

Name of meeting: Cabinet
Date: 26 July 2016

Title of report: Proposals to update the Councils RIPA Policy

Is it likely to result in spending or saving £250k or more, or to have a significant effect on two or more electoral wards? If the answer is yes cabinet is taking a “key decision”	No
Is it in the Council’s Forward Plan? All forthcoming “key decisions” should have been included at least 6 weeks in advance in the Council’s Forward Plan of key decisions (produced monthly) unless an urgent decision is required.	No
Is it eligible for call in by Scrutiny?	Yes
Date signed off by Director & name Is it signed off by the Director of Resources? Is it signed off by the Assistant Director – Legal, Governance and Monitoring	David Smith – 13 July 2016 Yes Julie Muscroft – 13 July 2016
Cabinet member portfolio	Resources

Electoral [wards](#) affected: All
Ward councillors consulted: None

Public

1 Purpose of report

- 1.1 To brief the Executive on the use of the Regulation of Investigatory Powers Act 2000 and to seek approval to the adoption of an amended Regulation of Investigatory Powers Act 2000 (RIPA) Policy and Guidance document. The role of Cabinet in RIPA matters is to provide strategic oversight and to keep the Council’s use of surveillance under review.

2 Key points

- 2.1 The Council is subject to the requirements of RIPA which sets out how and when a local authority such as Kirklees Council, can use covert surveillance. The three types of surveillance regulated by RIPA are directed surveillance, the use of covert human intelligence sources (informants) and the obtaining of communications data (which does not include obtaining the content of any electronic communication). The Cabinet adopted the current RIPA Policy on 4 June 2013 and it sets out in detail how the requirements of RIPA were to be met.
- 2.2 Surveillance can only be authorised via RIPA where it is both necessary and proportionate to the aims to be achieved and the intrusion into other people's privacy which may result. Accordingly covert surveillance will only be appropriate where other options are not available. The Council cannot authorise "intrusive surveillance" which is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and it is most unlikely that the Council would wish to use a covert human intelligence source as part of any investigation unless a request was made by West Yorkshire Trading Standards Service.
- 2.3 The Council was inspected by the Office of the Surveillance Commissioners on 18 July 2013 in relation to its use of directed surveillance and of covert human intelligence sources. The Inspector's Report forms Appendix 1 to this report. The Report included the following as part of its conclusions - *"Overall Kirklees is a well performing Council in regard to its RIPA obligations. The officers interviewed impressed with their knowledge and dedication to achieving RIPA compliance. Those issues raised could largely be addressed by more regular training"*. The inspector found that virtually all the recommendations made following the previous inspection in March 2011 had been implemented, although he referred to the need for more detail in the records of the cancellations of authorisations. The inspector made a small number of recommendations for further amendments to the RIPA policy and guidance document primarily to reflect legislative changes and good practice. Unfortunately due to changes in personnel; the recommended changes to the policy have not been made. This oversight has not had any practical consequences for the Council as the number of RIPA authorisations sought during the period has been very small (five in total and none in the last two years) and all have all been made in compliance with the law and with the approval of the Court.
- 2.4 The draft RIPA Policy at Appendix 2 is intended to replace the RIPA Policy approved by Cabinet on 4 June 2013 and incorporates the

amendments recommended by the Office of the Surveillance Commissioners and includes a revised list of officers with responsibilities for RIPA. The list of main statutory documents relevant to the policy at page 3 has also been updated.

- 2.5 It should be noted that a new Investigatory Powers Bill is currently being considered by Parliament and therefore there may be a future review of how we use this kind of activity moving forwards.

3 The Recommendations of the Office of Surveillance Commissioners

3.1 The Inspector made the following recommendations:

- 3.1.1 To include refusals on the central record. Where an authorising officer refuses to grant an authorisation for surveillance the fact of the refusal and the reasons for it will be kept on the electronic record. This change has been implemented .
- 3.1.2 To address the weaknesses highlighted in the report by the establishment of a programme of regular refresher training and to ensure that such training addresses the management of covert human intelligence sources. Officers have attended training provided by West Yorkshire Police and West Yorkshire authorities respectively on RIPA and the use of covert human intelligence sources. Further training is planned.
- 3.1.3 To ensure that cancellations are adequately articulated. The Inspector wished there to be more detail in the records of cancellations of authorisations to show what had or had not been achieved via the surveillance authorised. The Council's authorising officers have been advised accordingly.
- 3.1.4 To raise RIPA awareness. The Inspector was concerned about the risk of officers, especially those having little resort to covert surveillance, unwittingly carrying out covert surveillance without RIPA authorisation. Officers will take steps to communicate this to managers and others within the Council. Further training of officers whose role may involve them in regulated activities is planned.
- 3.1.5 To reduce the number of Authorising Officers. The Inspector recommended a reduction to two authorising officers plus the Chief Executive and the Director of Resources [as the Senior Responsible Officer for RIPA] to reflect the limited number of applications being made. The Chief Executive is concerned that this may be too few for an organisation of the size of the Council and has suggested to the Office of the Surveillance Commissioners that three authorising officers

would be more appropriate. At the present time there is only one authorised officer in addition to the Chief Executive and Director of Resources, this is due to changes in the personnel. For this reason it is recommended below that the Chief Executive be given delegated authority to nominate officers to be authorising officers and to remove officers from the list of nominated authorising officers in the RIPA Policy and Guidance document. It will be then possible for the Chief Executive to appoint an additional officer if thought necessary (and subject to that person having had the requisite training).

- 3.1.6 To amend the Council's RIPA Policy and Guidance, which the Inspector endorsed as "*excellent guidance for practitioners in the use of RIPA*". A revised version of the Policy and Guidance, incorporating the recommended amendments, forms Appendix 2 to this report.

4 Implications for the Council

- 4.1 It is important that the Council's limited use of covert surveillance is in accordance with the RIPA regime. Failure to do so could lead to legal challenge and/or evidence gathered via unlawful surveillance being ruled inadmissible in legal proceedings.

5 Consultees and their opinions

- 5.1 The following have been consulted on the contents of this report and have approved them:

5.1.1 The Cabinet Member for Resources.

5.1.2 The Director of Resources, as the RIPA Director and Senior Responsible Officer.

5.1.3 The Assistant Director of Legal, Governance and Monitoring.

5.1.4 The Council's proposed Authorising Officers for RIPA.

6 Next steps

- 6.1 To comply with the recommendations of the Inspection Report as set out at paragraph 3.1 above.

7 Officer recommendations and reasons

- 7.1 That members note the steps being taken to implement the recommendations of the Office of the Surveillance Commissioners.

- 7.2 That members approve the adoption of the revised RIPA Policy and Guidance document as set out at Appendix 2.
- 7.2 That the Chief Executive be given delegated authority to nominate officers who are to be authorising officers for the purposes of the RIPA regime and to remove officers from the role of authorising officer.

8 Cabinet portfolio holder's recommendations

- 8.1 The cabinet portfolio holder supports the officer recommendation.

9 Contact officer and relevant papers

- 9.1 John Chapman , Interim Deputy Head of Legal Services and nominated RIPA Monitoring Officer

Telephone: 01484 221000

Internal: 77881

E-mail: john.chapman@kirkles.gov.uk

10 Assistant director responsible

- 10.1 Assistant Director for Legal, Governance and Monitoring.



Office of Surveillance
Commissioners

Chief Surveillance Commissioner,
Office of Surveillance Commissioners,
PO Box 29105,
London,
SW1V 1ZU.

18th July 2013.

**INSPECTION REPORT
KIRKLEES COUNCIL**

Inspection 18th July 2013
Inspector His Honour Norman Jones, QC.
Assistant Commissioner

Kirklees Metropolitan Borough Council.

1. Kirklees is a Metropolitan Borough in West Yorkshire covering 157.8 square miles with a population of 423,000. Kirklees Council is the local government administrative body for the Metropolitan Borough with Huddersfield its principal town housing the Council headquarters.
2. The Senior Corporate Management structure is lead by the Chief Executive, Mr. Adrian Lythgo who heads a team of five Directors who in turn are supported by Heads of Services.
3. The Council was last inspected for the OSC in March 2011 by Mr. Neil Smart, Surveillance Inspector.
4. Since my last visit to the Council in 2009 there has been a substantial reduction in the number of authorisations granted. Some fifty five had been granted in the period preceding my visit. At the time of Mr. Smart's visit that had reduced to eighteen and at this time that figure has been halved to nine. The Council may now be regarded as a limited user of RIPA. All were for *directed surveillance* and none for CHIS, none were for *confidential information* or used the *urgency* procedure or were self authorised.
5. The Senior Responsible Officer (SRO) for RIPA is Dr. David Smith, Director of Resources with responsibility for Legal and Governance. The RIPA Monitoring Officer is Mr. Dermot Pearson, Senior Legal Officer and solicitor. Whilst both officers were in office at the time of the last inspection in Dr. Smith's case that had been for one month and in Mr. Pearson'sS only a matter of a day or so.

6. Some five officers are currently nominated as Authorising Officers with the CEO responsible for authorising for *confidential information* and juvenile and vulnerable *CHIS*.
7. The address of the Council is The Civic Centre, 3 Market Street, Huddersfield, HD1 1WG.

Inspection.

8. Dr. Smith, Mr. Pearson and Mr. Dave Thomas, Head of Customer Services and Authorising Officer extended a warm welcome to Kirklees. Later they were joined by Ms. Louise Carter, Assistant Legal Officer and *RIPA* Record Keeper. All officers afforded their enthusiastic assistance which was much appreciated and each impressed with their familiarity with their role and understanding of the *RIPA* process.
9. The inspection was conducted by way of interview and discussion with the officers in a group during which a wide range of *RIPA* topics was explored. Thereafter an examination took place of the Central Record of Authorisations and a sample of four of the most recent applications/authorisations, reviews, renewals and cancellations. The inspection was completed by a discussion concerning the findings from that examination.

Examination of Documents

10. The Central Record of Authorisations is maintained on an electronic spreadsheet. It is compliant with the *Codes of Practice* and well maintained. However it has not been the practice to include refusals on the record, a deficiency which should be addressed. It is the responsibility of Ms. Carter to populate it with information extracted from submitted documents. It can be used as a tool of the *RIPA Monitoring Officer* to ensure that actions are completed in a timely manner.

See recommendation

11. One case was reported to the OSC as a breach during the previous period. The concern arose from the fact that the activity was one which the Council suspected fell outside the parameters of their normal activities and was more within that of the police. However in the circumstances it would not normally attract consideration as a breach. No action was taken by the OSC.
12. Two authorisations have been subjected to Magistrate's approval since the commencement of the *Protection of Freedoms Act 2012* and the *RIP(Directed Surveillance and CHIS)(Amendment)Order 2012, SI 2012/1500*. Both related to disruptive behaviour which was seriously criminal, namely using local government housing for the purposes of supplying drugs and prostitution. Both were approved by a single lay Magistrate.
13. Each authorisation was for the purpose of conducting surveillance by means of CCTV cameras and video recording equipment on the entrances to each address. The applications were of a high quality detailing the reasons for the application and the nature of the proposed surveillance. In each case the details were precise and in one supported by a photograph with the viewing angles clearly demonstrated. *Necessity and proportionality* were concisely but adequately articulated as was *collateral intrusion*. *Confidential information* was dealt with by a clear negative response. The only criticisms which could be made are that URNs were not entered on the documents, though they were on the Central Record, and

there was insufficient outline of the intelligence relied upon. The authorisations provided good detail of what was being authorised and in the earlier one (2012/004) of *necessity* and *proportionality*. The second (2012/005) failed to adequately articulate these issues. Review dates were set in both and a review carried out in one. Expiry dates were set from the date of authorisation and it should be noted that the duration of such authorisations now runs from the date of the Magistrate's approval. It was noted that both authorisations followed the best practice and were handwritten, as were all authorisations examined. Adequate summaries were provided for the Magistrate. The review would have benefitted from more detail and a fuller exposition of the continuing *proportionality* and *necessity*. A comment to the effect that the Authorising Officer was approving a continuation of the operation should have been supported by some reasoning rather than a comment that the decision had been taken following a conversation with the reviewing officer.

14. The two earlier authorisations examined requesting the installation of covert CCTV also related to instances of disorder though varying in type. One related to incidents of repeated human defaecation at night in a street. The intelligence provided in the application was limited and, although comments later in the *proportionality* box indicated with no detail some frequency and local concern, the box requiring the reasons for the application did not deal with those matters. On the basis of the content of the entries in those boxes proportionality may have been questioned. *Proportionality* and *necessity* were otherwise well considered as was *collateral intrusion* and *confidential information*. It was appropriately cancelled. The fourth authorisation relating to the usage of premises for prostitution was initially refused by the Authorising Officer with comments indicating his considerations at that time and inviting a resubmission when appropriately amended. This was not recorded in the Central Record although the document was filed. A resubmission with amendments was subsequently authorised. The application was in good form with sufficient detail of what was requested and good articulation of *proportionality* and *necessity*. The authorisation similarly was of adequate detail but deficient in its consideration of *proportionality* and *necessity*. Timing details were appropriate but a cancellation was lacking in detail about what had/had not been achieved.
15. Overall the quality was compliant with the legislation but attention should be paid in training to the issues raised, especially the requirement to fully articulate in the authorisations the considerations of the Authorising Officer relating to proportionality and necessity and the better detailing of cancellations, the latter being the subject of a recommendation in the last report (see paragraph 16.III below).

See recommendation

Previous Recommendations.

16. Mr. Smart made three recommendations in his previous report:

- I *RIPA training should be reviewed and focus on the issues of "painting the picture" as to why directed surveillance is required as a tactic, the documentation of an appropriate summary of supporting evidence, proportionality, confidential information and , in particular, what should be written on the RIPA forms including how an authorisation should be documented. The Council should also conduct a training needs analysis to ensure all staff engaged in RIPA processes receive the training they require for the roles they perform*

Following receipt of the report a debriefing meeting was held with all officers actively engaged with *RIPA*. The report was fully debated and all recommendations considered. The staff actively engaged with *RIPA* have subsequently been more closely identified and training provided by an external professional trainer who was invited to deal specifically with these issues. This recommendation has been discharged.

- II *A formal oversight process should be established recording the process and matters identified on a simple spreadsheet to enable analysis of issues over the year and the result. It is important that issues identified in the oversight process generate remedial action where required and in addition are fed into RIPA training to ensure others have the benefit of learning. A formalised process should also be established to ensure the Senior Responsible Officer is able to fulfil the role described in paragraph 3.29 of the Code of Practice for Covert Surveillance and Property Interference.*

A computerised spreadsheet has been adopted (see paragraph 10 above). The new Magistrates' procedure enforces the requirement for immediate oversight of the authorisation by the *RIPA Monitoring Officer* prior to submission for Magistrate's approval. In the event of documentation appearing to the *RIPA Monitoring Officer* to be sub standard the document is referred back to the Authorising Officer for reconsideration. That has been done twice recently. The SRO considered these processes with the *RIPA Monitoring Officer*. The SRO, who had been in post only one month at the time of the last inspection, has since received training from the *RIPA Monitoring Officer* and is well aware of his role as set out in the *Codes of Practice* and in the Council's *RIPA Policy and Guidance* document. He discusses *RIPA* issues with the *RIPA Monitoring Officer*, has examined specific cases, discussed issues with the West Yorkshire Trading Standards Service (WYTSS), considers *RIPA* policy and liaises with Elected Members. This recommendation has been discharged.

- III *The Council must ensure that authorisations are cancelled as soon as they are no longer required, and contain details of what surveillance activity was conducted, the reason for the cancellation, confirmation that equipment has been removed, give an account as to how the surveillance has assisted the investigation i.e have the objectives been achieved and the authorising officer provide direction for the management of the product.*

This recommendation was considered during the review of recent authorisations. (see paragraphs 13 and 14 above). Whilst cancellations are now effected timeously they are regularly not considered in the detail required and this issue remains to be addressed. This recommendation has been partially discharged.

See recommendation

RIPA Management

17. Since shortly before the last inspection there has been a substantial change in the management of *CHIS* and of the Authorising Officers. The former is spoken to above and the latter below under **Authorising Officers**. The process of

departmental authorisation has been abandoned for a more centralised and independent process based on fewer Authorising Officers. The *RIPA Co-ordinating Officer* has his responsibilities outlined in considerable detail in the *Procedures and Guidance* and has readily assimilated the role. It would be advisable to add to it the responsibility for ensuring *RIPA* awareness throughout the Council. The *RIPA Monitoring Officer* carries out some training himself and otherwise arranges for external training. He exercises oversight as described earlier in this report

18. A prime concern for all Councils, especially those having little resort to covert surveillance, is the risk of officers unwittingly carrying out such surveillance without authorisation. This requires a high degree of *RIPA* awareness throughout Councils. Kirklees has addressed this problem partly by assessing the degree of unawareness existing through the process of audit by the Audit Department and the inviting to training a limited number of officers from unlikely *RIPA* user departments. The feeling overall was that there was a low risk of such surveillance occurring. However it would be advisable to spread the information on as wide a scale as possible and suggestions were made to effect efficient cascading down of information from management meetings and the using of the Council's intranet to advertise the risks and identify the *SRO* and *RIPA Monitoring Officer* as officers to contact when in doubt

See recommendation

Authorising Officers

19. Since the last inspection when there were eight, there has been a further reduction in numbers of Authorising Officers (see paragraph 6 above). It is anticipated that one effect of the *Protection of Freedoms Act 2012* will be some further limited reduction in the number of applications made. At the present time the authorisations process is centralised and mainly concentrated on Mr. Thompson. It was readily appreciated that some Authorising Officers are not undertaking any authorisations and that the number could therefore be reduced further. During discussion that number was considered. There is a necessity to cover the usual contingencies and in those circumstances it was felt that two regular Authorising Officers would be sufficient. Dr. Smith, as *SRO*, should be an Authorising Officer but should only authorise in exceptional circumstances. The CEO and whoever may deputise for him in his absence, if not Dr Smith, should authorise the sensitive applications. All Authorising Officers must be trained to the requisite standard and it was encouraging to note that at Kirklees Council if an Authorising Officer fails to attend training s/he is not permitted to authorise until having done so.

See recommendation

Training

20. Kirklees does not have a *RIPA* training programme. Instead it has relied on a process of external training at intervals of about three years. Whilst such training is highly commendable there is a need to constantly keep officers refreshed, especially when the usage of *RIPA* is low. At present this is sought to be achieved by a *ad hoc* process of the *RIPA Monitoring Officer* providing training when he perceives a weakness occurring. It would be better addressed by establishing a corporate form of internal training provided by the *RIPA Co-ordinating Officer* or other member of the legal staff at intervals of 12/18 months. Authorising Officers and those likely to be applicants should be obliged to attend

or independently be provided with the training. It could be supported by the simple process of a PowerPoint presentation. By this system officers would be reminded of issues such as those presenting in the authorisations examined.

21. Consideration was given to the likely usage of CHIS by the Council. It has never authorised such and the officers considered it was unlikely to do so. Some circumstances which may require their employment were debated. These included the unexpected CHIS who suddenly present him/herself and the Council's duty requires it to employ him/her. The position of Social Networking Sites was also considered in this regard (see SNS below). At the present time the Council does not have trained controllers or handlers and this should be addressed by future training. It is noted that it is the Council policy that all CHIS authorisations must be by the CEO. It would be anticipated that any officer considering such an application would first speak to the *RIPA Monitoring Officer*

See recommendation

Social Networking Sites

22. The investigation of sites such as "Facebook" was considered. At the present time the Council does not hold a Facebook" or other SNS account for operational purposes. However accounts are held for public relations purposes. The Council has no proposal for engaging such methods but it is an issue which may arise in relation to WYTSS in the future, for whom the Council provides authorisation for operations undertaken in its area. It should also be observed that usage for housing benefit fraud may arise. In such cases the exploration of sites within the publicly available pages, "open source material", cannot be considered as requiring authorisation even if conducted using a covert account. However the progress beyond into areas requiring entry through privacy controls (becoming a friend) are likely to require *directed surveillance* authorisation if a covert account is used. Further progress involving the setting up of a contact personally with the account holder/operator is likely to result in the establishment of a "relationship" which would require CHIS authorisations and the statutory management by a controller and handler.

Protection of Freedoms Act 2012

RIP(Directed Surveillance and CHIS)(Amendment)Order 2012, SI 2012/1500

23. This legislation commenced on the 1st November 2012 and the first application in Kirklees was made to the Magistrates on the 12th. November. As remarked above it was of good quality though the second which followed about two weeks later could have been improved in some areas. The legislation is likely to have some effect on the number of authorisations. Its major provisions are fully appreciated by the *RIPA* officers though one or two issues were drawn to their attention. In particular that the provisions for oral *urgency* are no longer available to the Council (See *Protection of Freedoms Act 2012, Schedule 9(9)(2)*) and that the period of duration commences at the date of the Magistrate's approval. *Protection of Freedoms Act 2012, Schedule 9(9)(3)*. It should be noted that most occasions when *urgency* has been used the provisions of *Section 26(2)(c) of RIPA*, the "immediate response" provisions, would have been available.
24. The appearance before the Magistrate was attended by the investigating officer and the *RIPA Co-ordinating Officer*. The investigating officer was sworn and some questions were posed by the Magistrate of which notes were taken, and which were closely pertinent to the application. Care must be taken to ensure that the investigating officer is competent to ask any questions posed. If questions are directly relevant to Authorising Officer considerations then that officer should give

the required evidence. It must be borne in mind that the application should be self standing and therefore of a quality which does not require further oral exposition.

25. The Council had established a liaison with the Magistrates' Court before the Home Office Guidance had been released. This has assisted in making convenient arrangements for hearings.

Policy and Procedures

26. The *RIPA* policy and procedures of the Council are to be found in the *Policy and Guidance on RIPA*. Mr. Smart observed in his report that it was "excellent guidance for practitioners on the use of *RIPA*" an observation which commands endorsement from this inspection. It is concise, succinct and easily assimilated. It drew from Mr. Thomas the accolade that he never grants an authorisation without having it by his side. It has been suitably amended to accommodate the recent legislation. Only four further amendments are suggested:

- Remove references to *urgency* authorisations and replace with a note indicating that such is no longer available.
- Add reviews to the list of items required for the Central Record. (However it is noted that the Central Record does already accord with this requirement).
- Add the raising of *RIPA* awareness to the *RIPA Monitoring Officer* responsibilities.
- Amend Appendix 6 concerning ASB to reflect the effect of the removal of "disorder" from the grounds available to the Council for *directed surveillance* and the provisions of *RIP(Directed Surveillance and CHIS)(Amendment)Order 2012, SI 2012/1500*. (note that only offending within the parameters of 2012/1500 is embraced by this and that there are offences of violence, disorder and harassment which fall outside)

See recommendation

CCTV

27. The process is as it was at the last inspection. No protocol has been agreed with the WY Police on the provision of a redacted authorisation before use of the equipment. A form exists which requires completion by the police with the details of the authorisation relied upon to enable the CCTV Manager to assess whether the surveillance undertaken complies with the authorisation. Correctly completed this is, in effect, the same as a redacted authorisation. It suffers from the defects that it does not identify the authorisation by its URN nor does it bear the signature of an officer confirming on behalf of the WY Police that the details conform to the authorisation. This whole problem could be resolved if agreement could be achieved, as it is in many other parts of the country, that the police supply an appropriately redacted copy of the authorisation to be filed at the CCTV Control Centre.
28. Ultimately it should be borne in mind that, whilst the Council is desirous of assisting the police, the equipment nevertheless belongs to the Council and it is entirely the decision of the Council whether it is made available to the police. It is therefore for the Council to determine the conditions upon which this assistance will be provided.

Elected Members

29. As required by the *Codes of Practice* Councillors receive annual and quarterly reports of covert surveillance activity. It must be remembered that it is important to keep Elected Members informed when no *RIPA* authorisations have been granted as well as when they have been.

Other Issues

30. It was noted that the forms in use are Home Officer forms updated with prompts relating to the *Protection of Freedoms Act 2012*.
31. The use of *RIPA* for internal Council investigations was considered together with *C v The Police and Secretary of state for the Home Office*. The Council were advised in accordance with the *Code of Practice for Covert Surveillance and Property Interference*, 2.26.
32. The use of unauthorised covert surveillance with the Council's approval in cases falling outside of *RIPA* was discussed in the context of the Council using a *RIPA* type system of "authorisation." This would be designed to demonstrate that the Council had applied Human Rights considerations to the decision to take such action. It was pointed out that the provisions of the *Protection of Freedoms Act 2012* and the *RIP(Directed Surveillance and CHIS)(Amendment)Order 2012, SI 2012/1500* were designed to limit local authority use of covert surveillance and that that consideration would be in the mind of any court or tribunal considering "authorisations" of this type, though it was appreciated that some local authorities did employ such means. In effect if this was done the Council must take its chances before the court or tribunal.

West Yorkshire Trading Standards Service.

33. Trading Standards powers within West Yorkshire are devolved by the five Metropolitan District Councils (Bradford, Calderdale, Kirklees, Leeds and Wakefield) to a Joint Services body, the West Yorkshire Trading Standards Service. The lead Council is Wakefield and each authority pays a contribution to Wakefield for the support of the Service. Wakefield is responsible for the payment of staff.
34. Mr. Mullins attended at the Bradford inspection to deal with Trading Standard issues relating to Bradford MDC. The opportunity was taken at this meeting, and a further meeting which he attended on the next day at the Wakefield Council inspection, to address Trading Standard issues which affected all five of the regional councils. This attendance would therefore avoid Mr. Mullins having to attend at each Council being inspected during this period. It follows that certain paragraphs of each report will be common to each other.
35. At the time of the last round of inspections of West Yorkshire Councils particular attention was paid to the position of the West Yorkshire Trading Standards Service. Comment was made in the report that the Service was operating in a manner appropriate for a local authority which was included within the schedule of such authorities for the purposes of *RIPA* when, in effect, the Service did not hold such status. Since that time the Service has given consideration to its position and has recognised the force of those observations, not least because it would mean that each

authorisation granted under the regime would fail to be compliant with *RIPA* and, if subjected to challenge in a courtroom, would undoubtedly fail to satisfy a judge.

36. Although it is somewhat regrettable that it took so long, nevertheless since November 2012 the Service has adopted a practice of seeking authorisation from an Authorising Officer of the Council in whose area the investigation requiring authorisation is being undertaken. Authorised investigations are therefore undertaken by the WYTSS acting as agent for that Council. Original authorisations are lodged with the Central Record of that Council and details are recorded within the Central Record. The Council will be responsible for ensuring that reviews, renewals and cancellations are appropriately undertaken. This ensures compliance with the legislation and the authenticity of authorised covert surveillance operations undertaken by the WYTSS.
37. One previous *directed surveillance* "authorisation" had been granted in 2010 for an operation in Kirklees and was therefore under the regime which prevailed at that time. It related to the surveillance of a petrol pump, which had been ordered to close on inspection by TS officers, to ascertain whether it was still in use. Granted under the provisions of preventing or detecting crime or preventing disorder it was questionable whether it was proportionate and whether other means could have been used, eg ascertaining if the fuel levels went down by dipping. Both the application and the authorisation were poorly constructed with no real detail of how observations were to be undertaken. Neither *necessity* nor *proportionality* was appropriately articulated - failing to address any of the essential elements, no review date was set and the expiry date was incorrect. It was appropriately cancelled but would not have been approved by the Magistrates.
38. It is fair to remark that this "authorisation" was undertaken before training was afforded to the Service by Mr. Richard Winter of Bradford City Council following the last inspection.
39. An excellent *RIPA Policy and Procedures to Obtain Authorisations* has been produced for the Service which was revised as recently as April 2013. It is concise and contains all that is necessary to guide officers seeking *RIPA* authorisation. It outlines procedures which include oversight procedures which lead to the authorisation by an Authorising Officer of the relevant Council where the investigation is to take place and thereafter to the obtaining of Magistrate's approval. The only amendment required is to remove reference to oral *urgency* applications which are no longer available to Local Authorities.

See recommendation

40. The WYTSS does monitor websites for the sale of counterfeit and illegal goods. However it only examines public page sites and uses information gained as a basis for investigation. The WYTSS does not have a ghost website or a covert Facebook account. It does have an overt Facebook account and information gleaned through it or from websites normally stimulates a warning letter being sent to the account holder. Any information requiring a deeper investigation would be reported to the Regional Trading Standards Service. WYTSS staff are aware of the pitfalls involved in the covert investigation of SNS and of having entered pages through privacy controls. Staff are aware that they must not set up relationships in their investigation of sites. Discussion did lead to some concern as to whether there was a full appreciation that an entry through privacy controls may in any event require a *directed surveillance* authorisation. It is appreciated that if the Service expands its operation in SNS to the extent that relationships are formed and *CHIS* authorisations are granted then the *CHIS* will need to be managed in accordance with *RIPA* requirements, namely by a controller and a handler with a full record being maintained.

See recommendation

Conclusions

Kirklees Council

41. Overall Kirklees is a well performing Council in regard to its *RIPA* obligations. The officers interviewed impressed with their knowledge and dedication to achieving *RIPA* compliance. Those issues raised could largely be addressed by more regular training.
42. Virtually all of the recommendations of the last report were fully discharged, though that relating to detail in cancellations requires to be further addressed.
43. The proposed further reduction in the number of Authorising Officers coupled, with the already existing centralisation of the authorisation process, can only lead to heightened efficiency.

WYTSS

44. The practices of the Service in relation to *RIPA* have recently shown a substantial improvement following the acceptance of the status of the Service and the adoption of an authorisation procedure which accords with the legislation.
45. The WYTSS is a limited user of covert surveillance within the region with its largest activity in the Leeds area. This situation is unlikely to change unless there is a dramatic increase in the investigation of counterfeit sales and other illicit goods through SNS.

Recommendations

46. Kirklees Council

- I Include refusals on the Central Record. (*Paragraph 10*)
- II Address the weaknesses highlighted in this report by the establishment of a programme of regular refresher training and ensure that such training addresses the management of *CHIS*. (*Paragraph 13-15, 20 and 21*)
- III Ensure that cancellations are adequately articulated. (*Paragraph 13-15 and 16.III.*)
- IV Raise *RIPA* awareness. (*Paragraph 18*)
- V Reduce the number of Authorising Officers. (*Paragraph 19*)
- VI Amend the Council's *Policy and Guidance for RIPA*. (*Paragraph 26*)

WYTSS

- I Amend the *WYTSS Procedure to Obtain Authorisations* to delete the reference to *urgency*. (*Paragraph 39*).
- II Ensure that officers are equipped to undertake and manage Social Networking Site investigations in accordance with *RIPA* requirements if and when authorisation for such is obtained. (*Paragraph 40*).

**His Honour Norman Jones, QC.
Assistant Surveillance Commissioner.**

**KIRKLEES COUNCIL
POLICY AND GUIDANCE ON**

**THE REGULATION OF
INVESTIGATORY POWERS ACT 2000
(RIPA)**

CONTENTS

Title	Page
Introduction	3
The Office of the Surveillance Commissioners (OSC) and the Interception of Communications Commissioner's Office (IOCCO)	7
The Role of Elected Members	7
The Use of Home Office Forms	7
Who Can Authorise Surveillance?	7
When Can Covert Surveillance Be Authorised?	7
Review of Authorisations	8
Confidential Information	9
What Steps Must Be Followed in Authorising Covert Surveillance?	9
Duration of Authorisations	10
The Keeping of Records	11
Retention and Destruction of Materials	12
The Roles of RIPA Officers	12
APPENDICES	
Appendix 1 List of Officers Responsible for RIPA and List of Authorising Officers	13
Appendix 2 Flowchart	15
Appendix 3 Duties of Authorising Officers	16
Appendix 4 Duties of Officers in Charge of Investigations	18
Appendix 5 Management of Covert Human Intelligence Sources	19
Appendix 6 Policy statement	22
Appendix 7 RIPA And Anti-Social Behaviour Enforcement	24
Appendix 8 Communications Data	26

Introduction

The Regulation of Investigatory Powers Act (RIPA) controls and regulates surveillance, and other means of gathering information, which public bodies employ in the discharge of their functions. Information gathering is one of the Council's many activities which could involve an interference with an individual's human rights, specifically an individual's rights under Article 8 of the European Convention on Human Rights to respect for his private and family life, his home and his correspondence. RIPA provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. The Home Office has issued Codes of Practice under RIPA which provide further guidance.

RIPA provides a statutory authorisation process for certain types of surveillance and information gathering. The Council may be required to justify, by reference to RIPA and the relevant Codes of Practice, the use or granting of authorisations in general or the failure to use or grant authorisations. No authorisation, renewal or notice issued by an authorising officer can take effect without judicial approval from a Justice of the Peace (magistrate). A failure to apply RIPA and the Codes of Practice in an appropriate manner may be considered by the courts in deciding whether material obtained via surveillance should be admissible in evidence or whether an individual's human rights have been infringed.

Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a Covert Human Intelligence Source (CHIS) do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by the Council (e.g. one party to a relationship having a covert purpose on behalf of the Council) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

The following are the main statutory documents relevant to this policy document:

- Regulation of Investigatory Powers Act 2000 (RIPA)
- Part II of the Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012
- Covert Surveillance and Property Interference Revised Code of Practice (2010)
- Covert Human Intelligence Sources Code of Practice (2014)
- Acquisition and Disclosure of Communications Data Code of Practice (2007) (This code does not relate to the interception of communications nor to the acquisition or disclosure of the contents of communications)

These Codes of Practice, along with the text of RIPA and copies of approved forms are available on the Home Office website or from Legal and Governance. This document reproduces material from the Codes of Practice.

The following terms are defined in RIPA and the definitions are summarised in the relevant Codes of Practice as follows:

“surveillance”

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

“directed surveillance”	Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of <i>private information</i> about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek <i>authorisation</i> under RIPA)
“intrusive surveillance”	Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device). The Council cannot authorise intrusive surveillance.
“interference with property or wireless telegraphy”	There is a procedure for obtaining authorisation for interference with property or wireless telegraphy set out in the Police Act 1997 to enable the maintaining or retrieving of any equipment, apparatus or device whose placing or use has been authorised under RIPA. This procedure is available to the Police and other agencies but is NOT available to the Council and advice should be sought immediately from the RIPA Monitoring Officer if any proposed surveillance by the Council might involve any act of trespass.
“covert human intelligence source ”	<p>a person is a CHIS if:</p> <ul style="list-style-type: none"> a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c); b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. <p>NB It is most unlikely that the Council would wish to use a CHIS for surveillance purposes.</p>
“private information”	Private information is any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person’s private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation

“collateral intrusion”	Collateral intrusion is the risk of obtaining private information about persons who are not subjects of the surveillance
“communications data”	<p>The term ‘communications data’ embraces the ‘who’, ‘when’ and ‘where’ of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of ‘dial through’ fraud and other crimes where data is passed on to activate communications equipment in order to obtain communications services fraudulently)</p> <p>NB The only form of communications data which the Council is ever likely to wish to obtain is the identity of individuals who are the subscribers for particular telephone numbers. To date the Council had not sought to obtain communications data.</p>
“subscriber information”	Subscriber information relates to information held or obtained by a Communications Service Provider about persons to whom the Communications Service Provider provides or has provided a communications service
“Confidential information”	Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material.
“Confidential personal Information”	Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.
“Confidential constituent Information”	Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters
“Confidential journalistic Material”	Confidential constituent information 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

“Legal privilege”

Legal privilege relates to communications between a lawyer and a client for the purposes of obtaining legal advice or conducting litigation but does not include communications made with the intention of furthering a criminal purpose

RIPA regulates the use of covert surveillance which consists of directed surveillance, intrusive surveillance, the conduct and use of covert human intelligence sources and the acquisition of communications data. Local authorities such as the Council can only authorise the use directed surveillance if:

- The authorisation is for the purpose of preventing or detecting conduct which constitutes one or more criminal offences; and
- The criminal offence or one of the criminal offences would be either –
 - Punishable, whether on summary conviction (in the magistrates’ court) or on indictment (in the Crown Court), by a maximum term of at least 6 months of imprisonment; or
 - Is an offence under:
 - section 146 of the Licensing Act 2003(2) (sale of alcohol to children);
 - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
 - section 147A of the Licensing Act 2003(3) (persistently selling alcohol to children);
 - section 7 of the Children and Young Persons Act 1933(4) (sale of tobacco, etc, to persons under eighteen).”.

Local authorities such as the Council can only authorise the use of CHIS or the acquisition of communications data if *“for the purpose of preventing or detecting crime or the preventing of disorder”*

Where covert surveillance activities are unlikely to result in the obtaining of private information about a person, or where there is a separate legal basis for such activities, neither RIPA nor the relevant Code of Practice code need apply, but there is an assumption that intrusive surveillance will involve the obtaining of private information. It is important to distinguish between the types of surveillance and information gathering regulated by RIPA, and normal general observation, in the course of discharging the Council’s functions. It is acknowledged that low-level general observation will not usually be regulated under the provisions of RIPA. The relevant Code of Practice gives the following examples of this kind of general observation:

- patrolling to prevent and detect crime,
- review of images gathered by overt CCTV after the event to help identify the perpetrators of crime (however the use of such systems in a pre-planned manner to target a particular individual or group may require authorisation)
- officers attending a car boot sale where it is suspected that counterfeit goods are being sold, but where the intention is, through reactive “policing”, to identify and tackle offenders.

The Office of the Surveillance Commissioners (OSC) and the Interception of Communications Commissioner's Office (IOCCO)

The OSC is one of the statutory regulators for RIPA. The OSC's aim is to provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities. This includes inspecting public authorities and publishing reports on their compliance with RIPA. The most recent report on the Council by OSC can be obtained from Legal and Governance. The regulator in respect of the acquisition of communications data is the Interception of Communications Commissioner's Office (IOCCO).

The Role of Elected Members

Cabinet should review the authority's use of RIPA and set the policy at least once a year. They should also consider internal reports on use of RIPA on at least a quarterly basis to ensure that it is being used consistently with the Council's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

The Use of Home Office Forms

The forms which should be used in authorising, renewing, reviewing and cancelling surveillance are available via the RIPA part of the Home Office website. They are not reproduced as part of this document in order to avoid the use of out of date forms. Until the Home Office issue a revised form in relation to Directed Surveillance incorporating the requirements of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 the RIPA Monitoring Officer will circulate a form to Authorising Officers for use in authorising directed surveillance.

Who Can Authorise Surveillance?

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 permits the following officers within a local authority to grant authorisations - "Director, Head of Service, Service Manager or equivalent". The Council officers who can authorise directed surveillance and CHIS are set out in Appendix 1.

There are specific reporting requirements for confidential information and the OSC must be advised whether confidential information has been acquired and if so it must be made available to the inspector. In any case where confidential information is likely to be acquired advice should always be sought from the RIPA Monitoring Officer.

When Can Covert Surveillance Be Authorised?

The only specified ground upon which the Council can grant an authorisation is preventing or detecting crime or preventing disorder. There are no other grounds available to local authorities.

RIPA stipulates that the person granting an authorisation for directed or intrusive surveillance must believe that the activities to be authorised are necessary *for the purpose of preventing or detecting crime or of preventing disorder*.

If the activities are deemed necessary on this ground, the person granting the authorisation must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the

subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all those involved in undertaking directed or intrusive surveillance activities under RIPA are fully aware of the extent and limits of the authorisation in question.

All applications should include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria.

Judicial Authority

As above no authorisation, renewal or notice issued by an authorising officer can take effect without judicial approval from a Justice of the Peace (magistrate). Applications for Judicial Authority are the responsibility of the RIPA Monitoring Officer. The Home Office guidance suggests that investigating officers may be authorised to present such applications to the magistrates and such authorisation would be a matter for the RIPA Assistant Director.

Review of Authorisations

Regular reviews of all authorisations should be undertaken to assess the need for the surveillance activity to continue. The results of a review should be retained for at least three years. Particular attention is drawn to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

In each case the frequency of reviews should be considered at the outset by the authorising officer. This should be as frequently as is considered necessary and practicable. Any proposed or unforeseen changes to the nature or extent of the surveillance operation that

may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

Confidential Information

Special consideration must also be given to authorisations that involve confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the OSC during the next inspection and the material be made available to him if requested. It is not anticipated that the Council would wish to engage in surveillance which would involve confidential information but if it did, only the Chief Executive could authorise the surveillance.

What Steps Must Be Followed in Authorising Covert Surveillance?

Responsibility for authorising the carrying out of directed surveillance rests with the authorising officer and requires the personal authority of the authorising officer.

The Code of Practice on Covert Surveillance and Property Interference refers to authorisations being granted verbally in urgent cases and records being made as soon as reasonably practicable but this procedure is NO LONGER AVAILABLE to the Council as it is incompatible with the requirements for obtaining judicial authority.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved

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

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

Duration of Authorisations

A written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time at which it took effect.

Renewal of Authorisations

If, at any time before a directed surveillance authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months but such authorisations do not take effect until judicial authority is granted by the Magistrates' Court. 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. All applications for the renewal of a directed surveillance authorisation should record (at the time of application):

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

Authorisations may be renewed more than once, if necessary and provided they continue to meet the criteria for authorisation. The details of any renewal should be centrally recorded.

As above, for any renewal of an authorisation to take effect judicial authority must be obtained.

Cancellation of Authorisations

During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. They must cancel the authorisation if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer.

As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. However effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

The Keeping of Records

A record of the following information pertaining to all authorisations shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the OSC upon request.

- the type of authorisation;
- the date the authorisation was given;
- name and job title 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 subjects, if known;
- The date of any review and the details of the decision made.
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and job title of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled.

The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- 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 over 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;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the authorising officer.
- The order of the magistrates' court granting judicial authority for the surveillance, including judicial authority for the renewal of authorisations, or any such order refusing authority.

The written records of every directed surveillance and CHIS authorisation, review, renewal, refusal or cancellation must be sent to the RIPA Monitoring Officer for inclusion in the Central Record, which will be made available to the OSC upon request. It is the responsibility of all Authorising Officers to ensure that the RIPA Monitoring Officer receives the relevant forms within 7 days of refusal, authorisation, review, renewal or cancellation.

Retention and Destruction of Materials

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by the Council relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review. There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations

Where surveillance is being carried out as part of a criminal investigation officers are reminded of the requirements of the Code of Practice issued under the Criminal Procedure And Investigations Act 1996.

The Roles of RIPA Officers

The Director of Resources is the Senior Responsible Officer and is responsible for:

- the integrity of the process in place within the Council to authorise directed surveillance, the management of CHIS and the acquisition of communications data;
- compliance with RIPA, the Code of Practice on Covert Surveillance and Property Interference, the Code of Practice on Covert Human Intelligence Sources and the Code of Practice on Acquisition and Disclosure of Communications Data;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

The Assistant Director with responsibility for supporting the Senior Responsible Officer is the Assistant Director for Legal, Governance and Monitoring and is referred to as the RIPA Assistant Director.

The RIPA Monitoring Officer is the solicitor within Legal, Governance and Monitoring responsible for advising the Senior Responsible Officer and the Council upon RIPA issues and for providing day to day advice and support to investigating and authorising officers. The RIPA Monitoring Officer will:

- Take steps to raise awareness of the requirements of RIPA across the Council
- maintain a central record of all directed surveillance operations
- monitor the quality of authorisation, review, renewal and cancellation forms
- raise issues as necessary with the Applicant Officer, the Authorising Officers and/or the Senior Responsible Officer as relevant
- return an application for authorisation to the relevant Authorising Officer for further information if deemed appropriate as a result of the information on the form
- keep the Senior Responsible Officer informed about the Council's conduct of directed surveillance and compliance with the law and relevant codes of practice, etc
- act as the contact point for any enquiries from the Office of the Surveillance Commissioners
- provide first line advice to those involved in covert surveillance
- ensure that all areas which may undertake directed surveillance operations are familiar with the RIPA legislation and codes of practice and the Council's Policy and Code of Practice
- in conjunction with the RIPA Legal Advisers, may carry out spot checks on any forms/activity from department to department, or may visit departments to check knowledge of RIPA.
- provide or arrange RIPA training, awareness raising, briefing notes and other corporate

communications as necessary

- be responsible for applications to the magistrates' court for judicial authority

Overall responsibility for each directed surveillance operation will lie with the Authorising Officer in charge of the operation. Officers who authorise directed surveillance are responsible for granting, reviewing, renewing and cancelling authorisations. Corporate responsibility for monitoring the use of covert surveillance rests with the Senior Responsible Officer.

The RIPA Monitoring Officer in conjunction with the Senior Responsible Officer will ensure that relevant members of staff are suitably trained as applicants for RIPA authorisations and as authorising officers, as well as ensuring that relevant departments are kept informed of any significant changes in RIPA.

The Council's Internal Audit service will review this area of work when requested to do so by the RIPA Monitoring Officer.

APPENDIX 1

LIST OF OFFICERS RESPONSIBLE FOR RIPA DUTIES

Senior Responsible Officer	David Smith (Director of Resources)
RIPA Assistant Director	Julie Muscroft (Assistant Director (Legal, Governance and Monitoring))
RIPA Monitoring Officer	John Chapman (Interim Deputy Head of Legal Services)
RIPA Legal Advisors	Samantha Lawton (Senior Legal Officer) Louise Carter (Assistant Legal Officer)

LIST OF AUTHORISING OFFICERS

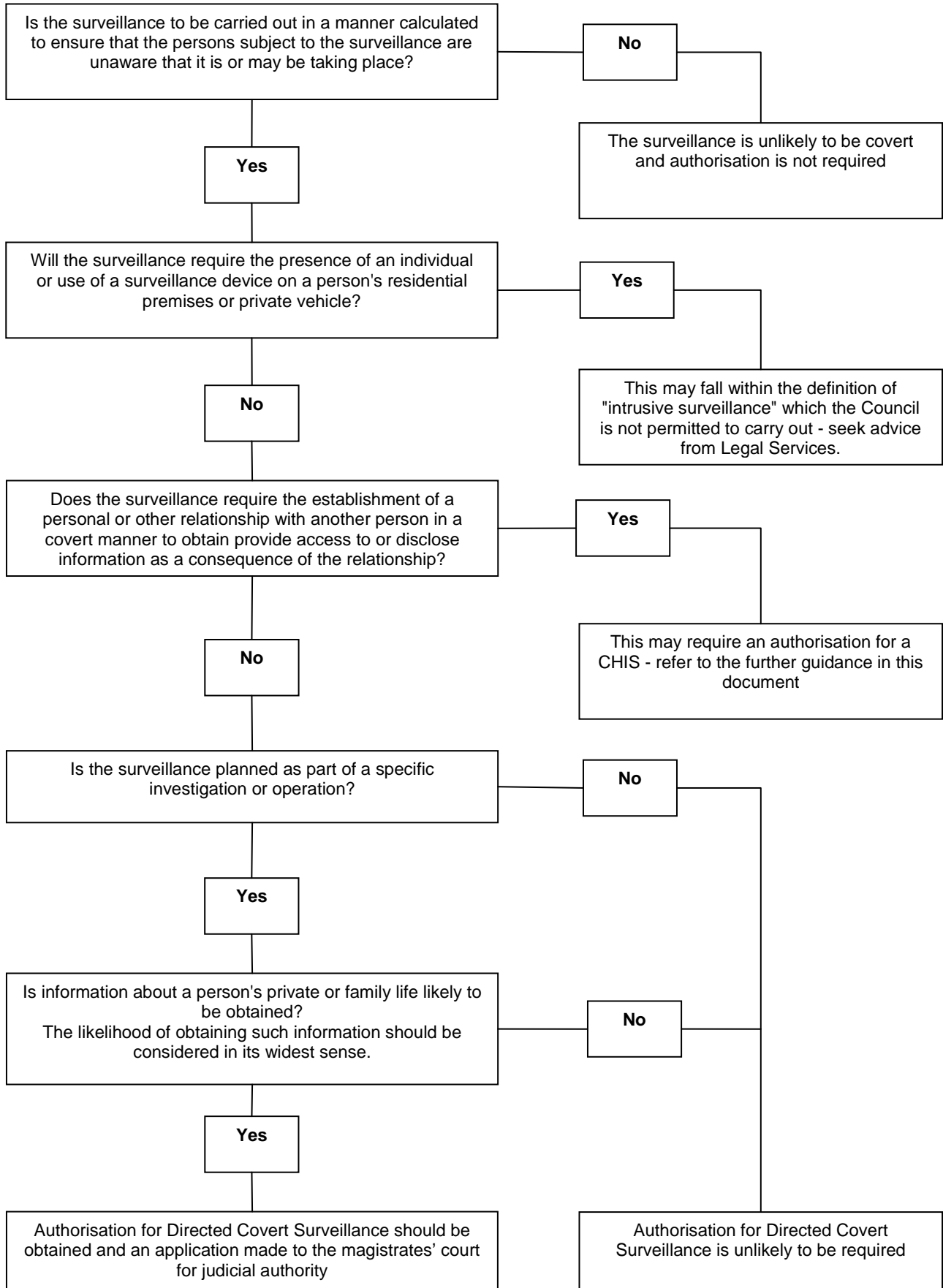
Adrian Lythgo	Chief Executive (for confidential information and juvenile CHIS authorisations)
David Smith	Director of Resources (for authorisation in exceptional circumstances)
Dave Thompson	Customer Services Manager (Customer and Exchequer)

NOTES

- A. Only the Chief Executive or in his absence, the Senior Responsible Officer can authorise activities involving confidential information or the use of CHIS
- B. No person shall become an Authorised Officer and/or an Applicant Officer without undergoing and maintaining RIPA training. In the case of Authorised Officers, no person shall become an Authorised Officer until their appointment is confirmed by the Senior Responsible Officer following training provided by or arranged by the RIPA Monitoring Officer.
- C. If an Authorising Officer is in any doubt about an individual matter they should consult the RIPA Monitoring Officer or RIPA legal advisers before any directed surveillance and/or CHIS is refused, authorised, reviewed, renewed or cancelled.

APPENDIX 2

FLOWCHART



APPENDIX 3

DUTIES OF AUTHORISING OFFICERS

- A. Nominate Applicant Officers within their Services who can make applications and ensure that any Applicant Officer who submits an application to them has received appropriate training prior to making the application
- B. Only grant an authorisation for directed surveillance if it is necessary for the purpose of preventing or detecting conduct which constitutes one or more criminal offences; and the criminal offence or one of the criminal offences would be either –
 - Punishable, whether on summary conviction (in the magistrates' court) or on indictment (in the Crown Court), by a maximum term of at least 6 months of imprisonment; or
 - Is an offence under:
 - section 146 of the Licensing Act 2003(2) (sale of alcohol to children);
 - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
 - section 147A of the Licensing Act 2003(3) (persistently selling alcohol to children);
 - section 7 of the Children and Young Persons Act 1933(4) (sale of tobacco, etc, to persons under eighteen).”.
- C. Only grant an authorisation for CHIS or the acquisition of communications data if it is necessary for the purpose of preventing or detecting crime or of preventing disorder.
- D. Only grant an authorisation that is proportionate to what is sought to be achieved by carrying out surveillance
- E. Before authorising surveillance, take into account the risk of collateral intrusion
- F. Be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities that might be taking place by other public authorities
- G. Unless it is unavoidable, do not issue authorisations if you were directly involved in the original investigation(s)
- H. Ensure that you have sufficient information and justification to authorise an investigation, if in doubt seek further information
- I. Nominate the appropriate level of officer to be in charge of the investigation
- J. Determine how often a review should take place in each case and ensure that this is at intervals of no longer than one month and review authorisations granted, at intervals of no longer than one month, to assess the need for the surveillance to continue

- K. Ensure that the RIPA Monitoring Officer is informed whenever an authorisation is refused, granted, reviewed, renewed or cancelled and that the relevant form is sent to the RIPA Monitoring Officer within 7 days
- L. Ensure that no surveillance commences unless and until the RIPA Monitoring Officer has obtained judicial authority
- M. Only renew authorisations where appropriate
- N. Cancel the authorisation if you are satisfied that the surveillance no longer meets the criteria applied when it was authorised
- O. On cancellation, issue appropriate instructions to officers in charge of investigations
- P. In cases where confidential information is likely to be acquired ensure that the case is referred to the RIPA Monitoring Officer for a decision on authorisation to be made by the Chief Executive. If in doubt consult the RIPA Monitoring Officer
- Q. Provide an annual return to the RIPA Monitoring Officer recording the RIPA training which shows the RIPA training received by themselves and by their Applicant Officers

APPENDIX 4

DUTIES OF OFFICERS IN CHARGE OF INVESTIGATIONS

- A. Seek authorisation for surveillance where it is likely to interfere with any person's rights to privacy by obtaining private information about that person
- B. Make formal applications for Directed Surveillance and CHIS where appropriate
- C. Inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who were not considered by the authorisation
- D. Make the Authorising Officer aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the surveillance
- E. Ensure that authorisations are regularly reviewed
- F. Apply for renewal shortly before the expiry of the authorisation period and at least 7 days before expiry where possible
- G. Cancel the authorisation when the surveillance is completed and advise any officers involved in the investigation accordingly
- H. Act immediately to terminate surveillance when instructed by the Authorising Officer
- I. Make the Authorising Officer aware of any likelihood that confidential information may be acquired if surveillance is authorised
- J. Properly store and retain the product of surveillance
- K. Ensure that no surveillance commences unless and until the RIPA Monitoring Officer has obtained judicial authority.

APPENDIX 5

MANAGEMENT OF COVERT HUMAN INTELLIGENCE SOURCES

Information Note: The use of a CHIS in Council investigations is most unlikely. Any officer contemplating such use should immediately seek advice from the RIPA Monitoring Officer

This is the text of the 2010 Home Office Code of Practice on Covert Human Intelligence Sources, Chapter 6 Management of Covert Human Intelligence Sources

Tasking

6.1. Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of [RIPA], asking him to obtain, provide access to or disclose information.

Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

6.2. Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

6.3. It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and if the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4. Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 29(5)(a) or (b) of [RIPA] must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5. Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in section 29(5)(a) and (b) of [RIPA] for each CHIS.

6.6. Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities.

6.7. The person referred to in section 29(5)(a) of [RIPA] (the "handler") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;*
- directing the day to day activities of the CHIS;*
- recording the information supplied by the CHIS; and*

- *monitoring the CHIS's security and welfare.*

6.8. The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.9. The person referred to in section 29(5)(b) of [RIPA] (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Joint working

6.10. In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The controller and handler of a CHIS need not be from the same public authority.

6.11. There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- *The prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross boundary or international drug trafficking;*
- *The prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/ local authority anti-social behaviour operation on a housing estate;*
- *Matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.*

6.12. In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

6.13. Management responsibility for CHIS, and relevant roles, may also be divided between different police forces where the Chief Officers of the forces concerned have made a collaboration agreement under section 23 of the Police Act 1996 or section 12 of the Police (Scotland) Act 1967, and the collaboration agreement provides for this to happen.

Security and welfare

6.14. Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, court.

6.15. The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- *the validity of the risk assessment;*

- *the conduct of the CHIS; and*
- *the safety and welfare of the CHIS.*

6.16. *Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.*

Sections 7.3 and 7.4 of the same Code of Practice provide:

Individual records of authorisation and use of CHIS

7.3 *Detailed records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS 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 CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.*

7.4 *Public authorities are encouraged to consider maintaining such records also for human sources who do not meet the definition of a CHIS. This may assist authorities to monitor the status of a human source and identify whether that source becomes a CHIS.*

Officers should be particularly careful to ensure that individuals who are not a CHIS at the outset of an investigation do not inadvertently become a CHIS by a process of “status drift”. If, for example a complainant volunteers to obtain further information about a person being investigated, care should be taken to consider whether the proposed action would involve the complainant becoming a CHIS and if so whether that is appropriate and in accordance with RIPA and the CHIS Code of Practice.

Appendix 6

Policy Statement

Kirklees Council takes seriously its statutory responsibilities and will take great care at all times to make sure that the use of surveillance is proportionate to the desired outcome of that surveillance.

In addition the RIPA Monitoring Officer can be contacted for further advice and assistance and the officers with particular expertise in this area are also listed at Appendix 1 and referred to throughout this document as the RIPA Legal Advisers.

Kirklees Council will only use directed surveillance:

- where it is necessary to do so for the prevention or detection of conduct which constitutes one or more criminal offences; and the criminal offence or one of the criminal offences would be either –
 - Punishable, whether on summary conviction (in the magistrates' court) or on indictment (in the Crown Court), by a maximum term of at least 6 months of imprisonment; or
 - Is an offence under:
 - section 146 of the Licensing Act 2003(2) (sale of alcohol to children);
 - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
 - section 147A of the Licensing Act 2003(3) (persistently selling alcohol to children);
 - section 7 of the Children and Young Persons Act 1933(4) (sale of tobacco, etc, to persons under eighteen).".
- in a way that is proportionate to the circumstances

Kirklees Council will only use CHIS or the acquisition of communications data;

- where it is necessary to do so for the prevention or detection of crime or to prevent disorder
- in a way that is proportionate to the circumstances

Kirklees Council will when using directed surveillance:

- do so with due consideration of human rights issues
- properly investigate any complaints made about its use
- actively monitor its use
- observe the appropriate law and Home Office Codes of Practice

- ensure that staff (and contractors) are properly trained

In the normal course of any covert surveillance activity the Council will not use Covert Human Intelligence Sources unless the surveillance is for the purposes of the West Yorkshire Trading Standards Service. If there appears to be a need to employ such sources, the application must be authorised by either the Chief Executive or the Senior Responsible Officer. The appropriate Home Office Code of Practice will then be followed.

The Council will not carry out intrusive surveillance within the meaning of RIPA.

The Council will, through the RIPA Monitoring Officer, maintain a central record of all directed surveillance operations which it undertakes and will monitor the quality of all forms created for this purpose. Any issues will initially be raised as necessary with Authorising Officers and will be drawn to the attention of the RIPA Monitoring Officer.

Responsibilities

Overall responsibility for each directed surveillance operation will lie with the Authorising Officer in charge of the operation.

Officers who authorise directed surveillance are responsible for granting, reviewing, renewing and cancelling authorisations.

The RIPA Monitoring Officer will be responsible for making applications for judicial authority.

Corporate responsibility for monitoring the use of covert surveillance rests with the Senior Responsible Officer.

The Council's Internal Audit service will review this area of work when requested to do so by the RIPA Monitoring Officer.

In cases where the Council's equipment or premises are used by the Police for the purposes of their investigations, the Police will be responsible for obtaining the necessary authorisations under the Act. Council officers should ensure that an appropriate authorisation has been obtained. If the Council officer is not satisfied that an appropriate authorisation has been obtained the Police should not be allowed to use the Council's equipment or premises. In cases where joint operations are undertaken, the lead authority should obtain the authorisation.

APPENDIX 7

RIPA AND ANTI-SOCIAL BEHAVIOUR ENFORCEMENT

- 7.1 Persons who complain about anti-social behaviour and thereafter keep a diary or incident log sheet will not normally be a CHIS as they are not required to establish or maintain a relationship for a covert purpose.
- 7.2 Recording the level of noise such as the decibel level, will not normally capture private information and therefore does not require directed surveillance authorisation.
- 7.3 Recording sound with a DAT recorder or matron box on the complainant's private premises will be directed surveillance unless it is done overtly, for example by informing the alleged perpetrator that a complaint has been received and monitoring will take place. The alleged perpetrator should also be informed of the period when this monitoring is likely to take place (e.g. over the next three months) and what this monitoring may involve (e.g. the use of log sheets, matron boxes etc).

Placing a covert stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will also require an authorisation for directed surveillance.

NB There will be types of Anti-Social Behaviour which no longer meet the conditions for the authorisation of directed surveillance because the underlying criminal conduct does not carry a penalty of at least 6 months imprisonment. Such conduct may involve minor offences of violence, disorder or harassment. If there is any doubt as to what the underlying offences might be or what penalties they carry advice must be sought from the RIPA Monitoring Officer.

APPENDIX 8

WORKING WITH OTHER AGENCIES

Where another agency has been instructed on behalf of Kirklees Council to undertake any action under RIPA, this document and the forms referred to in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

Where another agency such as the Police wishes to use the Council's resources (e.g. CCTV surveillance system), that agency must use its own RIPA procedures and before any officer agrees to allow the Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the record or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources in accordance with any service/end agreement and/or Code of Practice in force between agencies.

Where another agency such as the police wishes to use the Council's premises for their own RIPA action and is expressly seeking assistance from the Council, the officer should normally co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agency's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only assisting, not being involved in the RIPA activity of the external agency.

If the police or another agency wishes to use the Council's resources for general surveillance as opposed to specific RIPA operations, an appropriate information request and the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other agency before the Council's resources are made available for the proposed use.

APPENDIX 9

COMMUNICATIONS DATA

There are two types of communications data which can be obtained by local authorities such as the Council. These are:

Service data (s21(4)(b)) This covers itemised telephone call records, connection records, timing and duration of calls, connection, reconnection and disconnection data, use of forwarding or redirection service, additional telecom services and records of postal items.

Subscriber Data (s21(4)(c)) This includes information on subscribers of E-mail and telephone accounts, account information, including payment details, addresses for installing and billing and abstract personal records such as sign-up data.

Accordingly the Council cannot access the content of communications. The Council has an agreement in place with an external agency who will contact a communications provider if data is required. For more information on this contact the RIPA Monitoring Officer or the RIPA Legal Advisers. Authorisations will only be granted where necessary and proportionate. It seems unlikely that the Council would wish to use this facility unless requested to do so by the West Yorkshire Trading Standards Service.

Any errors must be reported to the RIPA Monitoring Officer who in turn will notify IOCCO as appropriate.