City of Bradford MDC
www.bradford.gov.uk

Report of the City Solicitor to the meeting of the Governance and Audit Committee to be held on Tuesday 27th June 2017.

D

Subject: Regulation of Investigatory Powers Act 2000 (RIPA) – Policy, use and enforcement activity – Annual Review

Decision of the Governance and Audit Committee held on 28th June 2016:

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) – POLICY, USE AND ENFORCEMENT ACTIVITY – ANNUAL REVIEW

Resolved -

Resolved-

(1) That the duties placed on the Council under the Human Rights Act 1998 were considered in the context of this report.

(2) That the Council's continued compliance with RIPA and the completion of OSC (Office of Surveillance Commissioners) recommended training following the inspection in July 2013 be noted.

(3) That the OSC inspection scheduled for the 13th October 2016 be noted and a report relating to the outcome of the inspection be presented to the Committee in April 2017.

(4) That the 2016 programme of training of Officers (in order to continue to raise awareness) and enforcement officers under RIPA be noted.

(5) That the guidance at Appendix 3 attached to Document "B" (regarding Internet investigations and the communication to all Assistant Directors and Enforcement team Managers in order to raise awareness of the risks of such investigations) be approved as Council Policy.

Action: City Solicitor

City Solicitor
Parveen Ahktar
Report Contact: R J Winter – Senior Lawyer
Interim Team Leader Property Commercial and Development
RIPA Coordinator and Monitoring Officer (RICMO)
Phone: 01274 434292
Email: richard.winter@bradford.gov.uk

1. Summary

This report is prepared to provide information relating to:-

- The legal framework and how the Council's officers may deploy covert surveillance techniques authorised and approved under RIPA to investigate serious crime.
- The OSC inspection October 2016.
- The Council's use and outcomes of authorised and approved covert surveillance operations for the last 3 years and overt enforcement activity.
- The role of the Council's Senior Responsible Officer (SRO), the Council RIPA Coordinator and Monitoring Officer and the annual review and internal audit May 2017
- The Council's continued compliance with RIPA, use of close circuit television (CCTV), body cameras and covert internet Investigations.
- The 2017/18annual training programme for officers.
- Contribution to the Council's priorities.

NB Please see Glossary at APPENDIX 5

2. The Legal Framework and how the Council's officers use RIPA.

2.1 As members are aware RIPA provides a legal framework for the control and regulation of covert (''covert'' is defined as being calculated in a manner to make sure that the person subject to the surveillance is not aware it is been carried on) surveillance and information gathering techniques.

2.2 Given the highly technical nature of the legislation, codes of practice and guidance a glossary of terms is set out at appendix 5 of this report to assist members and officers of the Council.

2.3 Covert surveillance techniques may be used by officers of public bodies (including officers of the Council when investigating ''serious crime'' (by definition offences which carry a term of imprisonment of six months or more) and where there are no overt means of obtaining the evidence but conditional on it being necessary and proportionate to what it seeks to achieve. The Council's stated policy has for many years restricted covert surveillance to serious crime. The Councils historical stated policy of limiting the use of covert surveillance techniques to serious crime became mandatory by statute following amendments to RIPA which took effect from the 1st November 2012.

2.4 There are three types of covert techniques (with the objective of obtaining evidence to prove serious crime) available for use by the Council's investigating officers namely by definition ''directed surveillance'' (DS), ''a covert human intelligence source'' (CHIS) and ''data communications '' (DC) investigation.

2.5 Surveillance includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without assistance of a surveillance device and includes the recording of any information.

2.6 A fourth covert surveillance technique defined as ''intrusive surveillance''(IS) is surveillance that is carried out in relation to anything taking place on residential premises or in a private vehicle and involves the presence of a person or device in the premises or vehicle or the use of a surveillance device. NB This type of surveillance can only be undertaken by the Police and Intelligence Services and not local authority investigators.

2.7 Directed surveillance is covert, but not intrusive, surveillance that is conducted for the purposes of a specific investigation or operation that is likely to result in the obtaining of private information about a person and is conducted otherwise than as an immediate

response to events or circumstances of such a nature that it would not be reasonably practicable for an authorisation to be sought.

2.8 A covert human intelligence source is someone who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining, disclosing or providing access to private information. This includes public informants who work for the Police and Security services the Council's criminal investigators who make test purchases or act as secret passengers in taxi investigations in certain limited circumstances.

2.9 Data Communications (DC) with the covert purpose of obtaining of private information can include the post, phone calls and text messages to and from a person. The obtaining of DC by an investigator can only include information regarding the 'who', 'when' and 'where' of a communication e.g. Letters from and to a named person, telephone numbers of calls made to and by a named person (subscriber) and text messages and emails made to and from a defined number of a subscriber. DC investigations can not include the 'what' (i.e. the content of what was said or written in a telephone call text message email or letter. RIPA groups DC into three types: 'traffic data' (which includes information about where the communications are made or received); 'service use information' (such as the type of communication, time sent and its duration); and 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services). This information can only be obtained via a service provider such as the Post Office, British Telecomm, Orange, AOL and Yahoo etc.

2.10 The need for regulatory control and careful control by RIPA arose following the enactment of the Human Rights Act 1998 (HRA) which embodied in English Law (amongst other rights) Article 6 (Right to a fair trial) and Article 8 (Right to respect for a private and family life) of the 1950 European Convention of Human Rights (ECHR1950). It was not specifically enacted to address terrorism although undoubtedly this forms part of its remit in the context of the investigation and detection of exceptionally serious crime by the Police and Security Forces.

2.11 If a Council investigator uses a covert investigation technique without proper authorisation then the Council is liable in damages to the person subject to the investigation for breach of their Human Right to a private and family life and can seek damages against the Council from the civil courts. Such action is contrary to the Council's policy on the use of covert surveillance and is a breach of its disciplinary code see Para 6.9 at appendix 1.

2.12 The Council has a number of teams of enforcement officers based in the Council's Environmental Health Service, the Housing Standards Service, the Planning and Building Control Service, the Corporate Fraud Team. the Licensing (liquor licensing and taxi licensing) service, the Council's Joint West Yorkshire Trading Standards Service (WYTSS), the antisocial behaviour team and Youth offending Team.

2.13 As stated above since November 2012 directed surveillance authorised by RIPA must relate to ''serious offence '' by definition i.e. carry a penalty of at least six months in prison. It is worthy of note ''the serious offence test'' is satisfied for example in respect of offences investigated under the Food Safety Act 1990, the Environmental Protection Act 1990, the Social Security Administration Act 1992, the Fraud Act 2006 and the Trade Marks Act 1968. Also the sale of alcohol (Licensing Act 2003) or cigarettes (Children's and Young Persons Act 1933) to a person under the age of 18 is also regarded as a serious offence even though the penalty is £5000.00 and £2500.00 respectively.

2.14 The Council's enforcement teams are very much more often than not able to gather sufficient evidence of the criminal offences which connect with the Council's investigatory powers by overt means.

2.15 In exceptional circumstances investigators may need to use a covert investigative technique mentioned above authorised and approved under RIPA to prove the offence under investigation.

2.16 Authorisations under RIPA when required must be sought by the Council's investigating officers from the Council's Chief Executive (or in her absence the nominated Strategic

Director), the City Solicitor or the Assistant City Solicitor and are limited to the ground of the prevention or detection of serious crime.

2.17 If and when an authorisation is granted for covert surveillance before the authorisation can be acted upon the Court must be invited to scrutinise the authorisation and approve it.

2.18 Only where covert surveillance is considered to be necessary and proportionate can an authorisation be granted and approved by the Councils authorised officers and the Court respectively.

2.19 During covert investigations some private information about the suspect and non suspects e.g. members of the public visiting the suspect's home or work place could be potentially included in the covert evidence gathering. This evidence must not be recorded or used in respect of none suspects. Evidence not relevant to offences is destroyed or not recorded at all. This reduces what is described in RIPA as 'collateral intrusion'.

2.20 The investigating officer's approved authorisation is also limited by its duration. The evidence recorded is limited to evidence which can support the criminal offence being investigated.

2.21 RIPA also contemplates and defines confidential information which is information of a type which if obtained is more holds a greater level privacy than other '' private information ''.

2.22 Confidential information is defined as ''medical or religious information''. No such information has ever been authorised to be sought by the Council's enforcement officers, as it is highly unlikely to be relevant to the commission of any criminal offence investigated by a local authority. Care should be taken in the investigation of the breaches of local government regulatory law not to seek or record confidential information. If confidential information is to be sought then the authorisation can only be granted by the Council's Chief Executive as Head of the Council's Paid Service.

2.23 RIPA and associated Regulatory Codes of practice and guidance define Covert Human Intelligence Source (CHIS).

2.24 Since 2000 RIPA has not been used by the Council's officers to investigate none serious crime i.e. breaches of schools' admission policies, dog fouling or littering. Investigation of this type i.e. of less serious criminal offending has historically been widely criticised in the press and advised against by the Local Government Association. Indeed some years ago the Council's admissions policy has been amended to make it clear only overt investigations relating to such breaches of the policy are used by the Council.

2.25 The Council other than through the West Yorkshire Trading Standards Joint Service (WYTSJS) has not needed to obtain evidence of criminal offences by the acquisition of ' Data communications ' under RIPA i.e. interception of mail, details of the use of telephone either mobile or land lines or use of the internet.

2.26 The Council is periodically audited by an appointed inspector of the Office of the Surveillance Commissioner (OSC). The OSC audited the Council compliance with RIPA in 2002, 2004, 2006, 2010, 2013 and 2016 commendations and recommendations followed each inspection.

2.27 The Council is also externally audited by the Office of the Interception of Communications Commissioner. (OICC) An inspection was undertaken by the inspector of the OICC in September 2012 and the report was entirely satisfactory.

2.28 The Council was recommended to use officers of the local government national anti fraud network (NAFN) if data communication authorisation is required. Those officers are based at Tameside and Brighton Councils. To date no such authorisation has been required.

3. External inspection by the OSC October 2016.

3.1 In October 2016 the Council was inspected by His Honour Judge Norman Jones QC as Deputy Surveillance Commissioner from the Office of the Surveillance Commissioner. The conclusions and recommendations can be seen below.

3.2 **Conclusions** (including a summary of those relating to the West Yorkshire Trading Standards Service arising from the inspection at Wakefield Council on 20th July 2016)

a) Bradford MDC has continued to reduce its resort to covert surveillance until it now does not undertake such activity. Nevertheless it maintains a highly effective *RIPA* process supported by excellent officers and comprehensive guidance. Whilst it is not possible to assess the quality of authorisation those applications which were refused were of a good standard. A good training programme is in existence which could perhaps be supplemented periodically by external professional training and more regularly by e--learning.

b) It was somewhat disappointing to note that some of the recommendations of the last inspection were not fully discharged. Undoubtedly Mr Winter will pay attention to ensuring that they are now discharged alongside those few recommendations of this report.

c) West Yorkshire Trading Standards Services .The WYTSS is a joint services body which forms part of West Yorkshire Joint Services which holds devolved powers from each of the five West Yorkshire local authorities (Bradford, Calderdale, Kirklees, Leeds and Wakefield) in relation to a number of functions including trading standards. WYTSS acts as the trading standards authority for each Council. Wakefield MBC is the lead Council collecting contributions from each of its sister councils and being responsible for the resulting resources being applied to the Service.

d) Mr David Strover, Trading Standards Manager at the WYTSS, IS the Senior Responsible Officer appointed by the Service and attended at the inspection conducted at Wakefield Council on 20 July when general trading standards issues and those pertinent to each individual authority were 'discussed. Consequently a substantial portion of this section of this report is common to each of the five West Yorkshire authoritiee inspected in this round of inspections and will appear in each such report.

e) The WYTSS now rarely resorts to covert surveillance. Whilst it continues its juvenile test purchasing activities it does not utilise video recording equipment and a protection officer in the shop at the time of a purchase is instructed to confine his/her observations to the transaction taking place. The view is taken that no private information is likely to be obtained and no relationship requiring *CHIS* authorisation takes place. Hence *R/PA* is not engaged for these purposes. The service has only undertaken two authorisations since the last inspection one in Leeds and the other in Kirklees.

f) The lack of authorisation was considered with Mr Strover and three principal reasons were advanced.

- it has been found in almost all circumstances that satisfactory overt processes were available for the gathering of information;
- staffing levels have been substantially reduced thus curtailing the range of activities that can be undertaken;
- there has been a reduction in prosecution with more emphasis laid on advisory procedures.

g) No authorisation has been granted for WYTSS by Bradford MDC since the last inspection.

h) WYTSS does not engage in covert surveillance thus reflecting an ethos of openness which permeates all of the West Yorkshire local authorities. Were it to be felt to be required' the Service is trained and competent to undertake such activity and on rare occasions does so. The applications reviewed during these inspections are of a high quality and it is anticipated future applications will reflect that good performance.

3.3 Recommendations to the City of Bradford MDC and the WYTSS.

a) Amend the Central Record of Authorisations. (Paragraph 9 The Central Record of Authorisations is contained within separate spreadsheet records with a separate record for each Directorate. The Central Record is maintained by Mr. Winter and is compliant with the *Codes* of *Practice* requirements save that it continues, as at the time of the last inspection, to require a column to reflect self authorisation. A prompt is activated to remind the *RIPA Co-coordinating Officer* when an authorisation is approaching its expiry date. It is noted that following the advice tendered at the time of the last inspection the record now contains refusals as well as grounds of authorisation. Three such refusals have been recorded since the last inspection. Consideration' should be given to combining the separate records into one central record spreadsheet document covering all Directorates.

b) Raise *RIPA* awareness throughout the Council. (Paragraph 19 the level of *RIPA* awareness throughout the Council was discussed and it was conceded that more required to be done. It is appreciated by the officers that the greatest risk of unauthorised surveillance lies with it being undertaken by officers who are ignorant of the requirements for consideration of *RIPA* authorisation whenever covert surveillance is contemplated. The problem was addressed some 'four years ago by a *RIPA* article being placed in the internal newsletter but the exercise has not been repeated. Reliance is placed on the raising of the issue at top-level management meetings with the hope that the information can be cascaded down to officers within departments. Again it was conceded that the cascade is likely to become a small trickle by the time the information reaches the lower levels of the staff where the risk of unauthorised surveillance is greatest. It was agreed that the *RIPA Co-coordinating Officer* should be more proactive in this role in the insertion of articles within the Council's intranet information channels to ensure it reaches all staff.).

c) Amend the *RIPA policy, guidance and procedures document. (Paragraph 26* The Council's policy and guidance on *RIPA* is to be found in its *RIPA Policy, Guidance and Procedure Document* which was last reviewed in January 2016 and again updated in September. It has been described in the previous three inspections reports as being of high quality, and it remains so. Only one amendment is required which was raised at the time of the last inspection but not undertaken. That is to remove references to the urgency procedures which are no longer available to local authorities.)

d) Ensure regular reports are given to Elected Members which include information relating to *RIPA* activity or inactivity. (Paragraph 27An annual report is made to the Audit and Governance Committee of the Council accompanied by a copy of the annual *RIPA* audit undertaken by Mr. McKinnon-Evans. A report is given to the Leader of the Council whenever an authorisation is undertaken. Care must be taken to ensure that this is a report and that the Leader does not become personally involved in any element of the determination of the authorisation. Currently there are no further regular reports given to councillors on *RIPA* activity or inactivity. This practice does not fully address the requirements of the *Code of Practice for Covert Surveillance and Property Interference,* 3.35 which requires that *"(elected members) should also consider internal reports on the use of the 2000 act on* a *regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose".* This may be achieved by a more regular reporting process to a committee of the Councilor by direct information being given to Councillors through other regular communications).

e) Reinstate the equipment record and make it a subject of the internal *R/PA* audit. (Paragraph28 it is a requirement of the *Policy, Guidance and Procedures Document* that a schedule is maintained of all equipment that may be used for covert surveillance purposes. Mr. Winter was of the opinion that such a schedule was maintained up to a few years ago but that it had fallen into abeyance. It was advised that it should be reinstated and that its contents should be subject to the annual *RIPA* audit).

f) Amend the WYTSS policy and procedures document. (Paragraph 40The Service has its own individual policy and procedures document which was made available at the Wakefield inspection. I have had the opportunity subsequently to review it. Whilst it is succinct and easily read and provides the ground. work basis for an application it does not purport to be a comprehensive guide to *RIPA.* Further reference to the Codes of *Practice* is required and, following its publication in July 2016, reference to the current edition of the OSC *Procedures and Guidance* should be afforded. Following an internal audit of the Service in July 2016 a report was produced by Wakefield Council indicating overall satisfaction with the arrangements for *RIPA* authorisation but remarked upon the lack of any guidance relating to the use of social media sites, a view endorsed by this report. The following amendments should be undertaken:

- A section should be introduced dealing with the noticeable omission of social media guidance. For further guidance see **CHIS and** Social **Media** above and the OSC *Procedures and Guidance 2016, paragraph 289.*
- The guidance document should provide' reference to the fact that the penal threshold introduced by the *RIP (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 1500,* is only applicable for *directed Surveillance* and does not apply to *CHIS.*
- It should be made clear that the duration period of an authorisation commences with the magistrate's approval.
- All documents and flowcharts should distinguish between <u>authorisation</u> which is granted by a Council authorising officer and <u>approval</u> which is granted by a magistrate.

3.4 The four recommendations made in the 2013 lOSC report were as follows.

t. *Embrace the CEO, and whoever may deputise for him in his absence, within the RIPA training programme and ensure they receive training to enable· them to authorise in the event* of *being required to do so.*

Mr. Winter has provided training on one occasion to the CEO on a one-to-one basis in April 2016. <u>This recommendation has been partially discharged</u>.

ll. Officers should be trained to manage CHIS.

Three officers, including one from the fraud team, together with Mr. Winter, attended in July. 2013 training organised by Wakefield MDC but delivered by officers from the West Yorkshire police which included specific training directed to the management of *CHIS.* <u>This recommendation has been discharged</u>.

iii. Amend the Policy Guidance and Procedure.

This related to the removal of a section concerning urgency procedures which are no longer available to local authorities following the *Protection* of *Freedoms Act 2012*. These have not been removed and consequently t<u>his recommendation has not been discharged.</u>

iv. ***(West Yorkshire Trading Standards Service)***

Ensure that officers are equipped to undertake and manage social networking site investigations in accordance with RIPA requirements if and when authorisation for such is obtained. The training delivered by West Yorkshire police in July 2013 was attended by officers WYTSS. This covered detail practices which were appropriate for those engaged in social media investigation. This recommendation has been discharged

4. The Council's use and outcomes of authorised and approved covert surveillance operations for the last 3 years and overt enforcement activity generally.

4.1 The figures for authorisations for the last 3 years are set out below. The figures relate to each department that could have used covert surveillance authorised under RIPA prior to November 2012 i.e. Environmental Health Service (EHS), Corporate Fraud Team (CFT), Planning and Building control service, Hackney Carriages and Private Hire (Taxi Licensing) service, Liquor Licensing service, the Housing standards service, the Antisocial behaviour team (ASBT), the West Yorkshire Trading Standards service (WYTSS) and the Youth offending team (YOT). Since November 2012 there are no longer any offences which meet the definition of the ''serious offence test'' which are investigated by the Council's Housing Standards service, the ASBT ,the YOT, the Planning and Building Control service and the Councils Licensing services. This gives in an explanation as to why the numbers of authorisations appear as ''not applicable'' for each of the last 3 years in those enforcement services. In any event in the author's opinion the investigation of the types of offences in those service areas (see below) do not require the use of a covert investigative technique.

Year	EHS/	WYTSS	CFT	Planning Service & Building Control	Housing Standard service	ASBT and YOT	Licensing Services	Refusals /withdrawn	Authorisations/Approvals
2014/15	0	0	0	n/a	n/a	n/a	n/a	0	0
2015/16	0	0	1	n/a	n/a	n/a	n/a	1	0
2016/17	1	0	1	n/a	n/a	n/a	n/a	2	0

4.2 It can be seen from the above list in those service areas which can still seek authorisation of directed covert surveillance under RIPA i.e. investigate offences which carry a term of imprisonment of six months or more, by comparison of the last 3 years the number of authorisations to NIL as overt means of obtaining evidence have been found e.g. data sharing by public bodies e.g. between the CFT and the DWP and additional powers to obtain information for example from banks and interview techniques bring a greater focus on overt means (see table below). In the last year the authorisations have fallen to zero across all departments as overt means have been used to investigate all criminal offending investigated by the Council and one application was refused on the basis of R v Police 2006 and to await the outcome of the RIPA inspection.

4.3 Set out below is the number of prosecutions for each of the last 3 years which gives an indication of the number of investigations which led to convictions and which relied on overt means of obtaining the evidence.

Year	EHS	WYJS	CFT	Planning Service & Building control	Housing standard service	Liquor Lic. Service	Hackney Carriage & Private Hire Licensing Service	ASBO & YOT
2014/15	58	12	65	11	8	2	10	16
2015/16	46	8	17	7	5	0	4	9
2016/17								

4.4 **The Environmental Health Service (EHS).**

Members may be interested to know the type of offences the Council's EHS investigate. The services investigates offences of food safety, food hygiene, and fly tipping of controlled waste, prohibition of smoking in public places, littering and dog fouling amongst others. The offences arise under the Environmental Protection Act 1990, the Food Safety Act 1990, the Food Hygiene Regulations 2013, the Health Act 2006 and the Council's Dog control orders made under the Clean Neighbourhoods and Environment Act 2005.

4.5 **The Council's West Yorkshire Trading Standards Service (WYTSS)**

The WYJS investigates many consumer protection offences for example trade marks offences relating to counterfeit good, sale of cigarettes and alcohol to children, and weights and measures offences. These offences are all serious offences under the Consumer Protection Act 1998, the Trade Marks Act 1998, The Licensing Act 2003 and the Children's and Young Persons Act. The investigation of these offences could where necessary and proportionate be carried out covertly and be authorised under RIPA.

4.6 **The Council's Counter Fraud Team (Finance) (CFT)**

The CFT role in investigating benefit fraud along side the Department of Work and Pensions (DWP's) investigators under the Social Security Administration Act 1992 has recently changed and these matters are now prosecuted by the DWP's solicitors alone. The CFT continues to investigate serious criminal offences of internal fraud (e.g. social care direct payments) under the Fraud Act 2006; the Proceeds of Crime Act 2002 (money laundering) related mortgage fraud and fraud by abuse of position. All fraud offences are serious by definition and carry terms of imprisonment of six months or more and could use covert surveillance if necessary and proportionate and be authorised and approved under RIPA.The team also investigates less serious summary offences of misuse of blue badges.

4.7 **The Council's Planning and Building Control Service**.

This service investigate breaches of planning development control under the Town and Country Planning Act 1990 breaches of building regulations under the Building Regulations 2010, and listing building offences under the Town and Country Planning (Listed Buildings and conservation Areas) Act 1990. None of the offences investigated can be authorised as covert under RIPA as they carry penalties of less than six months in prison.

4.8 **The Council's licensing services (Liquor and Taxis)**

These services investigate criminal offences under the Licensing Act 2003 and the Local Government (Misc. Provisions) Act 1976. The taxi licensing service is continues to be closely involved with the Police in investigating and disrupting issues of Child sexual exploitation. The hackney carriage and private hire licensing service has in the past used covert means to investigate plying for hire but the offences do not carry penalties of more than six months in prison and thus cannot since November 2012 be authorised under RIPA.

4.9 **The Council's Housing Standards Service.**

This service investigates breach of standards of residential housing in the private sector and criminal offences arise under the Housing Act 2004. All the offences are summary offences which do not carry a sentence of six months or more in prison. This team has never found it necessary or proportionate to investigate the offences covertly.

4.10 **The Council's Anti-Social Behaviour Team (ASBT) and Youth offending team (YOT).**

The ASBT investigates matters of anti-social behaviour and seek injunctions to stop it under the Anti-Social Behaviour Crime and Policing Act 2014.

The Youth Offending team provided the supervision of young persons who have committed criminal offences. Those young people are under the age of 18 and will have been prosecuted by the Police for serious offences and then for example for breaches of supervision orders or Youth rehabilitation orders. Neither team has ever used covert surveillance for such investigations as it is not necessary or proportionate.

5. Year on Year Compliance with RIPA

5.1 Before officers consider deploying any of the 3 investigative techniques e.g. DS CHIS or DC officers must comply with RIPA or leave the Council open to criticism from the OSC and sanctions imposed by the Courts.

5.2 Compliance with RIPA and properly authorised and approved covert surveillance investigations give the Council an absolute defence under s 27 RIPA to a claim of damages for breach of the Human Rights Act through the use of covert surveillance i.e. breaching a person's right to privacy under the Human Rights Act 1998.

5.3 Compliance with RIPA by the granting of duly authorised and approved covert investigations avoid the exclusion of evidence before the Court/tribunal should a criminal prosecution or an employee disciplinary sanction follows the covert investigation.

5.4 The Council has the option to allow its authorised officers to be any director, head of service, service manager or equivalent.

5.5 However following a resolution of the Executive from the 1st September 2011 all authorisations are granted by either the Council's Chief Executive, or its City Solicitor (or in absence their nominated deputies) in consultation with the Leader of the Council. Each application for authorisation is also subject to legal advice from the Council's RIPA coordinator and monitoring officer. Prior to that time all Strategic Directors and their Assistant Directors were authorised officers.

5.6 Until the 1st November 2012 local authorities had the option to authorise covert investigation of less serious crime e.g. littering dog fouling and schools admissions. This power has now been removed by the ''serious offence test'' which states directed surveillance can only be used for offences which are subject to imprisonment of six months or more.

5.7 Consideration has been given by the Council's SRO and RIPA coordinator and Monitoring officer as to whether or not covert surveillance outside the authorisation and approval mechanism of RIPA be approved by the Council's policy and such a course of action for refused by C&AC in 2015.

5.8 **The Council's CCTV system and use of it for covert surveillance by the Police.**

a) The Council owns a substantial CCTV system which assists in the prevention and detection of crime within the City Centre.

b) From time to time the Council is asked to direct the use of its cameras specifically for the surveillance of criminal activities. This requires authorisation under RIPA and such authorisation is provided by the Police to the Council's CCTV manager Mr Philip Holmes.

c) The Council's CCTV system has been considered in inspections by the OSC. In October 2016 the OSC Assistant Surveillance Commissioner advised that the Council through its CCTV manager needed to make sure that those public authorities e.g. the Police and Department of Work and Pensions DWP who request to make use of the CCTV system to detect crime provide sufficient detail of authority to undertake covert surveillance of the suspected crime being investigated prior to the Councils system being used. It can be noted that in fact in 2014/15 2 refusals were made by the Council's CCTV manager. A West Yorkshire local authorities and Police protocol was reviewed and implemented in early 2017 to address this concern.

d) This arrangement continues to be managed by Mr. Holmes and over the last year the Council has permitted the use of the Council's CCTV system for covert surveillance on 18 occasions over 8 separate operations. Of those applications all came from the police. None were requested by the Council's investigative services or the DWP.

e) The table below shows comparative figures for the last 3 years.

Year	Police	DWP	Refusals	Accepted	Total Operations
2014/15	26	1	2	27	12
2015/16	22	1	0	23	8
2016/17	19	0	0	19	8

5.9 **The Council's warden service and the use of body cameras.**

a) Body worn cameras are deployed the Council as an overt tool for frontline uniformed Council Wardens. Any video recordings and images captured by the cameras are the property the Council and will be retained in accordance with this policy.
b) In accordance with Section 29 of the Data Protection Act 1998 the Council share any recordings with the Police to support ongoing Police investigations into offences committed against Council Wardens. The Council has a ''Retention Policy relating to body worn camera footage set out at Appendix 2 of this report.
c) The Council's warden service have been advised that if the body cameras were to be used in a covert way then authorisation and court approval should be carefully considered.

5.10 **The monitoring of social media websites for evidence of criminal activities**.

(a) It was noted at the last OSC inspection in 2013 that the WYTSS uses internet monitoring to obtain evidence of the sale of counterfeit goods. However the WYTSS only examines public page sites and uses information gained as a basis for investigation. The WYTSS does not have a ghost website or a covert Face book account. It does have an overt Face book account and information gleaned from it or from websites normally stimulates a warning letter being sent to the account holder. Any information requiring a deeper investigation would be reported to the Regional Trading Standards Service. WYTSS staff is aware of the pitfalls involved in the investigation of Social Network Sites (SNS) covertly and having entered pages through privacy controls.

(b) However all Council staff need to be aware that covert investigation on public social media websites and the creation of covert relationships with members of the public in their investigations would require approval under RIPA.

(c) The Council's RIPA coordinator and Monitoring officer and the Council's SRO have a concern as to whether there is a full appreciation by enforcement officers and their managers of the use of internet investigations and the approval required under RIPA. Thus specific training was provided In April 2015 by the west Yorkshire police and in September 2016 in house by RiCMO to deal with Internet investigation even though not obviously covert (entry through privacy controls) may in any event require a *directed surveillance* authorisation AND where covert relationships are formed a *CHIS* authorisation is granted then the *CHIS* will need to be managed in accordance with *RIPA* requirements, namely by a controller and a handler with a full record being maintained.

(d) Appendix 3 to this report sets out the policy a document which has been circulated by the Council RiCMO which was resolved to be adopted in June 2016.

6. The role of the Councils Senior Responsible Officer and the annual review and training programme.

6.1 The Council's Senior Responsible Officer (SRO) role is an internal auditing role with regard to the Council's departmental use and compliance with RIPA in accordance with the relevant regulations, codes of practice and guidance.

6.2 The SRO undertakes an audit of the Council's compliance with RIPA each year and a reference to that audit is referred to at APPENDIX 4 of this report.

6.3 The recommendations are to implement the OSC inspectors' recommendations and the Council's RIPA Coordinator and Monitoring Officer to continue to monitor comply with RIPA and continue annual training.

6.4 Annual training for authorising officers and investigators has been arranged.

7. FINANCIAL & RESOURCE APPRAISAL

7.1 There are no financial implications arising from a resolution adopting the recommendations of this report.

7.2 The training planned for 2017 is to be provided by an external provider.

8. RISK MANAGEMENT AND GOVERNANCE ISSUES

Recommendation 5 is intended to avoid risks of unauthorised covert surveillance by officers of the Council using internet investigation which authorisation would be unlawful.

9. EQUALITY & DIVERSITY

There are no equality impact or diversity implications as a result of a resolution adopting the recommendations of this report

10. SUSTAINABILITY IMPLICATIONS

There are no sustainability implications as a result of a resolution adopting the recommendations of this report.

11. GREENHOUSE GAS EMISSIONS IMPACTS

There are no greenhouse gas emission impacts as a result of a resolution adopting the recommendations of this report

12. COMMUNITY SAFETY IMPLICATIONS

There is no community safety implications as a result of a resolution adopting the recommendations of this report as investigation into crime in the Councils district will continue by the police. The Councils Enforcement teams will continuer to undertake investigations of criminal offences overtly.

13. TRADE UNION

There are no trade union implications as a result of a resolution adopting the recommendations of this report

14. WARD IMPLICATIONS

There are no ward implications as a result of a resolution adopting the recommendations of this report

15. <u>RECOMMENDATIONS</u>

15.1.1 The duties placed on the Council under the Human Rights Act 1998 are considered in the context of this report and the Council's continued compliance with RIPA is noted.

15.1.2 The implementation of the OSC recommendations following the inspection in October 2016 is completed alongside those outstanding from the 2013 recommendations (see paragraphs 3.3 and 3.4 of the report).

15.1.3 The 2017/18 programme of training of Officers (in order to update SD's to raise awareness) and enforcement officers under RIPA is noted.

15.1.4 Reports of use or none use of covert surveillance techniques be presented to the Governance and Audit Committee quarterly.

16. Background documents

16.1.1 The Council's RIPA guidance document was last updated January 2017 (approx 120 pages) and is available on request from the author of the report and has been circulated to all enforcement managers.

16.1.2 The December 2015 updated RIPA Codes of Practice and Guidance on RIPA from the OSC.

17. Not for publication documents

17.1 None.

APPENDIX 1 the Council's policy on RIPA (implemented 2002).

Policy statement

1. **Purpose** – The Council's officers in the course of investigating frauds, breaches of legislation or regulation and in the interest of the safety and well being of the district may be required to undertake covert monitoring operations to gather evidence to present to a court. In doing so those Officers must comply with the relevant legislation i.e. RIPA and the associated regulations and codes of practice. Evidence collected without complying with the statutory procedures may become inadmissible before the Courts and prejudice the outcome of an investigation.
2. **Scope** – The policy covers the use of covert CCTV, monitoring equipment such as audio recording, cameras, video cameras, binoculars and covert human intelligence sources (CHIS). RIPA also covers the monitoring of Internet use, telephone use, or postal use where the individual whose actions are being monitored is unaware of the operation. The Council's policy does not contemplate the monitoring of Internet use, telephone use or postal use other than in exceptional circumstances as this is unlikely to be unnecessary and disproportionate in most if not all local authority criminal investigations.
3. **Exclusions** – City centre CCTV operating within defined boundaries and brought to the attention of the public by the use of signs is not covered by this policy.
4. **The procedure** – when a Council officer considers that covert operations are the only method of collecting the evidence required s/he should obtain authorisation and court approval for such activity in advance and follow the guidance in the Council's RIPA guidance document as issued by the Council's RIPA coordinator and monitoring officer. The Council's RIPA coordinator is available to advise on procedure and maintains a central register of all authorisations.
5. **Review of the policy** - the policy and guidance document is reviewed annually by the Corporate Governance and Audits Committee through changes where required by the Council's RIPA Coordinator.

6. **Guiding Principles**

6.1 Surveillance is an intrusion into the privacy of the citizen. The Council's officers will not undertake surveillance unless it is necessary and proportionate to the alleged offence and properly authorised and approved. Where there is an alternative legal means of obtaining the information that is less intrusive on the rights of the citizen, the Council will always take that alternative course rather than undertake surveillance.

6.2 Surveillance by covert human intelligence source (CHIS) will not be authorised by the Council other than in exceptional cases due to the adverse risk to the health and safety of the officers and such will usually only be authorised when working alongside the police and after a risk assessment has been approved by the City solicitor.

6.3 Covert surveillance will be conducted within the constraints of the authorisation. It will cease when the evidence sought has been obtained or when it becomes clear that the evidence is not going to be obtained by further surveillance. At that point the authorisation should be cancelled.

6.4 In every instance where surveillance is authorised the officer who conducts surveillance will consider and make plans to reduce the level of collateral intrusion into the privacy of third

parties.

6.5 All outstanding surveillance authorisations should be reviewed at least monthly and cancelled where there is no further need for surveillance.

6.6 All officers involved in applying for, authorising or undertaking surveillance will understand the legal requirements set out in RIPA and the codes of practice. They will personally take responsibility for ensuring the propriety of their involvement.

6.7 All authorisations, notebooks, surveillance logs and other ancillary documentation that relates to surveillance will be maintained to the required standards and retained for **three years**. All documentation will be volunteered for any management or regulatory inspection on demand.

6.8 Any failure of any part of the process will be brought to the attention of the investigation manager. S/he will consult the Council's RIPA coordinator to determine what action should be taken.

6.9 Wilful disregard of any part of RIPA, codes of practice or of internal procedures shall be a breach of discipline and subject to the Council's disciplinary code.

6.10 **Surveillance equipment.**

(i) The Council have a considerable amount of technical equipment which can carry out covert surveillance of operations e.g. Cameras, video cameras , binoculars, zoom lenses CCTV and noise tape recording equipment.

(ii) Bearing in mind that such equipment can be used by officers without supervision once authorisation has been granted continued monitoring and thus a record of the use of such equipment requires to be maintained i.e. its return to storage immediately once the covert surveillance has been undertaken.

(iii) Schedules of equipment are kept and updated by authorized officers for each Council department which undertakes surveillance either covert or otherwise. This is reviewed annually by the Council's RIPA coordinator and Monitoring Officer.

(iv) In order to effectively monitor the use of the equipment each separate piece of equipment is listed with it reference/serial number and its whereabouts.

(v) The responsibility to monitor the day to day use of such equipment by Council Enforcement officers is primarily that of each and every authorised officer (AO's) of the relevant Council Department. See schedule of AO's below

(vi) Included in this guidance are those departments that use surveillance equipment but such surveillance is deemed to be an exception to RIPA2000 e.g. Environmental services (noise monitoring where the person investigated is on written notice the noise is to be monitored and parks and landscapes who use of publicised motor bike mounted video camera for surveillance over general hot spots for crime rather than individual known suspects.

6.11 Wilful disregard of any part of RIPA, codes of practice or of internal procedures shall be a breach of discipline and subject to the Council's disciplinary codes.

7. Serious crime restrictions and magistrates court approval (1st November 2012)

a) It is noted from the 1st November 2012 due to statutory regulation all authorisations under RIPA 2000 for Directed Surveillance and Communications Data may only be granted in respect of ''serious crime'' as defined i.e. carrying a penalty of 6 months or more imprisonment.

b) Also from the 1st November 2012 all authorisations granted by the Council's authorised and designated officers of which are the Council's Chief Executive and the Council's City Solicitor (in consultation with the Leader of the Council) do not take effect until they have been approved by a magistrates upon application by the Council.

c) The procedure to be followed is similar to applying for a warrant to enter premises under relevant statutory powers.

d) The application to the Magistrates Court will be made in person usually by a Council solicitor advocate together with the applicant for the authorisation.

e) The existing authorisation for which approval is required will be submitted to the court in writing and with the approval application form completed under cover of a letter before the application for approval is heard formally before the court.

f) This statutory restriction was effectively part of the Council's existing policy in the context of making use of RIPA.

g) The policy already acknowledges RIPA is not to be used for none serious crime e.g. dog fouling , schools admissions and littering offences as has been so severely criticised in the press and by the court

APPENDIX 2

Retention Policy relating to body worn camera footage

Body worn cameras are deployed by Bradford Council as an overt tool for frontline uniformed Council Wardens. Any video recordings and images captured by the cameras are the property of Bradford Council and will be retained in accordance with this policy.
In accordance with Section 29 of the Data Protection Act 1998 Bradford Council will share any recordings with the Police to support ongoing Police investigations into offences committed against Council Wardens.

All footage shall be reviewed and deleted within 24 hours of recording. The only exception to this is where the footage is being used as evidence in an ongoing Police investigation. Accordingly, any footage forming part of an ongoing Police investigation would only be disclosed by the Police as part of their investigation. Bradford Council would not be able to provide a copy on these occasions.

Any person who has been recorded on a body camera can make a request for a copy of the footage provided the request has been made within 24 hours of the recording. Proof of identity must be verified for such requests.

Requests for footage that is not in the public arena and contains recording of other individuals will be sent to a specialist contractor so that the identities of those individuals captured on the footage can be disguised prior to despatch.

Subject Access Rights

In accordance with the Data Protection Act 1998 if a recording of a member of the public has been made on a body camera that person is entitled to a copy of the recording provided the request has been made within 24 hours of the recording. The exception to this is where the recording is part of an on-going Police investigation.

In accordance with the Retention Policy
Delete as appropriate:
* As the footage requested occurred on (input date) this footage has been deleted and no longer exists.
* The footage forms part of an ongoing Police investigation and the Council will not be providing copies.
* The footage exists and a copy will be provided once it has proof of the person's identity so that the Council can satisfactorily establish the subject access rights. The person will need to provide a copy of any one of the following documents preferably by email to (name.name@bradford.gov.uk) or by post to: (input full office address)

- Your Council Tax reference number
- Copy of current passport
- Copy of a current benefits payment book
- Copy of current driving licence

Any copy of footage provided can be collected personally upon production of proof of identity, or, delivered securely to an address nominated by the subject.

Guidance documents for use of Internet Investigations by local authority investigators

The Use of Social Networks in Investigations

1. Use of this Guidance

This document provides guidance to Council officers who use "open source" social networks to gather information about individuals or groups of individuals in support of any investigation carried out on behalf of the Council, including criminal, civil, child protection and employment investigations. "Open source" means that the information available is not protected by privacy settings and is openly available to anyone that wishes to view it.
This guidance does not facilitate the viewing or gathering of information from sources or profiles that are not "open source" and are protected by privacy settings. For example, a Face book profile where a friend request must be accepted before a profile can be viewed would not be an "open source" profile. Access to such information and the gathering of such information requires particular consideration under the Data Protection Act (DPA) 1998, Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000. If such activity is proposed legal advice should always be sought in advance. The guidance supplements the Council's Data Protection Policy which supports the delivery of the Information Governance Framework. The guidance should be read alongside the Council's RIPA Policy Guidance and Procedure.

2. Use of "Open Source" Social Networks

"Open source" social networks have become a large accessible source of information about individuals. The information placed on these networks has the potential to be accessed, acquired, used and retained by council officers on behalf of the Council, in particular by investigators seeking evidence to support criminal and civil investigations, defend actions brought against the Council, assist in child protection matters or support employee disciplinary matters.
In his latest annual report the Chief Surveillance Commissioner has stated his view that just because such material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA.
Whilst the viewing only of publicly available information, without gathering, storing or processing material or establishing a relationship with the individual is unlikely to engage an individual's right to privacy under the European Convention on Human Rights , where activities involve officers creating a record of personal data or private information, this activity must be justified with reference to the DPA and HRA to ensure that the rights of the individual have been respected and to ensure that ensuing proceedings are based upon admissible evidence.

3. RIPA, Covert Human Intelligence Sources & Directed Surveillance

3.1 Covert Human Intelligence Source (CHIS)

There may be circumstances where activity on social networking sites amounts to the use

of a CHIS which would require an authorisation under RIPA. The term CHIS is used to describe people who are more commonly known as informants. The use or conduct of CHIS would include work by officers working "undercover" whereby a covert relationship is established with another person. Such activity may arise if investigators are seeking to form covert relationships on social networking sites to circumvent privacy settings that have been put in place.
Many sources volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council. For example a member of the public volunteering information about something they have viewed on a social network, where a relationship will not have been established or maintained for a covert purpose, will not amount to CHIS activity. This information may be processed by the Council in accordance with the DPA.
Further information about the use of CHIS can be found in the Council's RIPA Policy, Guidance and Procedure. If officers believe that proposed use of social networks may involve the use of CHIS, legal advice should be sought and any CHIS activity must be authorised in accordance with the Council's RIPA policy.

3.2 Directed Surveillance

The Chief Surveillance Commissioner has expressed the view that the repeated viewing of open source sites for the purpose of intelligence gathering and data collation or a single trawl through large amounts of data ("data mining") could amount to activity for which a RIPA authorisation for Directed Surveillance should be sought, where the serious crime threshold is met.
Where private information is being gathered by officers from social networks to support a criminal investigation for an offence that attracts a maximum sentence of 6 months or more and the proposed use of the social network meets the definition of Directed Surveillance, authorisation must be sought in accordance with the Council's RIPA policy. Officers are advised to seek legal advice on such proposed activity.
Where information is gathered by officers from open source sites that would require a RIPA Authorisation for Direction Surveillance if it were not for the serious crime threshold then a Human Rights Audit should be completed in accordance with the Council's RIPA Policy, Guidance and Procedure.
Where individuals volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council, this activity will not amount to Directed Surveillance and the information may be processed by the council in accordance with the DPA.

3.3 Surveillance of Employees

Covert surveillance of an employee as part of a disciplinary process does not amount to Directed Surveillance for the purposes of RIPA as this is an "ordinary function" of the council rather than a "specific public function".
Where online covert surveillance involves employees then the Information Commissioner's Office's (ICO) Employment Practices Code (part 3) will apply. This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion. Whilst the code is not law, it will be taken into account by the ICO and the courts when deciding whether the DPA has been complied with (see section 3 below).

Where individuals volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council, this activity will not amount to covert surveillance and the information may be processed by the council in accordance with DPA.

4. Data Protection Act 1998

The provisions of the DPA apply to all personal data processed by the Council, including personal data acquired from open source social network sites. Personal data must only be processed in accordance with the DPA and the Council's DP policy.
All personal data must be processed fairly and lawfully and the processing of personal and sensitive personal data must be justified fewer than one or more of the fair processing conditions set out in Schedules 2 and 3 of the DPA.
The Council strives to adopt the least intrusive approach to the delivery of council services and any processing must be necessary and proportionate in order to be justified less than one of the fair processing conditions. "Necessary" means more than simply convenient or desirable for the Council, where processing corresponds to a "pressing social need". "Proportionate" means that the Council needs to try and strike a fair balance between the rights of the data subjects, and the legitimate aims of the Council. This means the data collected to support investigations must not be excessive and must take account of the particular circumstances of the data subject.
Officers must also consider whether the use of open source social networks as part of an investigation is likely to result in collateral intrusion and the personal data of uninvolved third parties being processed by the Council. The processing of third party data must also be justified under the DPA with reference to the fair processing conditions.
If officers are unsure as to whether processing is justified under the DPA, advice can be sought from the Directorate Data Practitioner, the Corporate Information Governance Team or Legal Services.

5. Human Rights Act 1998

Article 8 of the European Convention on Human Rights (ECHR) which was brought into force by the HRA provides that an individual's rights to family and private life may only be interfered with where the interference is in accordance with the law and necessary for one of a number of legitimate purposes including public safety, the prevention of crime or disorder, the protection of health and morals, or the protection of the rights and freedoms of others. In order to meet the requirement of necessity the interference must be proportionate to the legitimate purpose.
The case law recognises that the concept of "private life" is wide ranging. The test to be applied in determining whether Article 8 rights are engaged is whether there is a "reasonable expectation of privacy". This is a broad question that must take into account all the circumstances of the case. The creation of a permanent record from information currently in the public domain or the systematic retention of information may engage an individual's Article 8 rights. The Supreme Court has now confirmed that the state's systematic collection and storage in retrievable form even of "public" information about an individual is an interference with private life. Therefore the requirements of lawfulness,

necessity and proportionality should be considered by officers whenever information about individuals from social networks is acquired, used, or retained.
Given the need to consider issues of lawfulness, necessity and proportionality in order to justify the processing of personal data under the DPA, where the processing of personal data from open source social networks is justified under the DPA, any interference with the individual's right to privacy under Article 8 through the processing of that data will also be justified.
In order to comply with Article 8 consideration must also be given to any collateral intrusion that might occur and result in private information being obtained about uninvolved third parties, whether this intrusion is lawful, necessary and proportionate and how it can be avoided, minimised or mitigated.

6. Use of Corporate Accounts

Investigations using social networks should only be conducted using Corporate Accounts created for the purpose of carrying out such investigations. Accounts must be approved by your line manager and by your service area digital champion. You can find out who your digital champion is in the related documents section and more about the process of applying for an account in the 'general' toolkit guidance.

7. Case Study Examples

Case Study No.1

An officer in Children's' Services wish to search Facebook to try and locate a child who is missing from care; the search is only carried out for the purpose of trying to locate the child when other investigative methods have failed.
Yes –Children's Services have a statutory duty to safeguard and promote the welfare of children, providing the use made of Facebook and any information retained by Children's Service is necessary and proportionate in the circumstances. This use of social Facebook in these circumstances is likely to be lawful however care should be taken not to gather information on third parties unless this is justified in the circumstances.

Case Study No. 2

Environment and Housing receive reports from a neighbour that a tenant has abandoned their property. The housing officer believes it would be quicker to search Facebook to find evidence of the tenant living elsewhere than it would to visit the property and make enquiries with the neighbours and family members.

No – the use of Facebook and subsequent gathering of evidence would not be necessary or proportionate in these circumstances. Online investigations should not replace traditional less intrusive investigative methods simply because it is convenient to do so. This use of Facebook information is likely to breach both the DPA and Article 8 ECHR.

Case Study No.3

A manager has suspicions that members of the team are abusing the sickness absence policy and routinely carries out checks on Facebook to monitor the activities of staff that

are off work on sick leave, gathering evidence that they believe demonstrates abuse of the policy.
No – routinely using Facebook to monitor staff absences and gather information about staff members would not be necessary or proportionate and is likely to breach both the DPA and Article 8 ECHR.

Case Study No.4

Enforcement Officers believe that an individual suspected of fly-tipping is advertising his services to friends through Facebook. Privacy settings prevent the Enforcement Officers from accessing his Facebook profile sand they want to create a fake profile to befriend him to gain access to his posts.
No - using Facebook to establish a relationship with somebody to covertly gather information about them would be the use of Covert Human Intelligence source (CHIS) which requires authorisation under RIPA. This use of Facebook is likely to breach Article 8 ECHR

Case Study No 5.

Council officers investigating a tenancy fraud want to monitor a tenant's Facebook page constantly for a week to see if the tenant posts any information that could be used to support the investigation. They intend to take screen shots of posts as they are made to preserve the evidence in case the tenant later deletes the posts.
No - the monitoring in real time of a person's Facebook profile to try and obtain evidence to support a prosecution is likely to amount to Directed Surveillance and require authorisation under RIPA. This use of Facebook is likely to breach Article 8 ECHR.

Case Study No.6

A member of the public makes a complaint that an employee of Leeds City Council has been stealing council equipment and selling it on Facebook, they voluntarily provide a screen shot of the employees Facebook page showing council equipment for sale.
Yes – a member of public volunteering information that is accessible to them does not amount to CHIS activity and use of the evidence provided would be necessary in order for the council to investigate and address the allegations made. However the complainant should not be asked to continue to covertly gather information on behalf of the council as this would be intrusive and likely to breach Article 8 ECHR. The information should be retained is accordance with the council's retention rules.

31st May 2017 City of Bradford M.D.C (the Council)

Internal audit undertaken by the Council's Senior Responsible Officer Stuart McKinnon- Evans (SRO & CFO) with Richard Winter RIPA coordinator and monitoring officer (RiCMO) (Period 1st April 2016- 31st March 2017) in respect of the Councils use of covert surveillance techniques e.g. directed surveillance and covert human intelligence sources.

Audit check	Yes/No/Not applicable
SRO and Authorised officers and training	
a) The nominated authorised officer for obtaining 'private information' covertly. b) The nominated deputy authorised officer for the obtaining of 'private information' covertly. c) The nominated authorised officer for obtaining 'confidential information' covertly d) The deputy nominated authorised officer for obtaining 'confidential information' covertly e) The Councils RIPA coordinator and monitoring officer (RiCMO) f) Senior responsible Officer	a) City Solicitor – PA yes Sept 2016 b) Assistant City solicitor.- MB yes Nov. 2016 c) The Chief Executive (CEX) (Head of the paid service) KE yes Aug 2016.2016 d) The nominated Strategic Director authorised by the CEX to deputise in her/his absence. (SH etc) NO e) RW solicitor (with expertise of criminal investigations and prosecutions) yes f) Strategic Director Corporate Services (SMcE) yes August 2016
Necessity and proportionality	
(i) Where the Council has authorised the use of covert surveillance are those authorisations necessary and proportionate?	Not applicable- all investigations have been undertaken overtly without the use of covert surveillance.
Approval by a Justice of the Peace	
(ii) Were all authorisations approved by a justice of the Peace? If not why not and what can be learnt from this?	Not applicable- all investigations have been undertaken overtly without the use of covert surveillance.
Refusal of authorisation/approval	
(iii) Have any applications for authorisation/approval been refused/put on hold? If so why?	There have been no covert surveillance either directed surveillance or CHIS authorised by the Council since 2013. However there has been one application for directed covert surveillance in 2015/16. The application was made towards the end of 2015 carrying RIPA unique Reference number URN CFT No 1of 2015/16. This application was refused by the Council's Interim City Solicitor and Deputy Assistant City Solicitor in consultation with the Councils RiCMO. The application related to an investigation of a complaint from management at the Alhambra theatre in Bradford regarding the theft of coins from the machines used to make opera glasses available to the public at a small fee. The glasses are available at theatre goers'

Audit check	Yes/No/Not applicable
	seats whilst watching performances. It was believed by the senior investigator and manager of the Corporate Fraud Team that the thefts were likely to have been committed by cleaners. It was proposed to use hidden cameras to detect the person(s) who committed offences under the Theft Act 1968 and if detected report the matter to the police for prosecution. However given the case of R v Police 2004 and the refusal of a similar application in June 2013 by the magistrates court it was concluded that the approval should not be given. The case of R v Police 2004 states that RIPA does not apply to investigation of crime which do not form part of the ''core business'' of the investigating authority. In R v The Police the appellant a police officer had been investigated by the police for breaches of the disciplinary code. He had been investigated covertly. His lawyers attempted at his disciplinary hearing to have the evidence excluded. The appeal court held as the authorisation investigation was not the ‘’ core business’’ of the police a RIPA was not required and thus the evidence obtained without authorisation was admissible. Given that alleged offences of theft under the Theft Act 1968 are the core business of the police rather than the Council the Alhambra application was refused. Legal advice was provided to the investigating department i.e. Corporate Fraud Team by the Councils Interim City Solicitor and RiCMO that the complaint should be referred to the police for investigation. I have been referred by way of reminder of the refusal by the magistrate’s court to approve the 2013/14 application which related to the theft of large scale council catering equipment by a Council employee and later sale on EBay. The magistrates suggested the investigation be passed to the police. However at the inspection in October 2016 His Honour Judge Norman Jones QC advised this authorisation could have been granted for the reasons as set out in the report i.e. that the matter was to be reported to the police were evidence detected by the use of covert CCTV. A second application for the deployment of covert CCTV was effectively refused as overt means were found i.e. by signposting the use of the CCTV at the fly tipping location in question.

Audit check	Yes/No/Not applicable
Central Register of authorisations	
(iv) Is the management and upkeep of the Council's central record and register of authorisations satisfactory and in accordance with current legislation, Home Office and OSC guidance and recommendations arising from past inspections?	Yes I believe so. The self authorisation reference as advised at the October 2016 inspection to be inserted into the central register has been actioned. I have been referred to the 4 parts of the register which I believe all show a NIL return. The register is made up of separate parts for the Council's services e.g. Environmental Health Service. Corporate Fraud Team, The Planning Service, The Licensing services (taxis and liquor licensing) and the Housing standards service. The WY Trading standards service keeps its own central register and I mainframe this is up-to-date.
The quality of the completed applications and authorisations	
(v) Is the quality of the completed application and authorisations, reviews, renewals and cancellations documentation satisfactory?	Not applicable- all investigations have been undertaken overtly without the use of covert surveillance NB I am informed by RiCMO the 3 applications refused was of an acceptable quality (see below)
Review of the continuation and implementation of the Conclusions and Recommendations of the OSC Inspection October 2016.	
Deputy Surveillance Commissioner HH Judge Norman Jones QC October 2016 *Recommendations* 1. Amend the Central Record of Authorizations. (Paragraph 9). 2. Raise *RIPA* awareness throughout the Council. (Paragraph 19). 3. Amend the *RIPA policy, guidance and procedures document. (Paragraph 26)* 4. Ensure regular reports are given to Elected Members	Noted 1. Done by RiCMO 2. RiCMO to produce a short advice note to be distributed by SRO to all SD's and AD, s and SRO to raise awareness by cascading the information at CMT. 3. Done by RiCMO 4. RiCMO to present 3 short reports in Jan, April, July and October each year.

Audit check	Yes/No/Not applicable
which include information relating to *RIPA* activity or inactivity. (Paragraph 27). 5. Reinstate the equipment record and make it a subject of the internal *R/PA* audit. (Paragraph28). 6. Amend the WYTSS policy and procedures document. (Paragraph 40).	5. RiCMO to action in consultation with senior Managers of EHS, Corporate Fraud Team and Waste Enforcement. 6. RiCMO to action in consultation with David Lodge Head of WYTSS.
The Annual review of the Council's Policy and guidance document	
(vi) Is the Council's stated policy and guidance document for officers up to date bearing in mind current OSC guidance (last updated December 2014) Home office Codes of Practice (Last revised December 2014) and current legislation? (vii) Is the Councils current in house training material up to date?	Yes last updated January 2016 by RiCMO Next update Jan 2017 unless legislative changes are made before then. I have had sight of the updated document. Yes last updated September 2016 by the Councils RiCMO
Annual training programme	
(viii) Has the required annual training of all relevant officers been completed and a next years programme arranged?	I. The CEX has been in post since September 2015 and was trained in August 2016 with SRO. Further training of the Councils Strategic Directors (namely Parveen Akhtar was undertaken in September 2016. Strategic Directors Steve Hartley et al have yet to be trained. II Relevant 4th tier managers were trained on CHIS and internet investigation by the West Yorkshire Police in April and June 2015 and internally by Richard Winter in September 2016 III. Officers of the WYTSS attended the WYP training in April and June 2015 and hold counsels advice on this issue. I am satisfied as to the level of training provided in 2015 and 2016 by the WYP and RiCMO. IV. I am aware of the training recommendations made by the OSC in general terms i.e. annually. V. As there have been no authorisations granted in the last 2 years and I conclude the training of SD's and AD's can be by memorandum. VI. Training of enforcement officers and 4th tier

Audit check	Yes/No/Not applicable
	managers should be undertaken by webinars or by an external provider namely Ibrahim Hasan of Act Now training or some other suitable trainer.
(viii) CTTV use and authorised under RIPA for covert surveillance by the police and DWP.(obtained from Councils CCTV manager)	(viii) Evidence of RIPA authorisations granted by the external investigative agencies e.g. the WYP and the DWP (see figures to be inserted into committee report).
Conclusions & Recommendations by SRO	1. Arrange 2017 training as above. 2. Continue to make sure the Council's officers comply with RIPA and raise awareness as set out above. 3. Continue disapproval of the use of covert surveillance when not authorised and approved under RIPA. 4. RiCMO and SRO to raise awareness as stated above.

Prepared by Richard Winter RiCMO

Dated 31st May 2017

Signed by Stuart McKinnon Evans SRO

Dated 31st May 2017

G:\Legal Services\Property Commercial & Development Law\Richard Winter (RJW) PCD\Local Government advice files\RIPA2000 coordination\Senior Responsible officer\Finalinternalaudi310517rw.doc

APPENDIX 5 Glossary of terms and abbreviations (in the order they appear in the report)

Abbreviation	title/term	Background/definition
RIPA 2000	Regulation of Investigatory Powers Act	Regulates the use of covert surveillance and data communication in respect of private persons.
SRO	Senior Responsible officer	Required to take an overview of the Councils use of covert surveillance and compliance with RIPA
CCTV	Close circuit television	Used for safety and security purposes within Council buildings and the city centre
CS	Covert surveillance	Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.
DS	Directed surveillance	Surveillance which is covert, but not intrusive, and undertaken: a) for the purpose of a specific investigation or operation; b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is the target of the investigation or operation); and c) In a planned manner and not by way of an immediate response whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out.
CHIS	Covert human intelligence source	A person is a CHIS if: (a) s/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) s/he covertly uses such a relationship to obtain information or to provide access to any information to another person; or (c) S/he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.
IS	Intrusive surveillance	**Intrusive surveillance is defined as covert surveillance that:** a) is carried out in relation to anything taking

		place on any residential premises or in any private vehicle; and b) Involves the presence of any individual on the premises or in the vehicle or is carried out by means of a surveillance device. **If the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device consistently provides information of the same quality and detail as could be expected to be obtained from a device actually present on the premises or in the vehicle.**
	Private information	Includes any information relating to a person's private or family life. Private life also includes activities of a professional or business nature (Amann v Switzerland (2000) 30 ECHR 843). "Person" also includes any organisation and any association or combination of persons.
	Confidential material	*Includes:* ▪ matters subject to legal privilege; ▪ confidential personal information; ▪ Confidential journalistic material.
HRA 1998	Human Rights Act	Enacts ECHR into English Law i.e. absolute and conditional human rights
ECHR 1950	European Convention of Human Rights	Sets out absolute and conditional Human Rights across Europe
OSC	Office of the surveillance commissioner	Appointed by the government to oversee the police and other public bodies use of covert surveillance techniques.
OICC	Office of the Interception of Communications commissioner	Appointed by the government to oversee the police and other public bodies interception of data communications
NAFN	National antifraud Network	Joint local authority network for dealing with fraud of which the Council is a member
RiCMO	RIPA Coordinator and Monitoring Officer	Lead Officer on RIPA - Advises enforcement managers and officers of the RIPA process and procedure. Annually reviews and updates all relevant Policy and Guidance material and reports to CGAC
SNS	Social network sites	E.g. Facebook and Twitter