Commemorative Trees

PURPOSE

1. To seek approval of the Executive to allocate funds from the Climate Change budget.

RECOMMENDATION

2. The cross-party Climate Change Working Group (CCWG) recommends that:

   a) The Executive approves the allocation of £18K from the Climate Change budget towards woodland and commemorative tree as outlined in this report.

   b) That Full Council be recommended to note the Executive's decision and report.

REASONS FOR RECOMMENDATION

3. The schemes identified in the report will contribute to the objectives of reducing CO2 emissions and carbon sequestration.

SUMMARY OF KEY POINTS

4. The CCWG has considered the following proposals and recommends that the Executive approves the following allocation of funds from the Climate Change budget:

   Contribution of £15K to Lancashire Woodlands Connect

5. The River Ribble Trust has launched a decade-long campaign to plant more than half a million trees in Lancashire to fight climate emergency, improve air quality and reduce flooding and remove 100,000 tonnes of CO2 from the atmosphere.

6. Local authorities have been invited to become partners in the project. A contribution of £15K will enable the River Ribble Trust to undertake surveys and use their existing

mapping tools to identify, develop and secure grant funding to implement woodland planting schemes in Burnley.

7. By partnering with the RRTs Lancashire Woodlands Connect project and other Lancashire authorities, Burnley is more likely to be successful in securing grant funding for tree planting from the Government's Great Northern Forest initiative and the recently announced Local Authority Treescapes Fund.

8. Adjoining authorities including Hyndburn, Pendle and Blackburn have already signed up as partners

Contribution of £3K to the CoVid Commemorative Tree Scheme

9. The cross-party Climate Change Working Group wishes to link the spirit of tackling climate change through tree planting with remembrance of those who have sadly passed away from CoVid in the Borough.

10. CCWG recommends that the Executive approve an allocation of £3,000 which be used to plant a flowering cherry tree in each of the 6 main parks in partnership with the park friend's groups, which will help to co-ordinate and promote the planting ceremony in each park.

11. The cherry trees will flower in late March/early April, marking the anniversary of the beginning of the pandemic. Each tree will be of a good size (3-4m height) to have an immediate impact and will have an inscribed stone tablet and be planted around with native daffodils.

FINANCIAL IMPLICATIONS AND BUDGET PROVISION

12. The expenditure identified in this report amounts to £18K out of budget provision of £50K

POLICY IMPLICATIONS

13. The schemes identified in the report will contribute to the objectives of reducing CO2 emissions and carbon sequestration.

DETAILS OF CONSULTATION

14. Consultation with the Climate Change Working Group

BACKGROUND PAPERS

15. None

FURTHER INFORMATION	
PLEASE CONTACT:	**Simon Goff 07971 033197**
ALSO:	**Paul Gatrell**

Regulation of Investigatory Powers Act – Corporate Policy

REPORT TO THE EXECUTIVE

DATE	**20th April 2021**
PORTFOLIO	**Resources and Performance Management**
REPORT AUTHOR	**Catherine Waudby**
TEL NO	**01282 477198**
EMAIL	**cwaudby@burnley.gov.uk**

PURPOSE

1. To consider the revised Corporate Policy for Covert Surveillance and Covert Human Intelligence Sources under the Regulation of Investigatory Powers Act 2000 ("RIPA").

RECOMMENDATION

2. To approve the revised Corporate Policy for Covert Surveillance and Covert Human Intelligence Sources under the Regulation of Investigatory Powers Act 2000 ("RIPA")

REASONS FOR RECOMMENDATION

3. To fulfil the IPCO's recommendations to review the Policy.

SUMMARY OF KEY POINTS

4. RIPA regulates the Council's use of covert surveillance to prevent and detect criminal activity.

5. The Council's Policy for the use of Covert Surveillance and Covert Intelligence Source. was provided to the Investigatory Powers Commissioner's Office (IPCO) during the latest assessment which took place in March 2020. The report of the Investigatory Power's Commissioner made recommendations to further strengthen compliance with the legislation. These included revising the Policy to include examples of the types of matters the Council may come across and strengthening the policy in relation to the use of social media. Regular staff training on RIPA was also recommended.

6. The review of the Policy has been completed. The Policy attached to this Report has been updated to reflect changes in the organisation and generally. The section on the use of social media has been expanded to explain situations where RIPA may be engaged. The Policy also introduces the concept of a non- RIPA authorisation. This is to be used in cases where RIPA is not engaged as the activity carried out by the Council is

not strictly covert because the premises have been previously warned of a visit for a test purchase or where covert surveillance is undertaken but it is not in pursuance of the investigation of a crime. The use of a non RIPA authorisation is recommended to ensure that the Council does not breach Article 8 of the Human Rights Act 1998 – the right to respect for one's private and family life.

7. Training on the revised Policy is proposed to ensure that officers in the Council understand the obligations under RIPA and the wider circumstances where a non – RIPA type authorisation should be sought.

FINANCIAL IMPLICATIONS AND BUDGET PROVISION

8. None

POLICY IMPLICATIONS

9. None

DETAILS OF CONSULTATION

10. The Policy was considered by the Audit and Standards Committee on 24th March 2021 who resolved to recommend the approval of the revised Policy to the Executive.

BACKGROUND PAPERS

11. None.

FURTHER INFORMATION

PLEASE CONTACT: CATHERINE WAUDBY

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 IPCO on a regular basis and is required to provide annual statistics to the IPCO of 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.

Unique Reference Number	

NON-RIPA Authorisation Form

Application for Authorisation to conduct Covert Surveillance not regulated by RIPA

Sample Form with Notes to Assist Completion

This form should be completed by an officer of the Council seeking authorisation to carry out surveillance which **does not** fall within the definition of Directed Surveillance in section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA). This could include surveillance where the target is doing something which is not a criminal offence (or which does not carry a term of imprisonment of six months or more), misusing the work email/internet system or breaching a legal agreement (e.g. tenancy agreement) or overt surveillance such as in noise nuisance cases with a MATRON or other equipment where the subject has been warned that the surveillance could take place.

Before completing this form, please consult the Council's Corporate Policy, the Home Office Codes of Practice, and the Guidance by the Investigatory Powers Commissioners Office (IPCO.) Please use this form and after reading the notes please delete them and replace with the correct details as required.

Once completed this form should be forwarded to your manager to complete box 11 onwards.

Public Authority *(including full address)*	Burnley Borough Council Town Hall, Manchester Road, Burnley, BB11 1JA		
Name of Applicant		**Service Unit**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION

1. Give rank or position of the authorising officer

2. Describe the purpose of the specific operation or investigation

Explain what is being investigated. For example:

- Misuse of email/internet
- An employee "fiddling" his/her timesheet
- Breach of a tenancy agreement
- To obtain evidence to justify the service of a noise abatement notice where private information could be obtained.
  If possible, include the relevant legislation that which gives you the power/duty to investigate the matter and to take action.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, and recorded) that may be used.

The key phrase is "in detail." Therefore, a response which merely states "Video camera and recording equipment will be installed a at a fixed point" will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- How long will the surveillance last?
- Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times?
- Which premises are to be used and/or targeted?
- Which vehicles are to be used? Are they public or private?
- What type of equipment is to be used? e.g. covert cameras, audio devices
- What is the capability of the equipment to be used? e.g. zoom lense, remote controlled etc.
- Who else will be involved in the operation and what will be their role? e.g. private detectives, police

It may be appropriate to attach plans/maps showing where and how the surveillance will be conducted and indicating where any surveillance equipment will be installed.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity of the target(s) then say so. You could include a general description of the targets.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

Your statement here should be more detailed than in Box 2. You should give details of the precise information sought by those doing the surveillance. For example:

- "To ascertain what time the employee enters and leaves the office."
- "To find out what websites the employee has been visiting and what images have been downloaded."

6. Has any warning/notice been served on the target? If not, explain why this surveillance needs to be covert

The warning could be general one (e.g. signs/published policy) or it could be more specific (e.g. letter).

Explain any overt methods e.g. direct contact with the perpetrator or evidence from witnesses you have tried to obtain the evidence/information or why they are not appropriate.

Explain the consequences of the target finding out about this surveillance or if a warning had been given what are the chances of private information being obtained.

7. Explain why this surveillance is necessary

Include in this box details of:

- Why surveillance is needed to obtain the information/evidence that is sought
- Any other means you have tried (not involving surveillance) to obtain the same information/evidence
- Any other evidence/information you have to link the target with the offender which requires corroboration through surveillance.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion.

When doing surveillance, you may be invading the privacy of those who are not your target. You are required to think about their rights and what you can do to minimise the impact on them of your surveillance. People who may be the subject of collateral intrusion include:

- fellow employees
- visitors to a property
- friends or relatives of the suspect

When completing this section, three matters should be addressed:

Firstly, identify which third parties will be the subject of collateral intrusion and what that intrusion will be i.e., what information will be captured about them?

Secondly, state why this is unavoidable. This could be because of the nature of the premises (e.g., a restaurant) or because of what the person is doing (e.g. visiting the subject/target premises). In some cases there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly, set out what steps you have taken to minimise collateral intrusion if this is possible.

If you cannot minimise collateral intrusion you still need to show you have considered it. In some situations, all you may be able to state is that you cannot do anything to minimise collateral intrusion but you will not be making any decisions based upon the information gathered about third parties unless it shows them committing a criminal offence. Furthermore, you will ensure that officers who do the surveillance or view any recordings are mindful of who the real target of the surveillance is.

9. Explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

The RIPA Covert Surveillance Home Office Code of Practice contains detailed guidance on proportionality:

“4.5 This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who might be affected) against the need for the activity in investigative and operational terms.”

“ 4.6 The authorisation or warrant 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 alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.”

Here you demonstrate that you have:

- balanced the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explained how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considered whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
- evidenced, as far as reasonably practicable, what other methods had been considered and why they were not implemented or have been implemented unsuccessfully.

In order to comply with the above you need to address the following questions:

- Can you get information using less intrusive means/overt methods?
- What other means have you tried to obtain the same information/evidence?
- What have you done to try and lessen the impact on the target? Factors to address include:
  - Amount of information to be gathered during surveillance
  - The way the surveillance is done e.g. using still cameras rather than video to capture less information or using one camera rather than two.
  - Impact of the surveillance on the subject
  - Timing of the surveillance

At the same time, the above must be balanced with the need for the activity in operational terms. To demonstrate this balance you should address:

- What you are seeking to achieve?
- Seriousness and extent of the offence
- Impact of the offence on the victims, others/wider community and on the public purse

For more guidance on proportionality see chapter 4 of the RIPA Covert Surveillance and Property Code of Practice issued by the Home Office and the Employment Practices Data Protection Code issued by the Information Commissioner (Part 3).

10. Applicant’s Details			
Name (print)		**Telephone no.**	
Grade/Rank		**Date**	

Signature	

11. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: *[Why is the surveillance necessary, Who is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. Ensure that you are satisfied that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that it does not continue after the investigation is complete. Sufficient detail must be included here to demonstrate that you, as the Authorising Officer, have considered the application objectively. Reference can be made to the boxes completed by the Investigating Officer above but "cut and paste" should be avoided. The five "Ws" stated above must be addressed in detail. This is important so that the Investigating Officers are clear as to what they can and cannot do and the means they can adopt. You should not be afraid to reject the application if it lacks clarity or detail.

12. Explain why you believe the surveillance is necessary. Explain why you believe the surveillance to be proportionate to what is sought to be achieved by carrying it out.

You should satisfy yourself that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection. Set out what matters in the respective boxes you have given particular weight to when considering necessity and proportionality. You can also add any additional factors you have considered.

Date of first review		If the surveillance operation is going to last more than a month then you should consider whether it should be reviewed after a period of time. During a review, consideration will have to be given to whether the surveillance is still necessary and proportionate.		
Programme for subsequent reviews of this authorisation: Only complete this box if review dates after the first review are known. If not or inappropriate to set additional review dates then leave blank				
Name (print)		**Grade/Rank**	State the position of the Authorising Officer e.g. Head of Audit	
Signature		**Date and time**		
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, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons.				
Expiry date and time				

NOTE: Once an authorisation has been granted, a copy of this form must be sent to the legal department or other person in charge of keeping such records.

When the surveillance has ended or is no longer required it is good practice to cancel the authorisation. This can be done using the following form.

This page is intentionally left blank