Report No: G64/19

Eden District Council

Executive

8 October 2019

Regulation of Investigatory Powers Act - Annual Update and Review of Corporate Policy and Guidelines

Portfolio:	Resources
Report from:	Director of Corporate Services
Wards:	All Wards
OPEN PUBLIC ITEM	

1 Purpose

1.1 To enable consideration to be given to an update on the use of the Regulation of Investigatory Powers Act 2000 ("RIPA") by Council officers and a revision of the corporate policy and guidelines relating to RIPA.

2 Recommendation

It is recommended that:

1. it be noted that there have been:
   (a) no authorisations sought or granted by the Council under the Regulation of Investigatory Powers Act 2000 between 1 May 2018 and 31 April 2019; and
   (b) no non-statutory authorisations for covert surveillance (as referred to in paragraph 3.8 of this report) sought or granted by the Council between 1 May 2018 and 31 April 2019.
2. the revised Policy and guidelines which are attached to this report as Appendix 2 be adopted; and
3. the recommendations from the Inspection of the Investigatory Powers Commissioners Office as set out in paragraph 3.4 (below) be implemented; and
4. the observations from the Inspection of the Investigatory Powers Commissioners Office as set out in paragraph 3.5 (below) designed to reflect best practice, be implemented.

3 Report Details

3.1 The Investigatory Powers Commissioners Office (`the Commissioner') has oversight of the exercise of powers under the RIPA framework.

3.2 On 27 March 2019, the Commissioner conducted an inspection of the Council's arrangements under the RIPA framework and the Investigatory Powers Act 2016. The Council received the report from the Commissioner on in May 2019. A copy of the inspection report is enclosed as Appendix 1 to this report.

3.3 The investigation concluded that the Council had made good progress since the previous inspection and noted that although RIPA powers had not been exercised in the previous three years, there was a need to ensure that the arrangements for exercising such powers was efficient and robust.

3.4 The report made four recommendations as follows:

- The provision of a EXCEL based central register of authorisations;
- Drafting amendments to the policy to improve clarity;
- The provision of RIPA training for appropriate staff from an external provider; and
- The keeping of a central register of RIPA related training

3.5 The report made four observations designed to reflect best practice:-

- In respect of Direct Surveillance, the Council should consider the use of practice/mock authorisations on a periodic basis to test the integrity of the authorisation process
- In respect of Direct Surveillance, the Council could produce edited versions of Home Office standard RIPA forms to make them more relevant (by removing/amending sections relating to urgent oral provisions)
- With regards to Direct Surveillance (Noise Monitoring) the Council should carefully evaluate the capabilities of new technology or practice, which may result in the capture of private information through covert surveillance. This arises from an impact assessment that is required under Data Protection legislation.
- On the issue of Direct Involvement, the Council should consider no longer designating the RIPA Co-ordinating Officer as Authorising Officer.

3.6 Taken together, the above would ensure that the regulatory framework for RIPA that is operated by the Council is lawful, efficient, robust and in line with best practice, and the recommendation in section 2 of this report, is made on this basis. The Director of Corporate Services is currently in the process of arranging training for appropriate officers

3.7 Having regard to the Commissioner's report, a suggested revision to the Council's Policy and guidelines relating to RIPA is enclosed as Appendix 2 to this report.

4 Policy Framework

4.1 The Council has four corporate priorities which are:

- Decent Homes for All;
- Strong Economy, Rich Environment;
- Thriving Communities; and
- Quality Council.

4.2 The proposals within this report are relevant to the Quality Council corporate priority

5 Consultation

5.1 Not Applicable.

6 Implications

6.1 Financial and Resources

6.1.1 Any decision to reduce or increase resources or alternatively increase income must be made within the context of the Council's stated priorities, as set out in its Council Plan 2015-19 as agreed at Council on 17 September 2015.

6.1.2 The proposals within this report can be implemented within existing budgets.

6.2 Legal

6.2.1 The legal implications are contained in the body of the report and the policy and guidelines.

6.3 Human Resources

6.3.1 There are no specific implications.

6.4 Statutory Considerations

Consideration:	**Details of any implications and proposed measures to address:**
Equality and Diversity	The policy will have to be applied taking account of all relevant circumstances including any equality implications.
Health, Social Environmental and Economic Impact	The policy will have to be applied taking account of all relevant circumstances including any social and environmental issues.
Crime and Disorder	The policy relates to the investigation of relevant crimes and is designed to enable the lawful investigation of crimes for which the Council is the prosecuting authority.
Children and Safeguarding	The policy will have to be applied taking account of all relevant circumstances including any children / safeguarding issues.

6.5 Risk Management

Risk	**Consequence**	**Controls Required**
Risk to conduct of investigation and proceedings.	Adverse effects or comments in proceedings or a withdrawal of action or proceedings being compromised or adverse in monitoring the policy.	A thorough understanding of the policy and guidelines through adequate and appropriate training.

That the authority is hampered by the inability to use surveillance for offences or behaviour for which penalty is below the thresholds which would enable use of a RIPA authorisation.	Inability to investigate offences or anti-social behaviour or misconduct.	Policy allows the use of Non-RIPA Authorisations in such circumstances.

7 Other Options Considered

7.1 No other options have been considered, as the update on the use of RIPA is factual and the revisions suggested are non-substantive and either factual or minor textual changes.

8 Reasons for the Decision/Recommendation

8.1 To enable consideration to be given to an annual update and revised policy.

Tracking Information

Governance Check	**Date Considered**
Chief Finance Officer (or Deputy)	29 September 2019
Monitoring Officer (or Deputy)	18 September 2019
Relevant Director	20 September 2019

Background Papers:

Appendices: Appendix 1 – Report of the Investigatory Powers Commissioner's Office upon an inspection of Eden District Council

Appendix 2 – Draft revision to the Regulation of Investigatory Powers Act 2000, Corporate Guidelines and Policy (showing proposed revisions in coloured type).

Contact Officer: Matthew Neal, Director of Corporate Services

APPENDIX 1

IPCO
Investigatory Powers Commissioner's Office

Inspection Report – Eden District Council
Inspection report

Contents

1 Introduction

1.1 This inspection has been conducted to assess Eden District Council's (EDC) level of compliance with the Regulation of Investigatory Powers Act (RIPA) 2000, the Investigatory Powers Act (IPA) 2016 and all associated Codes of Practice in respect of the Council's use of directed surveillance, covert human intelligence sources (CHIS) and requests for communications data (CD).

1.2 Eden is a non-metropolitan district with a population of approximately 52,500. It is part of the county of Cumbria and is a second-tier authority. EDC is named after the Eden river that runs through the district and is based in the pleasant town of Penrith. It is ranked 319th by population of the 326 local authority districts of England yet covers an extensive, sparsely populated, rural hinterland of 2156 km^2 making it the least densely populated district in England. The council presently employs approximately 120 staff, making it one of the smallest local authorities.

1.3 The council is headed by a Chief Executive and has recently (February 2019) restructured to have 2 Directors: a Director of Corporate Services (Mr Matthew Neal) and a Director of People and Places. Mr Neal is the RIPA Monitoring Officer and is supported by numerous Assistant Directors including the Assistant Director of Legal Services who is also the RIPA Co-ordinating officer, Monitoring Officer, Data Protection Officer, and head of the council's legal team. She will be replaced on maternity leave by the former long-serving RIPA Monitoring Officer, Mr Paul Foote.

1.4 The inspection took place on 27th March 2019 and examined the period from the last inspection by the OSC, which was conducted on the 26th of November 2015 by Sir David Clarke. The inspection was conducted by IPCO Inspector Brendan Hughes.

1.5 This report should be addressed to:

Rose Rouse
Chief Executive
Eden District Council
Town Hall, Corney Square
Penrith
Cumbria, CA11 7QF

2 Inspection methodology

2.1 Prior to the inspection, key policy documents were made available. During the inspection, interviews and discussions of the use and non-use of RIPA powers by the council were held with the RIPA Monitoring Officer (effectively the Senior Responsible Officer – SRO). A focus group was also held with a number of senior council officers who are either designated as authorising officers (AOs) or potential applicants. This included:

- Rob Docherty (Assistant Director of Community Services)
- Lisa Tremble (Assistant Director, Governance, RIPA Co-ordinator and AO)
- Suzanne Fairer (Head of Revenue and Benefits and AO)
- Nick Atkinson (Planning Services Development Manager).

2.2 Discussion focused on topics such as the use of RIPA for noise monitoring, 'non-RIPA surveillance' and core functions, the conduct of general observation duties in plainclothes and the question of members of the public obtaining information for the council by means of a covert relationship acting on their own initiative. The council does not operate a public space CCTV system, although there was a general discussion about the possible (if very unlikely) use of other fixed and mobile council CCTV systems for directed surveillance by the council or a third party such as the police.

Eden District Council	Inspection period: 26/11/15-27/3/19					
	Total authorisations in current inspection period	Total authorisations in previous inspection period	Total records viewed at Inspection	Of this total, number of urgent oral records viewed	Of this total, number of major modifications viewed	Of this total, number of minor modifications viewed
Directed Surveillance	0	0	0	N/A	N/A	N/A
CHIS	0	0	N/A	N/A	N/A	N/A

Table 1. Key Statistics

3 Key findings

3.1 Recommendations

3.1.1 This was a good inspection, although inevitably somewhat limited given the lack of use of RIPA by EDC. Nevertheless, the council continues to maintain the integrity of its RIPA processes, although given the lack of current experience, care will be needed to ensure compliance should the need arise. Four recommendations have been made, three of which are minor and are listed in Table 2 below.

Number	Reference	In relation to	Recommendation	Recommendation type
R1	**5.10**	**Central Register**	The council should consider creating an Excel-based Centrally Retrievable Register of Authorisations capturing the data as required in the Codes of Practice and maintain it securely.	Recommendation - observed potential for improvements
R2	**5.39**	**Policy**	The RIPA Guidance and Procedure document should be amended to reflect the points made in 5.32 to 5.39 of the inspection report.	Recommendation - observed potential for improvements
R3	**5.41**	**Related Training**	AOs and other staff should receive updated RIPA training, preferably from an established external provider. Arrangements should be made for periodic refresher training as required.	Core recommendation - improvements must be made
R4	**5.44**	**Related Training**	All staff should receive basic RIPA awareness training. A central register of all RIPA related training should also be maintained.	Recommendation - observed potential for improvements

Table 2. Key recommendations resulting from inspection

3.2 Observations

3.2.1 The key observations arising from the inspection are listed in Table 3 below.

Number	Reference	In relation to	Recommendation	Observation type
O1	**5.16**	**Directed Surveillance**	The council should consider the use of practice or mock authorisations on a periodic basis to test the integrity of the authorisation process.	Comment – observation where practice could be improved
O2	**5.19**	**Directed Surveillance**	The council could produce edited versions of the Home Office standard RIPA forms to remove or amend sections relating to urgent oral provisions.	Comment – observation where practice could be improved
O3	**5.23**	**Directed Surveillance – Noise Monitoring**	The council should carefully evaluate the capabilities of any new technology or practice that may result in the capture of private information through covert surveillance. This arises from a Data Protection Impact Assessment as required under the Data Protection Legislation.	Comment – observation where practice could be improved
O4	**5.27**	**Direct Involvement**	The council should consider no longer designating the RIPA Co-ordinating officer an authorising officer.	Comment – observation where practice could be improved

Table 3. Key observations resulting from inspection

4 Previous recommendations

4.1 The previous inspection made one recommendation and the following progress was noted:

Recommendation 1. That EDC's Policy document be revised in accordance with paragraphs 12-15 of this report.

4.2 **Completed.** The previous inspection report recommended changes to EDC's RIPA policy to reflect the fact that it is possible for a member of the public to volunteer information to the council which they have obtained via a covert relationship and that the description in the policy of a CHIS should be changed to reflect this. It also asked for a section on non-RIPA surveillance to be included. Both changes had been made

and the recommendation is discharged. I make further observations on aspects of where the policy could be changed in section 5.31-5.39 below.

5 Inspection findings

Errors

5.1 No errors have been reported during the period under inspection and none were found during the inspection.

Confidential Information

5.2 There has been no case where confidential information has been obtained.

Journalistic Material

5.3 No journalistic material was sought or obtained.

Legally Privileged Material

5.4 No Legally Privileged Material was sought or obtained.

Informing Elected Representatives

5.5 The council has initiated compliance with the requirement to allow elected members to set RIPA policy at least once a year as set out in Section 3.30 of the CHIS and 4.47 of the Covert Surveillance and Property Interference (CSPI) Revised Codes of Practice of August 2018, which both state:

"Elected members of a local authority should review the authority's use of the 1997 Act and the 2000 Act and set the policy at least once a year. They should also consider internal reports on the use of the 1997 Act and the 2000 Act on a regular basis to ensure it is being used consistently with the local authority's policy and that the policy remains fit for purpose".

5.6 The policy was put to the Executive Committee on 5 June 2018 along with a review of the council's use of RIPA. This was good to see, as it is an area where many local authorities fail to comply with the Codes of Practice. EDC should continue to report in this manner on an annual basis. There is no need to report use of RIPA 'on at least a quarterly basis' as suggested by the Codes where there has been no actual use – annual reporting will suffice. In the unlikely event that EDC should become a more frequent user of RIPA powers, then this may need to change. I suggested during the inspection that the annual review and endorsement process be timed to coincide with the annual, calendar-year, statistical return requested by IPCO as this would enable both to be dealt with at the same time.

Centrally Retrievable Records of Authorisations

5.7 The centrally retriable record of authorisations was examined. This was in the form of a lever-arch file containing all past authorisations, reviews, renewals and cancellations. The central register itself was in the form of a series of printed out log-sheets at the front of the folder. These contained most of the necessary data fields, but it was pointed out that the latest codes of practice had expanded on what was required and that a digital register in the form of an Excel spreadsheet structured with a column for each of the relevant data fields and a 'sheet' for each calendar year, might be a better method of maintaining a central register. Any digital register would need to be protected, either by password protection of the Excel document itself (preferable) or by placing it in a restricted-access folder within the Council's electronic filing system, with access limited to the SRO and RIPA Co-ordinator.

5.8 Section 8.1 of the Covert Surveillance and Property Interference Revised Codes of Practice sets out what information should be recorded, which I repeat below for ease of reference, with my comments in square brackets:

- the type of authorisation/warrant; *[e.g. DS or CHIS]*
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation (if applicable);
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why; *[Not relevant to local authorities]*

- for local authorities, details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the authorised activity is likely to result in obtaining confidential or privileged information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled;
- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner.

5.9 Although the Central Record can be used to record all RIPA authorisations, both for directed surveillance and CHIS, it must be borne in mind that there are further central and individual record keeping requirements in relation to CHIS, which would require further columns. These additional requirements are set out in section 7 of the CHIS Code of Practice. The council should consider whether it would maintain a single Central Record for both DS and CHIS authorisations, or whether it would maintain two separate ones.

5.10 **Recommendation 1 (R1): The council should consider creating an Excel-based Centrally Retrievable Register of Authorisations capturing the data as required in the Codes of Practice and maintain it securely.**

Directed Surveillance

5.11 The council had not authorised any directed surveillance during the period of inspection nor had any applications been made. This means that no directed surveillance has been conducted since the introduction of the Protection of Freedoms Act 2012. From discussions, it was established that the reasons for this were largely the same as identified in the last inspection in 2015: responsibility for investigating more serious offences that would pass the 6-month threshold now often sat with other agencies, not least Cumbria County Council (responsible for trading standards enforcement), DWP and Cumbria Police; greater consideration was given to overt and preventative tactics and fewer resources were available to enforcement activity in general.

5.12 During the focus group session with AOs, the RIPA Co-ordinator and potential applicants, a number of common issues and scenarios relating to directed surveillance were discussed. In common with most second-tier local authorities, there were now few areas of enforcement that would require the use of RIPA powers. Some discussion was held on general observation duties and I pointed to section 3.33 of the CSPI Revised Codes of Practice which made it clear that patrolling of an area, in uniform or not, did not normally require a directed surveillance authorisation where any offenders would be immediately dealt with. This could be helpful if council officers were finding it difficult to conduct effective enforcement of issues like dog fouling or fly tipping in known problem areas with uniformed patrols.

5.13 The use of social media for digital or on-line investigation was also discussed. There is no technical restriction on EDC officers using official EDC computers to access social media sites. Given this, it is important that all officers have a basic awareness of RIPA and how on-line activity can, relatively easily, amount to directed surveillance. With the near universal ownership of smartphones, even technical restrictions on official computers cannot prevent the problem, as officers can be tempted to simply use a personal device for official purposes. Personal habits and behaviours for using the internet can easily be transferred to the work place. This is best tackled through policy and related training and is given further consideration in the relevant sections below.

5.14 The lack of use of RIPA is not an issue *per se*; there is no ‘right’ or ‘wrong’ level of usage for any given public authority and every authorisation is always considered entirely on its own circumstances. Lack of experience of accessing the powers does, however, raise risks. Firstly, a potential lack of general knowledge within the council about covert surveillance increases the risk of the conduct of unauthorised surveillance, as with the question of on-line research discussed above. Secondly, a lack of familiarity can lead to weaknesses in applications and authorisations when the need arises. Inevitably, when a case requiring directed surveillance does arise, it is likely to be a serious matter, and perhaps with considerable time pressures (such as acquiring further evidence to bolster an on-going prosecution). These pressures can quickly expose weaknesses in the authorisation processes.

5.15 Despite the lack of use, the council has done well to maintain its policy and processes to help mitigate against this risk. Effective policy is, however, not enough on its own and the continued delivery of routine RIPA training to likely applicants and all authorising officers is the key mitigation. In the absence of real cases, knowledge could be further supplemented by the conduct of an authorisation exercise testing various different scenarios and allowing applicants and authorising officers to practise completing the forms – infrequent applicants often greatly underestimate the detail required and AOs often fail to write an authorisation that clearly sets out what conduct is authorised and why it is necessary and proportionate, without making the error of simply relying on what the applicant has stated. For example, the specific offence should be detailed in necessity discussions. When considering collateral intrusion, detailed steps as to how this will be minimised and how any unwanted collateral product will be managed or disposed of should be stated.

5.16 **Observation 1 (O1): The council should consider the use of practice or mock authorisations on a periodic basis to test the integrity of the authorisation process.**

5.17 This level of detail lends itself to digital completion of the forms, which is already the practice used by EDC, with a wet signature by the AO. This is good practice. What matters is that the AO must be careful to show that they have engaged with the detail of the application and how *they* have arrived at *their* decision - the applicant will set out why the conduct is necessary and proportionate, but what matters is the record of the AO's thought processes and that they are their own and not simply a superficial re-statement of the applicant's arguments.

5.18 EDC correctly uses the most up-to-date version of the RIPA forms available from the Home Office RIPA webpage. The RIPA monitoring officer highlighted during the inspection that these forms, which are designed for all public authorities, still had a section of 'urgent oral' considerations which are not available to a local authority. This was a good point and underscores the fact that the Home Office forms are only a template and can be adapted. EDC could either edit the form to produce its own version without this box, or alternatively simply could insert a statement in the box with words to the effect: 'NOT AVAILABLE TO A LOCAL AUTHORITY'.

5.19 **Observation 2 (O2): The council could produce edited versions of the Home Office standard RIPA forms to remove or amend sections relating to urgent oral provisions.**

Directed Surveillance - Noise Monitoring

5.20 Noise monitoring was discussed in the focus group also. EDC would usually conduct such monitoring in an overt fashion, notifying the target of the monitoring by letter. It would consider a RIPA authorisation if there was a need for 'covert' monitoring. I pointed out that the Codes of Practice made it clear that even for such 'covert' monitoring, there was no need for a RIPA authorisation as it would be considered neither directed or intrusive surveillance. Section 3.40 of the Code of Practice refers:

"the covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be available."

5.21 The use of 'NoiseApp' – sound recording software that can be downloaded onto a smartphone belonging to a member of the public with a complaint of nuisance noise and used by them to capture and record excessive sound levels to then be provided to the council – was discussed. EDC was aware of the technology, but did not intend to subscribe to the service as it had concerns as to the integrity of any evidence gathered via the App. I noted that the neighbouring Carlisle City Council had adopted use of the App and had given considerable consideration into its usage and I noted that I was satisfied in my inspection of them the previous day that the App functioned in a manner as described in section 3.40 of the Codes and that RIPA authorisations were not required. It did illustrate the need for close understanding of the technical characteristics of the App – i.e. what sound levels it recorded at, how it was calibrated, and that these would not exceed that of the naked ear or in some other way enhance

the sensitivity of the phone's audio capture, otherwise there was a clear risk of it being used to conduct unauthorised intrusive surveillance (if capturing speech from within a residential premises or private vehicle) – a reportable error. Close attention also needed to be given to the guidance given to the user of the App, as the positioning of the phone during recording (i.e. trying to raise the sound level by pushing it through a gap in a fence, or placing it on a neighbour's window sill) would also risk being intrusive surveillance.

5.22 Under data protection legislation, all acquisitions of new technology now have to be screened for their processing of personal data with a data protection impact assessment overseen by the Data Protection Officer. This is an entirely separate statutory regime and personal data is not the same thing as private data under RIPA, but it is a mechanism where privacy considerations for new technology are considered and it is helpful as a method of detecting any potential deployments of new technology that may engage RIPA considerations. It is very helpful therefore that the current DPO is also the RIPA Co-ordinator and has common awareness of both statutory regimes.

5.23 **Observation 3 (O3): The council should carefully evaluate the capabilities of any new technology or practice that may result in the capture of private information through covert surveillance. This arises from a Data Protection Impact Assessment as required under the Data Protection Legislation.**

Covert Human Intelligence Sources (CHIS)

5.24 Since the last inspection there have been no authorisations for the use and conduct of a CHIS. Council policy covers the use of CHIS. The focus group did discuss the challenges faced by councils when receiving information from the public as it can be possible for a person to meet the definition of a CHIS without being tasked to establish or maintain a covert relationship by the council. Determining this can be hard without asking the right questions of the person volunteering the information. Likewise, care must be taken not to deter public spirted persons from passing information to the council with ill-put questions as to their methods and motives – civil society depends on such public mindedness. A pragmatic approach should be considered to evaluating the risk – if the member of the public is providing information on the same subject repeatedly, or it is clear that the information was private in nature and could only have been obtained by forming or exploiting a relationship for this purpose, then more searching questions as to how they obtained the information being volunteered could be asked and a risk assessment conducted, as the council will have a duty of care towards the member of public, not least to ensure the confidentiality of the information and their identity as the source, if this is necessary. If the information is of sufficient value to the council that it wished to obtain more, requiring further use of the covert relationship, then a CHIS authorisation should be sought.

5.25 It is hard to make a case for extensive investment in CHIS training when the council has never used this tactic and has no plans to do so. Securely handling and controlling CHIS who are not council officers is a specialised role and would need far greater investment to do so safely. Training is better invested in knowing how to deal with the public and to identify when one may be acting in a manner that could be defined as a CHIS. If the need to develop a CHIS who is not a council officer does arise, then partnership arrangements with other public authorities, such as Cumbria Police, may be a more effective route. Needless to say, any council officer who does act as a CHIS still also needs to be managed by appropriately trained handlers and a controller.

Direct Involvement (Self-authorisation)

5.26 There were no instances of self-authorisation. The council has five AOs including the Chief Executive. This is more than adequate, and it was suggested by the RIPA

Monitoring Officer that this number be reduced to four by removing the RIPA Co-ordinator from the list of designated AOs. I agreed with this suggestion as, ideally, neither the SRO or RIPA Co-ordinator should act as an AO. With the four remaining AOs there will be an adequate number with sufficient lateral and vertical separation in the management structure from likely applicants to mean that self-authorisation should not occur. It was pointed out that it is good practice for applications from one business area (e.g. environmental health) to be sent to an AO *without* direct responsibility for the business area. However, EDC certainly meets the definition of a small public authority and some latitude in this area is to be expected. I note that the Director of People and Places role is currently vacant, but will be appointed in the summer. They will be designated as an AO and should receive training as necessary before performing the role.

5.27 **Observation 4 (O4): The council should consider no longer designating the RIPA Co-ordinating officer an authorising officer.**

Communications Data (CD)

5.28 The Council retained the ability to obtain communications data under the provisions of Part 2 of RIPA during most of the period under inspection and will now continue to do so under Part 3 of IPA. No applications were made and no communications data obtained. The Council does not maintain a CD policy. Although applications for CD are dealt with by the National anti-Fraud Network (NaFN) Single Point of Contact (SPoC), applications still need to be initiated and the subsequent product dealt with lawfully if the need should ever arise. The Council should consider reviewing arrangements in place for the acquisition of CD to ensure they are compliant with Section 73 IPA, and in particular, paragraphs 8.1 to 8.7 of the Communications Data Code of Practice (2018). This may require having policy in place.

R. v Sutherland considerations

5.29 Given the lack of authorisations, there was no real way of testing compliance with the need to ensure those conducting surveillance have had sight of or been properly briefed on what conduct has been authorised by an AO. The issue was discussed with the RIPA Monitoring Officer and the requirement was well understood – given that a RIPA authorisation would be a rare event, any directed surveillance activity would be carefully managed.

Policy and Procedure

5.30 The council has a comprehensive and well-structured RIPA policy covering both the use of directed surveillance and CHIS which was last updated in June 2018. The policy if followed will ensure compliance with the legislation. A number of minor points were made where further improvements to this excellent policy could be made, as follows.

5.31 At 1.10 it may be worth including a statement that any error should be drawn to the RIPA Monitoring Officer's attention and may have to be reported to IPCO as set out in Section 8 (8.6 to 8.18) of the Covert Surveillance and Property Interference Code of Practice (and the similar provisions set out in the CHIS Code of Practice).

5.32 At 1.11, references to the RIPA Codes of Practice should be updated to refer to the most recent versions (August 2018). Any hyper-links to the codes should also be updated.

5.33 Section 1.20 on digital investigations could be made clearer and the fact that information is considered 'open source' may still require a DSA – it is the frequency

and depth of observation that can determine if something is directed surveillance, not that the observation occurs in a 'public space'. I suggest adopting the language used in note 289 of the OSC (now IPCO) Procedures and Guidance and making reference to the section on on-line covert activity in the CSPI Codes of Practice (Sections 3.10 to 3.17), which give some helpful examples.

5.34 The section on Non-RIPA Authorisations was presumably added to meet the recommendation made in the previous inspection and is well drafted. It should make clear that any such authorisation may not benefit from the protection of RIPA to ensure it is lawful, although appropriate drafting and handling, designed, for instance, to accommodate the ECHR, may ensure it is still lawful. Needless to say, great care should be taken when considering a non-RIPA authorisation, particularly in cases which relate to the core functions of the council (i.e. prevention and detection of crime).

5.35 At 1.26, as well as stating that the policy will be reviewed annually, it should also state that elected Members will be given the opportunity to set RIPA policy on an annual basis.

5.36 Section 4.11 could be updated to reflect the full record keeping requirements for Directed Surveillance as set out in the CSPI Codes of Practice as have been set out in 5.8 above.

5.37 It is not clear why section 4.46, which deals with Judicial Approval, is located in the document where it is – it is bracketed by sections dealing with CHIS. This could be moved to a more natural place in the policy, ideally immediately after the sections setting out what the AO must do when considering an application. This section could also be enhanced with more practical guidance on matters such as whom to contact in the court, who should attend etc. Section 5 of the Home Office guidance to magistrates' courts, published in 2012 and available on the Home Office RIPA webpages, gives useful detail in this regard.

5.38 It would be helpful at some point in the policy that the roles of RIPA Monitoring Officer and RIPA Co-ordinator were defined. Mr Neal suggested that the Monitoring Officer function simply be re-titled to Senior Responsible Officer (SRO). This makes sense – as already noted the two roles are identical, but SRO is the term used in the codes of practice and by most public authorities. Adopting it would eliminate any potential confusion on this point.

5.39 **Recommendation 2 (R2): The RIPA Guidance and Procedure document should be amended to reflect the points made in 5.32 to 5.39 of the inspection report.**

Related Training

5.40 A copy of the RIPA training material (a PowerPoint presentation) was made available during the inspection. This had been delivered in 2015 and attended by a range of staff who were potential applicants. All authorising officers had received RIPA training during various points in their career, but none had received particularly recent refresher training. Mr Neal volunteered at the outset that this was a weakness in the Council's compliance arrangements and I agreed with him and recommended that the four AOs (assuming the RIPA Co-ordinator will no longer have this function) receive updated RIPA training from an established external trainer familiar with all of the changes that have occurred since IPA 2016 became law. If resources permit, the Monitoring Officer/SRO and the most likely potential applicants should also attend any training. If practicable costs could be shared with neighbouring councils. Refresher training should be arranged on an ongoing periodic basis, preferably no longer than at 3-yearly intervals. New AOs should receive training as soon as possible and ideally, should not act as an AO until this is done.

5.41 **Recommendation 3 (R3): AOs and other staff should receive updated RIPA training, preferably from an established external provider. Arrangements should be made for periodic refresher training as required.**

5.42 Wider RIPA awareness training was also discussed. As highlighted above, there is a real risk in public authorities that do not use RIPA often, if at all, that its officers may inadvertently conduct unauthorised surveillance though lack of awareness of RIPA and its requirements. This is especially true for on-line investigation of social media sites – the personal smartphone can make a digital surveillant of anyone.

5.43 To mitigate this risk, all staff should receive basic RIPA awareness training. This is presently not addressed in EDC's training profile for all staff and it is recommended that it should be. The training need not be lengthy or explore the legal background and underpinnings of RIPA. Rather, it needs to make staff aware they cannot simply monitor members of the public, on-line (or otherwise) as they choose to and that they should seek guidance if they feel that they have need to do so. There are numerous means of delivering such basic awareness, e.g. e-learning modules or staff induction training. It generally sits well within the broader area of information governance and can often be delivered alongside data protection training. Social media policy, if available, should also make reference to RIPA. A register of, or means of centrally collating when necessary, all staff who have received RIPA training (AOs and others) should also be maintained.

5.44 **Recommendation 4 (R4): All staff should receive basic RIPA awareness training. A central register of all RIPA related training should also be maintained.**

6 Conclusion

6.1 This was a good inspection. Mr Neal was a welcoming and effective host and I thank him for his efforts in facilitating the inspection. The council had made a good effort to discharge the recommendation from the last inspection and was, on the face of it, able to comply with the legislation should the need arise – which is commendable given the very small size of the council. However, with no authorisations made, it is difficult to gauge how robust the compliance frameworks of policy, process and training would prove to be in reality, and the council must be mindful of this risk. Adoption of the recommendations on training will help mitigate this.

Brendan Hughes
IPCO Inspector

APPENDIX 2

Regulation of Investigatory Powers Act 2000

Corporate Guidelines and Policy

M Neal
~~Deputy Chief Executive~~Director of Corporate Services
Eden District Council
Town Hall
Penrith
Cumbria CA11 7QF

Updated October ~~June~~ 2019~~8~~

This page is left intentionally blank

Contents

This page is left intentionally blank

Section 1

Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides for public authorities to give authorisation to carry out **covert surveillance** activities. Public Authorities include local authorities therefore the Council may itself give an authorisation to its officers to carry out covert surveillance subject to approval by a Magistrate or a Justice of the Peace.

1.2 The fundamental premise of RIPA is to ensure that covert surveillance is carried out in the appropriate manner. It requires that the public body wishing to carry out such surveillance does so after carrying out a balancing exercise in which the need for covert surveillance is balanced against the rights of the individual. The Human Rights Act 1998 incorporated the European Convention of Human Rights ("the Convention") into UK law. This means that Convention rights are enforceable in our domestic courts.

1.3 Article 8 of the Convention provides that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence; and

2. 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.

1.4 For covert surveillance to be justified it must be both **necessary** and **proportionate** having regard to the need to prevent or detect crime or prevent disorder. If it is possible to obtain evidence overtly then this is the method in which it should be gathered.

1.5 Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that a person who is subject to surveillance is unaware that it is taking place. The definition of surveillance is very wide and includes such activities as:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device.

1.6 Although the term surveillance covers a wide range of activities, it is important to note that RIPA applies **only** to **covert** surveillance. If the person who is subject to the covert surveillance is aware that it is taking place it will not be necessary to obtain authorisations under RIPA.

1.7 The purpose of RIPA is to place covert surveillance activities on a lawful footing. The impetus for this has arisen from the coming into force of the Human Rights Act 1998 ('HRA'). If the Council fails to comply with the HRA it is in breach of statutory duty and two possible consequences may follow:

- any person who has suffered loss due to such breach may claim compensation from the Council; and / or
- any enforcement proceedings brought by the Council against a person who has suffered such breach may be subject to 'collateral challenge' by way of defence of non-compliance by the Council with the HRA.

1.8 A number of the Council's activities may involve covert investigations or surveillance of individuals and organisations. Service areas in which officers are likely to engage in covert surveillance include those dealing with licensing, benefit fraud, planning enforcement, noise nuisance and anti-social behaviour. RIPA was enacted in order to provide a clear statutory framework for the operation of certain investigative techniques and to provide for compliance with the HRA. The use and authorisation of covert Directed Surveillance and Covert Human Intelligence Sources are of particular relevance to local authorities. Safeguards are necessary to ensure that investigative techniques in a particular case are both necessary and proportionate to meet law enforcement objectives. Appropriate authorisation systems can ensure compliance with these objectives.

1.9 RIPA assists by:

- Clarifying what types of covert surveillance may be undertaken by local authorities; and
- Providing a scheme for the giving of authorisations.

1.10 The Director of Corporate Services is the designated Senior Responsible Officer and is thereby responsible for the oversight of the Policy and the application of the processes, training on RIPA and the maintenance of a Central Register of authorisations.

1.11 The Assistant Director Governance is the designated RIPA Co-ordinating Officer and has operational responsibility for the management and oversight of requests and authorisations under RIPA, updating of the Central Register of authorisations. and for liaison with the Magistrates Court in terms of any authorisations and renewals.

1.12 If the Council fails to obtain an authorisation for surveillance in accordance with the scheme set out in the RIPA it has not thereby committed a criminal offence nor is it automatically subject to any sanction or penalty imposed under civil law. However, in the absence of authorisation there is a risk that the Council will not be able to demonstrate that any covert surveillance has been carried out on a lawful basis. There then arises the further risk that any proceedings which the Council is then undertaking against the person concerned (eg statutory enforcement proceedings or a prosecution) may be subject to a successful challenge and/or the Council may be subject to a legal claim for compensation by the person concerned. Any error should be drawn to the attention of the Senior Responsible Officer and may need to

be reported to the Investigatory Powers Commissioner's Office in accordance with the Section 8 of the Covert Surveillance and Property Interference Code of Practice.

1.131 In order to provide public authorities with guidance the former Office of the Surveillance Commissioners ("OSC") and the Government issued various Codes of Guidance. The OSC has been superseded with effect from August 2018 ~~September 2017~~ by the Investigatory Powers Commissioner's Office (IPCO). The guidance which applies to local authorities are:

- OSC Procedures and Guidance (July 2016);
- Covert Surveillance and Property Interference (December 2014); and
- Covert Human Intelligence Sources Codes of Practice (December 2014).

1.142 The Government has also provided assistance by providing content on its website on RIPA. The website sets out the statutory provisions, the Codes and model forms for use by public authorities:

RIPA codes - GOV.UK

RIPA forms - GOV.UK

The IPCO's website address is http://www.ipco.org.uk

1.153 The purposes of this policy document are to explain what the Council's procedures are for the authorisation and carrying out of covert Directed Surveillance and the use of Covert Human Intelligence Sources and also to provide guidance for staff who are designated as Authorising Officers or who are authorised to carry out covert Directed Surveillance or to use or act as Covert Human Intelligence Sources.

1.164 The Protection of Freedoms Act 2012 made two significant changes to how local authorities use RIPA. The approval of a Magistrate or Justice of the Peace to a local authority authorisation is required. In addition there is a crime threshold relating to directed surveillance. A local authority can only grant an authorisation under RIPA for the use of directed surveillance where the authority is investigating particular types of criminal offence where there is a maximum custodial of six months or more or the offences relate to underage sale of alcohol or tobacco,

1.175 This policy document sets out the key concepts which are used in RIPA. An understanding of such key concepts is essential for all officers who are designated as Authorising Officers or who are authorised to carry out covert Directed Surveillance or who are authorised to use or act as Covert Human Intelligence Sources. It also sets out the procedures for obtaining authorisations and the Council's requirements for record keeping.

1.186 This guidance provides information as to the legislative requirements in relation to directed Covert Surveillance and Covert Human Intelligence Sources and the authorisation procedures. The guidance is based upon legislation and the Code of Practice for Covert Surveillance and Covert Human Intelligence Sources.

1.19~~7~~ This guidance should ensure that a consistent, simple and effective system is applied and maintained throughout the Council. The guidance will be supplemented by appropriate training for all relevant employees.

1.20~~18~~ The IPCO will from time to time carry out statutory inspections. A representative of the IPCO will look at the Council's policies and procedures and their application.

1.21~~9~~ Surveillance can be an intrusion on the privacy of a citizen. Investigations should be conducted in a manner which strikes a fair balance between the rights of citizens and the legitimate interests of the public in the proper administration of justice and the Council's functions. Surveillance should only be authorised if this is both necessary and proportionate. The application of this Guidance will ensure that RIPA is properly applied throughout the Council.

Social Media

1.22~~0~~ Social networking sites may provide a source of information in investigations. Care should be taken to understand how a social networking site works and whether it should be regarded as 'open source'. If access controls are applied there is a reasonable expectation of privacy so that the site should not be regarded as open source. If privacy settings are available but not applied the date may be considered to be open source. An overview or review of open source social networking sites generally will not require an authorisation. However, if an overview of a site is carried out in relation to an individual with regularity this may amount to directed surveillance for which an authorisation is required. Becoming a "friend" on a site or being connected" on someone's business network site to conduct an investigation and using a false identity will amount to directed surveillance for which an authorisation is required provided it is necessary and proportionate. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established. Legal advice should be sought on and before the use of social networking sites as part of an investigation.

Non RIPA Authorisation

1.23 RIPA does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise surveillance in a manner that ensures compliance with the HRA. Equally RIPA does not prevent surveillance from being carried out or require that surveillance may only be carried out under RIPA.

1.24 There may be times when it will be necessary to carry out covert Directed Surveillance or use a Covert Human Intelligence Source other than by using RIPA. For example there may be a serious internal investigation that may lead to criminal proceedings. In such circumstances RIPA procedures may be appropriate. However in relation to an investigation that for example a member of staff or a contractor is not carrying out their work as contracted, then a RIPA authorisation is not usually available as in such circumstances, because criminal proceedings are not normally contemplated.

1.25~~3~~ Similarly there may be serious cases of neighbour nuisance or involving anti-social activity which involve potential criminal offences for which the penalty is below the

thresholds which would enable use of a RIPA authorisation. Nonetheless in such cases there may be strong grounds for carrying out covert Directed Surveillance or use of a Covert Human Intelligence Source. Indeed there may be circumstances in which covert Directed Surveillance or use of a Covert Human Intelligence Source is the only effective means of efficiently obtaining significant information to take an investigation forward.

1.2~~6~~4 In the circumstances outlined above, a RIPA application may be completed in accordance with this Policy and the application must be clearly endorsed in red "NON_RIPA SURVEILLANCE" along the top of the first page. The application must be submitted in the normal fashion to the Authorising Officer who must consider it under the necessity and proportionality test in the same way they would a RIPA application. The normal procedure of timescales, review and cancellations must also be followed. Any non RIPA authorisation would not benefit from the protection of RIPA to guarantee lawfulness, although steps would be taken to ensure that such authorisations complied with other legal requirements such as those under the European Convention of Human Rights.

1.27 The authorisation, regular review, the outcome of any review, renewal applications and eventual cancellation must be notified to the Assistant Director (Governance ~~Legal Services~~) in the normal way and using the same timescales as would be applicable to a RIPA investigation. However for non RIPA surveillance the requirement to seek approval from the Magistrates Court is inapplicable. The authorisation, renewal or cancellation for non RIPA surveillance takes effect from the date that it is authorised or approved by the Authorising Officer.

Annual Review

1.2~~8~~6 The policy will be reviewed annually and the ~~C~~council ~~members~~Executive will be provided with the opportunity to have an input into this process.

Section 2

Legislative Background

2.1 The Council can only use Directed Surveillance or a Covert Human Intelligence Source for the prevention or detection of crime or for preventing disorder. The Council cannot seek to carry out surveillance under the auspices of a RIPA authorisation for any other purpose. It is unlawful for a public authority to act in a way which is incompatible with a Convention Right.

2.2 RIPA provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities and in particular it:

- regulates the interception of communications;
- puts other intrusive investigative techniques on a statutory footing;
- provides powers to help combat the threat posed by rising criminal use of strong encryption; and
- ensures that there is independent judicial oversight of the powers in the Act.

2.3 RIPA is consistent with the HRA and creates a system of safeguards reflecting the requirements of Article 8 of the Convention Rights. It provides that the covert surveillance which is undertaken in a manner which is necessary and proportionate for the detection or prevention of crime and disorder is lawful.

2.4 A public authority can only interfere with a person's Article 8 rights if it can be shown that:

- the interference had a clear legal basis;
- the aim of the interference was prevention of crime or disorder;
- it was necessary (and not just reasonable) to interfere with their rights; and
- the interference was proportionate, that is, going only as far as was required to meet the aim.

2.5 A public authority should weigh all the competing interests carefully so as to justify any interference before taking decisions affecting people's rights under Article 8. Rights under Article 8 may need to be balanced against other rights, for example, the right to free expression.

2.6 A public authority must also make a risk assessment on any possible collateral intrusion, ie impact on the lives of third parties who are not directly involved.

2.7 Parts of RIPA are only relevant to police and other law enforcement agencies such as, the provisions relating to intrusive surveillance. However the parts of RIPA relating to the use of covert Directed Surveillance, agents, informants and undercover officers are relevant to public authorities such as the Council. The Council cannot undertake any intrusive surveillance.

2.8 An authorisation and any renewal requires the approval of a Magistrate or Justice of the Peace and the crime threshold must be met in relation to directed Covert Surveillance or the use of a CHIS under RIPA.

Section 3

Directed Surveillance and Covert Human Intelligence Source (CHIS)

3.1 The Council is allowed to carry out Directed Surveillance and Covert Human Intelligence Sources (CHIS). Anyone who is engaged in the application of RIPA should have an understanding of the key definitions and considerations which are set out and commented upon in this Guidance and this Section 3.

3.2 Surveillance is defined in RIPA as:

- monitoring, observing, listening to persons, their movements, conversations, other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; or
- surveillance by or with the assistance of a surveillance device.

Surveillance can be directed or intrusive.

3.3 Directed Surveillance is:

- covert. Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is taking place;
- not intrusive. Surveillance is intrusive only if it is covert and:
    - is carried out in relation to anything taking place on residential premises or in a private vehicle; and
    - involves the presence of an individual on the premises or vehicle or is carried out by a surveillance device;
- undertaken for the purpose of a specific investigation or operation in a way likely to obtain private information about a person whether or not that person is specifically targeted for purposes of an investigation (otherwise than by immediate response to events which would make seeking authorisation under RIPA unreasonable e.g. spotting something suspicious and continuing to observe it).

3.4 RIPA states that surveillance does **not** include:

a) any conduct of a Covert Human Intelligence Source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;

b) the use of a Covert Human Intelligence Source for so obtaining or recording information; or

c) any entry on or interference with property or wireless telegraphy as this would be unlawful unless authorised under warrants for the intelligence service legislation or powers of police and customs officers.

3.5 Is the surveillance covert?

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

Whether or not the surveillance is covert is the first question which should be asked when considering the seeking of authorisation; if it is not covert, the framework of RIPA will not apply. Overt surveillance should be used whenever possible.

3.6 Is it for the purposes of a specific investigation or a specific operation?

This may include, for example, an anti-fraud operation conducted in relation to Housing / Council Tax Benefits.

3.7 Is it in such a manner that is likely to result in the obtaining of private information about a person?

'Private Information' is any information relating to a person's private or family life.

For example, an investigation is to observe a person's home to determine his / her comings and goings would be covered.

3.8 Is it otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

The Codes explain how a (Police) Officer would not require an authorisation to conceal himself and observe a suspicious person he came across in the course of a patrol.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within the RIPA framework.

3.9 Is the Surveillance Intrusive?

Directed surveillance becomes Intrusive Surveillance if it:

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 an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Furthermore, surveillance is intrusive if it is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information

of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

If the device is not on the premises or in the vehicle, it is only Intrusive Surveillance if it consistently produces information of the same quality as if it were. This might catch sound recording equipment which is placed in premises next door to the premises which is under investigation.

Commercial premises and vehicles are excluded from intrusive surveillance.

3.10 A local authority cannot undertake intrusive surveillance, only directed Covert Surveillance and the use of a CHIS.

3.11 A person is a CHIS if he/she establishes or maintains a personal or other relationship with a person for the purpose of facilitating the doing of anything that:

- covertly uses such a relationship to obtain information or to provide access to information to another person; or
- covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

3.12 The Authorising Officer must be satisfied that the conduct or use is proportionate to what is sought to be achieved and that arrangements are in place to ensure appropriate levels of management and oversight and that records contain the statutory particulars and are not available except on a need to know basis.

3.13 Conduct is defined as establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information. Use is defined as actions inducing, asking or assisting a person to act as a CHIS.

3.14 Directed surveillance and CHIS may be authorised by the individuals identified in Annex A. The categories of officers who may grant authorisations are specified by regulation. The Council has granted specific authorisations in line with the statutory requirements. An Authorising Officer has specific responsibilities under RIPA and the Code of Practice. Any Authorising Officer must be aware of the relevant statutory requirements and address ~~his/her~~their mind to the relevant issues.

3.15 An Authorising Officer must believe the authorisation to be proportionate to what is sought to be achieved by carrying it out and necessary to prevent or detect crime or prevent disorder.

3.16 A record of all authorisations must be maintained. The records are subject to inspection by the Investigatory Powers Commissioner's Office.

Section 4

Authorisations

The Authorisations and the Approval of a Justice of the Peace

4.1 An authorisation is required both through the Council's internal processes and externally from a Magistrate or Justice of the Peace. The internal process must be completed in its entirety and then an application must be made to a Magistrate or Justice of the Peace for approval to a grant or a renewal of an authorisation. An authorisation is not effective until it has obtained the authorisation from a Magistrate or Justice of the Peace and the directed Covert Surveillance or the use of the Covert Human Intelligence Source cannot take place until the authorisation from the Magistrate or Justice of the Peace is obtained.

Directed Surveillance

4.2 An authorisation under Part II of RIPA will provide lawful authority to carry out surveillance. RIPA does not impose a requirement on the Council to seek or obtain an authorisation where one is available under RIPA. However, where there is an interference by the Council with the right to respect for private and family life guaranteed under Article 8 of the Convention Rights and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of Section 6 of the HRA. The Police and Criminal Evidence Act 1984 (PACE) also regulates the admissibility of evidence. The proper authorisation of surveillance should ensure the admissibility of such evidence under common law, PACE and the HRA.

4.3 Employees of the Council are required to seek an authorisation where the surveillance is likely to interfere with a person's rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. The obtaining of an authorisation will ensure that the action is carried out in accordance with the law and will be subject to stringent safeguards against abuse.

4.4 The obtaining of an authorisation under RIPA will ensure that there is a justifiable interference with an individual's Article 8 Convention rights only if it is necessary and proportionate for these activities to take place. RIPA requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of the particular case for the statutory ground.

4.5 If the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. The Authorising Officer must balance the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less interfering or intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

4.5.1 An Authorising Officer and the officer who intends to carry out the surveillance must consider whether the crime threshold is met. Each officer should be aware of the nature of the offence which is the subject of the investigation. The offence should be identified. The maximum custodial sentence which is available for the offence should be identified and both the authorising officer and the officer carrying out the surveillance must be satisfied that the maximum sentence is one of six months or more or the offence itself relates to the underage sale of alcohol and tobacco.

4.6 The Conditions for Authorisation – Directed Surveillance

4.6.1 For Directed Surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he or she believes:

a) that an authorisation is **necessary** (on the grounds detailed below); and

b) the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

4.6.2 An authorisation must be **necessary** for the purpose of preventing or detecting crime.

4.6.3 **Significant** consideration must be given to the issue of necessity. Everyone has the right to respect for ~~his/her~~their private and family life (Article 8, Human Rights Act 1998). There shall be no interference with this right other than is necessary in the interests of the prevention of crime and disorder. 'Necessity' has to be established on the facts of each individual case before an individual's rights of privacy can be legitimately infringed.

4.6.4 Section 80 of RIPA provides a general saving for lawful conduct, i.e. if the conduct in question does not require authorisation under the Act and is lawful in any event then it continues to be lawful. The effect of this section is that if the Council's duty can be carried out without recourse to an authorisation then that is the preferred way to do it. In other words, if the required information can be obtained by overt means in any given circumstance, covert surveillance can never be **necessary**. The authorisation forms contain a section in which the applicant is required to identify why covert surveillance is necessary in any given case. **It is the task of the Authorising O~~o~~fficer to apply ~~his/her~~their their mind to this, as well as proportionality, before granting an authorisation**.

4.6.5 In addition the authorisation for the activity must be **proportionate**. This involves a balancing exercise of the need for the activity in operational terms against the degree of interference with the rights of the subject of the surveillance and of any other persons. It will not be proportionate if the interference is excessive in the circumstances of the case or if the information could have been obtained using less intrusive means. All activity must be carefully managed and must not be arbitrary or unfair.

4.6.6 The onus is therefore on the **Authorising Officer** who is considering an application to authorise surveillance to be satisfied that it is:

a) necessary for the ground stated above; and

b) is proportionate to its aim.

4.7 An Authorising Officer should take into account the risk of interference or intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion) before authorising the surveillance. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

4.8 An application for an authorisation should include an assessment of the risk of any collateral intrusion. An Authorising Officer should take this into account when considering the proportionality of the surveillance.

4.9 Any officer carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

4.10 Any person granting or applying for an authorisation or warrant will need to be aware of any particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. Where combined authorisations are necessary one agency can act on behalf of another and obtain the necessary authorisation.

The Central Register

4.11 A central register of all authorisations is held by the ~~Deputy Chief Executive~~ Director of Corporate Services on behalf of the Council as the ~~RIPA Monitoring Officer~~Senior Responsible Officer. The central register will be regularly updated by the Assistant Director Governance (as RIPA Co-ordinating Officer) whenever an authorisation is granted, renewed, cancelled or reviewed. The register will be made available to a representative of the Investigatory Powers Commissioner's Office upon request. The register must be retained for a period of at least three years. The central register must contain the details of any authorisation and in particular the following information:-

- the type of authorisation/warrant;
- the date the authorisation was given;
- the name, job title and grade of the Authorising Officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of the subjects, if known;
- if the authorisation is reviewed, when it was reviewed, who carried out the review, and the result of the review;

- details of any attendances at the Magistrates Court, to include the date and time of the hearing, the determining Magistrate, the decision reached and the date of decision;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name, post title and grade of the Authorising Officer;
- whether the investigation or operation is likely to result in obtaining confidential or privileged information as defined in the Code of Practice;
- whether the authorisation was granted by an individual directly involved in the investigation
- the date of the order from a Magistrate or Justice of the Peace confirming the authorisation;
- the date the authorisation was cancelled;
- where any application is refused, the grounds for refusal given by the issuing authority or Judicial Commissioner .

The URN in each case will follow the format "L/001" where "L" will be initials denoting the relevant service area followed by a sequential number commencing at 001.

4.12 In all cases, the Authorising Officer will maintain the following documentation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period for which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- details of the application to the Court and a copy of the order from the Magistrate or Justice of the Peace
- the date and time when any instruction was given by the Authorising Officer.

All original documents and authorisations and ancillary documents will be forwarded to the ~~Deputy Chief Executive~~ Director of Corporate Services as the ~~RIPA Monitoring Officer~~Senior Responsible Officer for inclusion on the central file within seven days of their completion. The originals of any relevant documentation should be supplied to the ~~Deputy Chief Executive~~ Director of Corporate ~~for~~Services for inspection or monitoring purposes when requested. All such documentation must be identified with the relevant URN. An authorisation may be cancelled orally. The details of when and by whom this was done should be endorsed on the cancellation form when it is completed and recorded on the central register.

4.13 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the disclosure requirements for a suitable further period, subject to any subsequent review. RIPA does not prevent material obtained from properly authorised surveillance being used in other investigations. Authorising Officers must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must ensure compliance with any data protection requirements in addition.

4.14 RIPA does not provide any special protection for "confidential information". Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. In a case where surveillance is likely to lead to knowledge of confidential information the Head of Paid Service (namely the Chief Executive) or (in his absence) the Director of ~~Finance~~ People and Place must make the necessary authorisation (see Annex A).

4.15 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). However, privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. A substantial proportion of the communications between a lawyer and ~~his/her~~their client(s) may be subject to legal privilege.

4.16 RIPA does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and surveillance which acquires such material may engage Article 6 (right to a fair trial) as well as Article 8 (right to respect for private and family life) of the Convention. Therefore an application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances and full regard should be had to the proportionality issues. The application should state how likely it is that information subject to legal privilege will be acquired and whether one of the purposes of the surveillance is to obtain legally privileged information. If in any doubt advice from the Assistant Director Legal Services should be sought on the handling or dissemination of information which may be subject to legal privilege.

4.17 Similar consideration must also be given to authorisations that involve confidential personal information and confidential journalistic material. Personal information is that concerning an individual (living or dead) who can be identified from it and relating to ~~his/her~~their physical or mental health or to spiritual counselling or assistance given or to be given to him/her. Confidential personal information is personal information which a person has acquired or created in the course of any trade, business, profession or other occupations, and which he/she holds in confidence; and communications as a result of which personal information is acquired or created and held in confidence.

4.18 Confidential journalistic material 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.

4.19 Under RIPA an authorisation for covert Directed Surveillance may be granted by an Authorising Officer only where he/she believes that the authorisation is necessary and proportionate in the circumstances of the particular case solely if it is:

- for the purpose of preventing and detecting crime or of preventing disorder.

4.20 An Authorising Officer must believe that the surveillance is proportionate to what it seeks to achieve. An Authorising Officer must consider the surveillance is necessary for the purpose of preventing and detecting crime or preventing order. An Authorising Officer must address and consider proportionality and necessity in each case in deciding whether or not to grant the authorisation.

4.21 The responsibility for authorising the carrying out of directed surveillance rests with the Authorising Officer and requires ~~his/her~~their personal authority.

4.22 An Authorising Officer must give authorisations in writing.

4.23 Authorising Officers should not be authorising investigations or operations in which they are directly involved.

4.24 A written application for authorisation for directed surveillance should describe any conduct to be authorised and the purpose of the investigation or operation. The application should include:

- the reasons why the authorisation is necessary in the particular case for the purpose of prevention and detecting crime;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- 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 which is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

An Application for directed surveillance authorisation must be made on the appropriate Form (please refer to Section 8).

4.25 A written authorisation will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

4.26 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion authorisations should be reviewed at least monthly. Authorising Oefficers should determine how often a review takes place. The appropriate form must be used in reviewing a covert Directed Surveillance authorisation (see Section 8).

4.27 Before an authorisation ceases to have effect, the Authorising Officer may renew it in writing for a further period of three months if he/she considers it necessary for the authorisation to continue for the purpose for which it was given.

4.28 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation.

4.29 All applications for a renewal of an authorisation for directed surveillance 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 provided on first application;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance; and
- the results of regular reviews of the investigation or operation.

The renewal should be kept/recorded as part of the central register of authorisations.

A renewal of a directed surveillance authorisation must be done using the appropriate form (see Section 8). A renewal also will require the approval of a Magistrate.

4.30 An Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on either the person who has taken over the role of Authorising Officer or another Authorising Officer.

4.31 As soon as a decision is taken that covert Directed Surveillance should be discontinued, an instruction must be given to those involved to stop all surveillance

of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation.

A cancellation of a Directed Surveillance authorisation must be done using the appropriate form (see Section 8).

4.32 RIPA establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

Covert Human Intelligence Sources

4.33 The provisions relating to CHIS do not normally apply where members of the public volunteer information to the Council, as part of their normal civic duties, or to contact numbers set up to receive information. The provisions may apply if a personal relationship is established or information is provided repeatedly. In practice the use of CHIS by the Council should be very limited.

4.34 The rules relating to necessity, proportionality, collateral intrusion and combined authorisations are the same for CHIS as they are for directed surveillance.

4.35 The Authorising Officer must be satisfied that the use of a Covert Human Intelligence Source is **necessary** and **proportionate**. Authorisations should be given in writing as described in paragraph 4.23 above and Authorising Officers should not be responsible for authorising their own activities e.g. acting as source or tasking a source save exceptionally where this would otherwise be unavoidable.

4.36 A central register of all authorisations will be held by the ~~Deputy Chief Executive~~ Director of Corporate Services on behalf of the Council and regularly updated whenever an authorisation is granted, renewed or cancelled. The central register will include records relating to the management of the CHIS. This register will be retained for a period of at least three years from the ending of the authorisation.

4.37 An application for the use or conduct of a source should record:

- details of the purpose for which the source will be tasked or deployed;
- the grounds on which authorisation is sought (e.g. for the purpose of preventing or detecting crime or preventing disorder);
- where a specific investigation or operation is involved, details of that investigation or operation;
- details of what the source will be tasked to do;
- details of the level of authority required (or recommended, where that is different);
- details of any potential collateral intrusion; and
- details of any confidential material that might be obtained as a consequence of the authorisation.

4.3~~8~~9 The conduct so authorised is any conduct that:

a) is comprised in any such activities involving conduct of a Covert Human Intelligence Source, or the use of a Covert Human Intelligence Source, as are specified or described in the authorisation;

b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a Covert Human Intelligence Source the authorisation relates; and

c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

4.39~~40~~ Nothing in RIPA prevents material obtained from the use or conduct of the source being used in evidence in Court proceedings. Existing Court discretion and procedure can protect, where appropriate, the disclosure of the source's identity.

4.4~~0~~1 The Authorising Officer must consider the safety and welfare of that source, and the foreseeable consequences to others of the tasks they are asked to carry out. A **risk assessment** should be carried out **before** authorisation is given. Consideration for the safety and welfare of the source, even after cancellation of the authorisation, should also be considered.

4.4~~1~~2 Before authorising the use or conduct of a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He/she should also take into account the risk of any collateral intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation. Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

4.4~~2~~3 Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

Records or copies of the following will be kept by the relevant service area and the originals should be sent to the ~~Deputy Chief Executive~~Director of Corporate Services:

- the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- any renewal of the authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;

- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a source.

4.43~~4~~ The records kept by the Council, by the ~~Deputy Chief Executive~~ Director of Corporate Services ~~and in the relevant department,~~ should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. An officer should be designated who will have responsibility for maintaining a record of the use made of the source.

4.44 The rules relating to confidential information are the same for CHIS and directed surveillance.

Status Drift

4.45 Officers should be careful to ensure individuals who are not a CHIS at the outset of an investigation become one through a process known as 'status drift'. A person may provide information initially about an individual and then be inadvertently asked to provide further information and in so doing operate and act as a CHIS. Any Officer who handles such a person should be aware of the risks to ensure status drift does not happen and be sufficiently aware to recognise if it may occur. Legal advice should be sought in circumstances where status drift may occur.

~~Application to a Justice of the Peace~~

~~4.46 Once the internal approval process has been completed and an authorisation has been granted an application must be made to the Magistrates Court for the approval or renewal of the authorisation. The officer who is undertaking the directed surveillance should contact the Assistant Director Legal Services who will arrange for a hearing in the Magistrates Court. The hearing will relate to the application for an order. The Assistant Director Legal Services will review the proposed authorisations taking account of the terms of any applicable guidance, the statutory provisions and this Policy. If the Assistant Director Legal Services is not satisfied with any aspect of the proposed authorisation he/she will refer the matter and authorisation to the Authorising Officer for re-consideration and review. The Assistant Director Legal Services will act as a control on the need for and terms of an authorisation. An authorisation should only be referred for judicial approval if the Assistant Director Legal Services is satisfied this is appropriate. The Assistant Director Legal Services will formally record his/her observations and approval or disapproval with proposed authorisations. The Assistant Director Legal Services will prepare the application for Judicial approval and the draft order for that approval. The Assistant Director Legal Services will provide copies of the application and a draft order to the officer who attends Court. The Assistant Director Legal Services will inform the officer concerned of the date of the hearing.~~

~~Ordinarily, the Assistant Director Legal Services will not be required to attend court but may do so on request. All officers who attend court should have the appropriate authorisation from the Council to appear in Court.~~

4.4~~6~~7 The Authorising Officer concerned should attend Court to substantiate the application for the order to the Justice of the Peace. The authorising officer should be aware of the circumstances of the application and be able to justify why the authorisation is considered to be necessary and proportionate. If the order is approved the Magistrate or Justice of the Peace will sign it. The original of the order should be provided to the Director of Corporate Services (in the capacity of ~~RIPA Monitoring Officer~~Senior Responsible Officer) for retention with the Council's central records. A copy of the order should be retained by the officer concerned.

4.4~~7~~8 The Government has issued guidance to local authorities on the Judicial approval process for RIPA and the crime threshold for covert Directed Surveillance or the use of a CHIS. The guidance contains the specimen form of the application for Judicial approval and the order made on such an application. The guidance is available on the Government website.

RIPA codes - GOV.UK

Management and Tasking of Sources

4.4~~8~~9 The Authorising Officer must ensure that satisfactory arrangements exist for the management of the source and for bringing to ~~his/her~~their attention any concerns about the personal circumstances of the source insofar as they might affect:

- the validity of the risk assessment;
- the proper conduct of the source operation; and
- the safety and welfare of the source.

Where such information is brought to the attention of the Authorising Officer, ~~he/she~~they shall determine whether or not the authorisations shall continue.

Use and Conduct of a Source

4.4~~9~~50 Authorisation for the use and conduct of a source is required prior to any tasking. Tasking is an assignment given to the source, asking him or her to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. It may involve the source infiltrating existing criminal activity in order to obtain that information.

4.5~~0~~1 A vulnerable person should only be authorised to act as a source in the most exceptional circumstances. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself/herself, or unable to protect himself against significant harm or exploitation. If a vulnerable individual is to be used as a source the authorisation has to be by the Chief Executive as Head of Paid Service or in his absence the Director of People and Place~~Finance~~. (see Annex A).

4.512 Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his/hertheir parents or any person who has parental responsibility for him/her. An appropriate adult must be present at meetings involving a source under 16 years of age. Before an authorisation is granted for the use of a source under 18 years of age a proper risk assessment must be carried out in relation to the nature and magnitude of risk of physical or psychological distress. The person considering the authorisation must be satisfied that the risks are identified and justified and that they have been properly explained to and understood by the source. It is recommended that advice from the Legal Section is taken in cases involving juveniles. Authorisations for juvenile sources will be granted by the Chief Executive as Head of Paid Service or in his absence the Director of Finance People and Place (see Annex A).

The duration of such an authorisation is one month instead of twelve months.

4.523 An authorisation for the use or conduct of a source may be granted where he/she believes it is necessary for one of the specified reasons, for the purpose of preventing and detecting crime or of preventing disorder. The Authorising Officer must believe that the authorised use or conduct of a source is proportionate to what is sought to be achieved by that use or conduct.

4.534 Responsibility for authorising the use or conduct of a source rests with the Authorising Officer and all authorisations require the personal authority of the Authorising Officer. Authorisations must be in writing. Authorising officers should not be responsible for authorising their own activities.

The application and authorisation process for CHIS must be completed on the relevant Form. All forms are accessible through the Government website (See Section 8).

4.54 Any authorisation, prior to it be being acted must be followed up by an application to the Magistrates Court for an order approving the authorisation.

Duration and Renewals

4.555 Authorisations lapse if they are not renewed:

- in 12 months from date of last renewal if it is for the conduct or use of a Covert Human Intelligence Source, or
- in all other cases (i.e. Directed Surveillance) 3 months from the date of their grant or latest renewal.

4.56 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms. However, for the conduct of a Covert Human Intelligence Source, a person should not renew unless a review has been carried out and that person has considered the results of the review. A review must cover what use has been made of the source, the tasks given to them and information obtained.

4.57 Regular reviews should be carried out of all authorisations which have been issued: it is for the Authorising Officer to determine the frequency of reviews to be carried out. Once a review has been conducted the result should be notified in writing to the ~~Deputy Chief Executive~~ Director of Corporate Services as the ~~Monitoring Officer~~Senior Responsible ~~in~~Officer in order that it may be recorded on the Central Register. In the case of CHIS authorisations, the review should include the use made of the source. In particular, reviews should be carried out frequently when it is likely that confidential material may be obtained or collateral intrusion may take place.

4.58 An authorisation may be renewed, before it expires. A renewal may be for up to a further 3 months (Directed Surveillance or, 12 months CHIS) if the Authorising Officer considers this to be necessary. An application for renewal, in the case of Directed Surveillance 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;
- the reasons why it is necessary to continue with the Directed Surveillance / use of the source;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- in the case of a CHIS the use made of the source since the date of the authorisation / renewal the tasks given to him and the information obtained from him; and
- the results of regular reviews of the investigation or operation.

4.59 ~~———~~Authorisations may be renewed more than once, if necessary, and the renewal should be kept / recorded as part of the central record of authorisations. Any renewal, prior to it be being acted must be followed up by an application to the Magistrates Court for an order approving the renewal.

Application to a Justice of the Peace

4.60 Once the internal approval process has been completed and an authorisation has been granted an application must be made to the Magistrates Court for the approval or renewal of the authorisation. The officer who is undertaking the directed surveillance should contact the Assistant Director Legal Services who will arrange for a hearing in the Magistrates Court. The hearing will relate to the application for an order. The Assistant Director Legal Services will review the proposed authorisations taking account of the terms of any applicable guidance, the statutory provisions and this Policy. If the Assistant Director Legal Services is not satisfied with any aspect of the proposed authorisation they will refer the matter and authorisation to the Authorising Officer for re-consideration and review. The Assistant Director Legal Services will act as a control on the need for and terms of an authorisation. An authorisation should only be referred for judicial approval if the Assistant Director Legal Services is satisfied this is appropriate. The Assistant Director Legal Services will formally record their observations and approval or

disapproval with proposed authorisations. The Assistant Director Legal Services will prepare the application for Judicial approval and the draft order for that approval. The Assistant Director Legal Services will provide copies of the application and a draft order to the officer who attends Court. The Assistant Director Legal Services will inform the officer concerned of the date of the hearing. Ordinarily, the Assistant Director Legal Services will not be required to attend court but may do so on request. All officers who attend court should have the appropriate authorisation from the Council to appear in Court.

Cancellations

4.6159 The Authorising Officer has a statutory duty to cancel an authorisation once satisfied that the criteria for authorisation of Directed Surveillance or the use or conduct of a source (as appropriate) are no longer satisfied (s45 RIPA) or the offence which is being investigated no longer meets the crime threshold. If the Authorising Officer is no longer available the task will fall on the person who has taken over the role of Authorising Officer.

4.620 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after Directed Surveillance activity is no longer necessary.

4.631 Authorisations for Directed Surveillance or CHIS are to be securely retained by the Authorising Officer, for a period of 3 years from the ending of the Authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, in accordance with established disclosure requirements (e.g. Civil Procedure Rules, Code of Practice under the Criminal Procedures and Investigations Act 1996) commensurate to any subsequent review. Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the ~~Business Unit~~ service should be disposed of in an appropriate manner (e.g. shredded).

4.642 Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by Directed Surveillance or through use of a CHIS which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.653 There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

Section 5

Implementation of the Guidance

5.1 It is essential to ensure that there is a consistent implementation of the corporate guidelines and policy relating to RIPA and thus in the application of the Act and the Codes of Practice. All members of staff who may need to seek an authorisation under RIPA should be aware of the legislation, the Codes of Practice and the Council's Corporate Guidance and Policy. Each ~~Deputy or~~ Assistant Director (which for the purposes of this section shall be deemed to include the IT ~~Services~~Shared Services Manager~~)~~ ~~will~~ ensure that members of staff have this awareness before engaging work which may give rise to the application of RIPA. The Corporate Guidance and Policy is available to all members of staff on Sharepoint.

Formatted: Font color: Auto

Formatted: Font color: Auto

5.2 The Council's Corporate Guidance Policy will be available so that there is public awareness of this issue and its application within the Council's departments.

5.3 Training has been and will continue to be provided to a number of the Council's Officers upon the Act. Members of staff should keep up to date on legislative changes through training opportunities or through the receipt of advice and guidance from the Legal Section. Periodic refresher training upon RIPA will be considered in connection with the review of this guidance and the application of RIPA in the Council's ~~department~~services~~s~~. Guidance is available on RIPA from the Legal Section.

5.4 ~~The Deputy Chief Executive as the RIPA Monitoring Officer is responsible for the oversight of the Policy and the application of the processes, training on RIPA and the maintenance of the Central Register.~~ Records relating to authorisations will be maintained within each Council ~~department~~service, as appropriate. All records relating to RIPA authorisations must be kept in the strictest confidence and accessible only on a strictly 'need to know' basis. The ~~Deputy Chief Executive~~ Director of Corporate Services is responsible for the safe keeping of the Central Register. Each ~~Deputy or~~ Assistant Director is responsible for ensuring, where relevant, that all records within ~~his/her~~their section relating to RIPA are kept safely and properly. Access to departmental records will be made available to the ~~Deputy Chief Executive~~Director of Corporate Services, Internal Audit and in relation to any inspection by the Investigatory Powers Commissioner's Office.

5.5 The ~~Deputy Chief Executive~~ Director of Corporate Services will undertake monitoring of the central and departmental records to ensure compliance with the Act, the Code of Practice and this Guidance and Policy. In addition the Council's Senior Auditor may undertake an audit of the Council's records to monitor compliance with the legislation, the Code of Practice and these guidelines.

5.6 Every Officer who is undertaking or conducting surveillance must do so within the constraints of the authorisation. Every outstanding surveillance authorisation must be reviewed on a monthly basis by the Authorising Officer and cancelled if there is no need for further surveillance. All Officers shall take responsibility for ensuring the propriety of their involvement in the application of surveillance activities.

5.7 Annex B provides a short statement of the key issues which an Authorising Officer must consider when determining whether to grant an authorisation. Annex C indicates the key issues to which an applicant for an authorisation must have regard in seeking an approval.

Section 6

Codes of Practice

6.1 There are Government codes of practice that expand on this guidance and copies are available on the Government website or on request from Legal Services.

6.2 The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, 'if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account'.

6.3 The Government's Codes of Practice and guidance on covert surveillance and the use of human intelligence sources are available on its website.

RIPA codes - GOV.UK

There is specific guidance for local authorities.

6.4 There is also a separate Procedures and Guidance document published by the former Office of Surveillance Commissioners in December 2016 available on the IPCO website
https://www.ipco.org.uk/docs/OSC%20Procedures%20&%20Guidance%20-%20%20July%202016.pdf

Section 7

Benefits of Obtaining Authorisation under the 2000 Act

7.1 Authorisation of surveillance and human intelligence sources

The RIPA states that:

- of authorisation confers entitlement to engage in a certain conduct; and
- the conduct is in accordance with the authorisation, then
- it shall be 'lawful for all purposes'.

However, the corollary is not true – i.e. if you do not obtain the RIPA authorisation it does not automatically make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). However, you cannot take advantage of any of the special RIPA benefits and that may entail that any enforcement action taken by the Council following unauthorised conduct they may sue the Council and claim compensation.

7.1 RIPA states that a person shall not be subject to any civil liability in relation to any conduct of ~~his/her~~their which:

a) is incidental to any conduct that is lawful by virtue of S27(1); and

b) is not itself conduct an authorisation or warrant for which is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

Section 8

Standard Forms

8.1 The standard forms are designed for use by all public authorities. The forms are consistent with the Code of Practice. Information should not be removed from the standard forms. The forms have been adapted to apply to the Council.

8.2 The forms are accessible from the Government website RIPA codes - GOV.UK

8.3 The forms relating to the approval of a Magistrate or Justice of the Peace are accessible on the Government website in the guidance to local authorities on the judicial approval process for RIPA.

Annex A

The employees who are designated to make authorisations for directed surveillance and covert human intelligence sources are:

Chief Officers:

- the Chief Executive
- the Director of ~~Finance~~People and Place

Assistant Directors are:

- ~~the Assistant Director Legal Services~~
- the Assistant Director ~~Revenues and Benefits~~Finance
- the Assistant Director Environmental Services

Employees designated to make authorisations for directed surveillance when knowledge of confidential information is likely to be acquired

The Chief Executive or, in his absence, the Director of ~~Finance~~ People and Place.

Employees designated to make authorisations for Covert Human Intelligence Sources when knowledge of confidential information is likely to be acquired or vulnerable individual or juvenile is to be used as a source

The Chief Executive or, in their ~~his~~ absence the Director of People and Place.~~Finance and the Assistant Director Legal Services~~

Any designated officer must have had training in the application of RIPA before making any authorisations.

Annex B

Authorising Officers and RIPA - Guidance on Key Issues

The Authorising Officer must consider each application for an authorisation. The application should be submitted on the form which is applicable to the particular circumstance concerned. The form should be duly completed by the applicant.

The onus is upon the Authorising Officer personally to be satisfied of the following matters:

1. The statutory ground as identified in the policy must exist;

2. An authorisation can only be granted to prevent or detect crime or to prevent disorder;

3. The Authorising Officer must properly consider the application and believe that the activities are proportionate to what is sought to be achieved by carrying them out. The activities must be considered to be necessary;

4. Consideration must be given to any risk of any collateral intrusion;

5. Regard must be had to any data protection implications; and

6. The crime threshold must be met.

The Authorising Officer should consider how often the authorisation requires to be reviewed and make a diary note of the review date. Consideration should be given as to when the authorisation should be cancelled and a diary note made to this effect.

The Authorising Officer should ensure that the applicant provides the authorisation and any renewal or cancellation to the ~~Deputy Chief Executive~~ Director of Corporate Services for inclusion upon the central register.

Annex C

Applicants for Authorisations - Key Issues for Consideration

The applicant must be satisfied that the authorisation is appropriate, that the statutory ground exists and that what is proposed is necessary and proportionate. The crime threshold should be met. The applicant must know the alleged offence which is being investigated.

The appropriate application form must be completed in its entirety and provided to ~~the appropriate~~ one of the designated Authorising Officers. ~~who, ordinarily, will be the Deputy or Assistant Director (which for the purposes of this section shall be deemed to include the IT Services Manager) of the service concerned. Reference should only be made to another person when the Deputy or Assistant Director is unavailable.~~

An authorisation should last for no longer than is necessary. An indication of the length of the authorisation should be established and justified.

A diary note should be made of any review, renewal or cancellation dates. The grant of the authorisation and any renewal or cancellation should be sent to the ~~Deputy Chief Executive~~ Director of Corporate Services for retention upon the central register. A copy should be retained.

If confidential information is likely to be acquired the application for authorisation must be submitted to the Chief Executive for approval.

The applicant must be satisfied that the authorisation is necessary to prevent or detect crime or to prevent disorder.

In order to obtain an authorisation it must be necessary to use covert surveillance and a proportionate response:

- to the mischief; and
- to the degree of intrusion of the target and any others.

All alternative means must be considered and have been discounted.