Audit and Standards Committee Report

Report of:	**Gillian Duckworth, Director Legal & Governance**
Date:	**11th January 2018**
Subject:	**Regulation of Investigatory Powers Act**
Author of Report:	**Steve Eccleston, Assistant Director, Legal Services**

Summary:

- SCC is empowered to use covert surveillance in investigations which have the aim of preventing and detecting crime and disorder. Approval for surveillance must be given by a Magistrate in addition to sign off at a senior level under well-established formal procedures.
- SCC is a low user of RIPA powers, having made no applications in the 2017
- This report is produced in compliance with the Office of the Surveillance Commissioners (OSC) requirement that the use of RIPA is reported at a senior level in the organisation on a regular basis.
- A new addendum policy to the council's use of social media has been approved by the Information Governance Board (IGB) in order to manage the risk of use of Social Media slipping into covert surveillance. This will be rolled out across the council in 2018 supported by an eLearning package.

Recommendations:

- That Audit and Standards Committee notes this report and the attached Social Networking Guidance: Covert Social Networking Checks and Surveillance Policy

Background Papers:

1. Report of the Office of the Surveillance Commissioner, 2017
2. Social Networking Guidance: Covert Social Networking Checks and Surveillance Policy
3. Central Record of RIPA authorisations for SCC
4. Report to IGB 20.10.17

Category of Report: OPEN

Regulation of Investigatory Powers Act

1.0 INTRODUCTION

1.1 On 23rd January 2017, the Council's use of covert surveillance was inspected by the Office of the Surveillance Commissioner (OSC). A number of recommendations were made designed to improve practices. In particular, work was required to mitigate the risk of council employee's use of social media slipping into covert surveillance. Also a refresh of training across the organisation and other policy/procedural changes.

1.2 Guidance recommends that Members be briefed on the Council's use of RIPA and this report is designed to serve that purpose. Changes in the law mean that surveillance is now rarely used by the council and, in general, risks related to the use of surveillance powers are very low.

1.3 Risks relating to surveillance arising out of the council (and societies) increasing use of social media have now been identified and this report sets out how the council proposes to manage those risks and issues.

1.4 Ensuring that the Council delivers best practice in the use of its powers will mean that the correct balances are struck enabling the rights of individuals to be protected and balanced against the rights of communities to be confident that the Council's regulatory powers are used to ensure their well-being.

2.0 BACKGROUND

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is the Act which defines when a public body can use surveillance to obtain information. The surveillance can take a number of forms, from undercover covert operatives (Covert Human Intelligence Sources – CHIS), through to covert surveillance (Directed Surveillance). All require authorisation under the Act

3.0 MAIN BODY OF THE REPORT

Including Legal, Financial and all other relevant implications (if any)

3.1 The initial "gateway" regime under RIPA enables local authorities to undertake covert surveillance for "the prevention and detection of crime or preventing disorder" (section 22(2)(b)). The RIPA Order 2010 raised the seniority of the authorising officer in local authorities from an "Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent" to a "Director, Head of Service, Service Manager or equivalent" (Part 2 of Schedule 2).

3.2 A range of types of surveillance conduct may be used in the course of a

local authority investigation. Key to whether RIPA applies to this conduct is its covert nature and whether it results in the obtaining of private information about a person who has a reasonable expectation of privacy

3.3 An example given in the Code of Practice on Covert Surveillance and Property Interference (the Surveillance Code) distinguishes between local authority officers merely photographing the exterior of a shop as opposed to recording a pattern of occupancy in a designated building. The former is considered to fall into the general observation duties of the authority, while the latter will likely require authorisation as a form of directed surveillance.

3.4 Governance of RIPA and surveillance is delivered through the requirement that a member of the Executive Management Team is identified as the “Senior Responsible Officer” (SRO). In this case that is Eugene Walker, Executive Director, Resources. The responsibilities include oversite of the system generally and also training. Mr Walker is supported in this task by Steve Eccleston, Assistant Director Legal Services. Support in the delivery of good governance is provided by Information Management (IM) and specifically John Curtis. RIPA, as a legal regime, sites coherently alongside Information Security, FOIA & DPA. It is a procedurally based regulatory regime. Thus Legal Services provide expert legal input, including applications to the Magistrates Court and support with the triennial inspection. Responsibility for policy and procedure oversight, record keeping, data and governance of process sits with IM

The Human Rights Act

3.5 The Human Rights Act 1998 requires that the exercise of any investigative power under RIPA 2000 must be both necessary and proportionate. For example, as a result of the controversy concerning certain local authority use of powers under RIPA 2000 against parents giving a false address to abuse the schools admissions system, the Surveillance Code now states that authorisation to engage in directed surveillance is "unlikely to be necessary or proportionate" for the investigation. However, while a breach of a provision of a relevant code of practice may be admissible as evidence, it does not directly give rise to any civil or criminal liability (section 72(2), RIPA 2000).

3.6 The Human Rights Act 1998 makes it unlawful for a Public Authority to act in a way which is incompatible with the European Convention of Human Rights, which, in Article 8, gives people the right to respect for their private and family life, home and correspondence. The advantage of properly obtaining authorisation under the Act, and in accordance with OSC guidance, is that such surveillance is rendered lawful and is admissible in legal proceedings. In summary, the use of surveillance under the HRA must be lawful, proportionate and necessary.

SCC use of RIPA

3.7 In keeping with most Local Authorities, Sheffield is a limited user of RIPA in its investigations. There were 18 authorisations during 2011 and, in line with a steadily decreasing trend, there were none in 2017.

The 2017 Inspection

3.8 On 23 January 2017, SCC received the report of the Office of The Surveillance Commissioners (OSC) triennial inspection. It was critical of what it identified as an insufficiency of training generally and also, specifically policy and training in the use of social media which could inadvertently slip into surveillance. This issue was identified as a national concern and was recently reiterated in the OSC's annual report. The inspection report is attached for information.

3.9 To remedy this, training on surveillance internally, and use of social media specifically, was commissioned. This was aimed at both EMT and operational investigators and took place over a whole day on the 5th September 2017, delivered by Act Now, a nationally recognised provider in this field. A follow up briefing was also held and, therefore, every member of EMT together with Gillian Duckworth Director of Legal Services have been trained in RIPA and surveillance.

3.10 Training was also held with operational staff from Trading Standards

3.11 A further full, bespoke training day was held on 19th December 2017, again delivered by a specialist trainer from Act Now, on the law and practice of managing undercover operatives known as Covert Human Intelligence Sources (CHIS). This was attended by Ian Ashmore, head of Environmental Regulation together with operational members of staff. SCC staff have now been trained in CHIS authorisation, handling and controlling as required by the Inspector

3.12 The inspection also required a policy to be drafted controlling and giving guidance in the use of social media to avoid the risk of it slipping into Directed Surveillance or Covert Human Intelligence Sources (CHIS). This policy has now been prepared is attached for the board to note.

3.13 Feedback on this policy has been obtained from a number of stakeholders including John Mothersole, Chief Executive, Eugene Walker, Executive Director Resources and SRO for RIPA, Lynsey Linton, Head of HR and Eddie Coates Madden Head of Communications. It has also been tested with a small project group in Children & Families, including the Principal Social Worker.

3.14 Key messages have been disseminated to staff via the front page of the intranet to ensure that undue risks were not created during the period of preparation of the policy

Conclusions

3.15 SCC is a low user of surveillance powers under RIPA. Where surveillance is considered to be a lawful, necessary and proportionate step in an investigation an application is made to a Magistrate for authority.

3.16 In accordance with the most recent report from the OSC, general training has been provided to applicants and approvers for directed surveillance. Bespoke training has been provided to EMT. A full days training has been provided in the authorisation and lawful operation of CHIS. A new policy has been developed to manage the risk in the use of social media unintentionally slipping into covert surveillance and a package of eLearning is being developed. The policy will be launched once the training package is available

4.0 RECOMMENDATIONS

4.1 That this report and the attached policy on Social Networking Guidance: Covert Social Networking Checks and Surveillance Policy are noted

Office of Surveillance Commissioners

OFFICE OF SURVEILLANCE COMMISSIONERS

INSPECTION REPORT

Sheffield City Council

9th January 20167

Assistant Surveillance Commissioner:
His Honour Norman Jones, QC.

DISCLAIMER

This report contains the observations and recommendations identified by an individual surveillance inspector, or team of surveillance inspectors, during an inspection of the specified public authority conducted on behalf of the Chief Surveillance Commissioner.

The inspection was limited by time and could only sample a small proportion of covert activity in order to make a subjective assessment of compliance. Failure to raise issues in this report should not automatically be construed as endorsement of the unreported practices.

The advice and guidance provided by the inspector(s) during the inspection could only reflect the inspectors' subjective opinion and does not constitute an endorsed judicial interpretation of the legislation. Fundamental changes to practices or procedures should not be implemented unless and until the recommendations in this report are endorsed by the Chief Surveillance Commissioner.

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version.

Office of Surveillance Commissioners

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

12th. January 2017.

INSPECTION REPORT
SHEFFIELD CITY COUNCIL

Inspection	9th. January 2017.
Inspector	His Honour Norman Jones, QC. Assistant Commissioner

Sheffield City Council.

1. Sheffield City Council is the Local Authority responsible for the local government administration of the City of Sheffield. The authority covers an area of 142.06 square miles in South Yorkshire and serves a population of about 570,000.

2. The Chief Executive, as at the time of the last inspection, is Mr John Mothersole who is supported by four Executive Directors and 18 Directors.

3. Mr. Eugene Walker, Executive Director for Resources, is the *RIPA Senior Responsible Officer* (*SRO*) and has been appointed since the last inspection. The *RIPA Co-ordinating Officer*, as at the time of the last inspection, is Mr Steve Eccleston, Assistant Director Legal Services, although some of the responsibilities are now shared by Mr John Curtis, Head of Information Management.

4. I conducted the last inspection of Sheffield City Council for the OSC in January 2014.

5. The Council has substantially reduced its recourse to covert surveillance in the period since the last inspection. In the period preceding that inspection, 42 authorisations had been granted whilst, since the last inspection, there have been only two. This pattern had already commenced at the time of the last inspection with only five authorisations being granted in 2013. Both examined authorisations on this occasion were for *directed surveillance* and each was justified with neither being concerned with *self authorisation* or *confidential information*.

6. The Council Offices are situated at the Town Hall, Pinstone Street, Sheffield, S1 2HH.

Inspection.

7. Mr. Eccleston and Mr Walker warmly welcomed me to Sheffield City Council. Mr Eccleston remained throughout the inspection the majority of which was attended by Mr Walker and Mr Curtis. The inspection was later joined by Mr Ian Ashmore, Head of Environmental Regulation (including Trading Standards and Environmental Health) and an authorising officer; Ms Elyse Senior-Wadsworth, Service Manager in Business Strategy and Children, Young People and Families (with responsibility for Information Governance) and Philip Glaves, Principal Officer - Fair Trading.

8. The inspection was conducted by means of discussion and interview with the *RIPA* officers and included an examination of the Central Record of Authorisations and the retained applications/authorisations, reviews, and cancellations. All officers engaged demonstrated a lively interest and a sound knowledge of *RIPA* principles.

9. Among the matters discussed were the reasons for the reduction in authorisation, actions taken on past recommendations, the management of *RIPA,* authorising officers, training, *CHIS*, social media, policy and procedures, reporting to Councillors and CCTV.

Reduction in Authorisation.

10. The reasons for the reduction in the level of authorisation were discussed with the officers. Principal reasons given include:

    - the loss of fraud benefit fraud investigation to the DWP;
    - the effects of the *Protection of Freedoms Act 2012* and the *RIP(Directed Surveillance and CHIS)(Amendment)Order 2012, SI 2012/1500* removing a number of offences from consideration for authorisation which had hitherto attracted a large number of authorisations, including in particular antisocial behaviour;
    - a change in the culture of investigation which now places greater emphasis upon deterrence and warning;
    - Trading Standards have been focused on investigations of a nature which would not naturally attract covert surveillance. The Department has been concerned to discover alternative more overt means for the obtaining of evidence and its resources have been concentrated in those areas, particularly that of rogue trading, which are particular problems in the Sheffield area. It is to be noted that Mr Ashmore was of the opinion that more covert surveillance was likely to be undertaken in the future particularly in relation to the investigation of sales of illicit tobacco.

Examination of Documents .

11. The **Central Record of Authorisations** is to be found in a spreadsheet format which is fully compliant with the *Code of Practice for Covert Surveillance and Property Interference, 8.1.* It is now maintained by Mr. Curtis and is completed up-to-date.

12. The two **applications/authorisations** were examined. Both were for *directed surveillance* with one relating to a benefit fraud investigation in March 2014, prior to the responsibility for such passing to the DWP, and the other to underage test purchasing at eight retail premises in February 2015.

13. The **application** provided a good outline of the intelligence basis for the benefit fraud investigation and an excellent outline of the proposed surveillance activity. Collateral intrusion was well considered, save that no consideration was given to intrusion upon the child of the family under surveillance. The considerations of *necessity* and *proportionality* covered all the essential elements. *Confidential information* was said to be "unlikely" to be acquired. If so that left open the possibility that there was some likelihood of acquisition and that would have required the authorisation of the CEO.

There was no such likelihood and the applicant should have so stated. The **authorisation** followed good practice of being hand written and there was good detail of what was being authorised with the "5W's" well considered. The articulation of *necessity* and *proportionality* was adequate but crammed into a very small box which, had the applicant given thought to prior to downloading the form, could have been expanded to provide sufficient space for a more detailed discussion. A review date was set but the expiry date was linked to the date of authorisation and not that of magistrate's approval. Such approval was obtained and a review was recorded giving thorough consideration of the actions already undertaken. The authorisation was appropriately cancelled with good detail of what had been achieved.

14. The test purchasing was to be conducted with a juvenile wearing a covert body video camera and entering eight shops unaccompanied but with a trading standards officer nearby outside to ensure the safety of the test purchaser. The **application** recorded that all shops visited had complaints recorded against them and had been written to and told that a test purchase would take place at some stage. Nevertheless there was no intelligence recorded against the premises individually which practice should be adopted. It also raises the question as to whether this form of test purchasing may be regarded as overt and thus not requiring authorisation. However the Council prefers to take a "belt and braces" approach on the issue. The consideration of *necessity* did not provide reasons why it was necessary to use covert surveillance as a tool of investigation and *proportionality* and did not balance the seriousness of the offence against the intrusion to be expected. One of the reasons given for the exercise was to be a "reminder to business regarding their obligations to challenge prospective purchasers" which does not fit easily into the single ground available to the Council. The **authorisation** followed best practice of being hand written and the actions proposed were well articulated but the authorisation did not indicate the specific addresses to which it should apply. *Necessity* and *proportionality* were well considered and an expiry date was set though linked to the date of authorisation rather than that of the magistrate's grant of approval. The authorisation was appropriately cancelled.

Previous Recommendations

15. I made four recommendations in my previous report.

    (i) *Ensure that the principles of* necessity *and* proportionality *are fully articulated in applications and authorisations.*

    These issues have been considered in feedback and training since the last inspection but could do with continuing attention. Applicants and authorising officers should recognise that they should always articulate as part of their consideration of *necessity* why it is necessary to use covert surveillance as a tool of their investigation. Furthermore they should readily identify each of the three basic elements of *proportionality* as *(a) that the proposed covert surveillance is proportionate to the mischief under investigation; (b) that it is proportionate to the degree of anticipated intrusion on the target and others; (c) it is the only option, other overt means having been tried or considered and discounted.* These issues are fundamental to the *RIPA* process and the *RIPA Co-ordinating Officer* should have them well in mind when he undertakes his gate keeping and oversight role in relation to any authorisation. This recommendation has been largely discharged but future robust oversight should continue to reflect the importance of these issues.

    (ii) *The* RIPA Co-ordinating Officer *should undertake a review of applications/authorisations before they are submitted to a prosecuting solicitor for presentation for a magistrate's approval.*

This practice has been adopted and this recommendation has been discharged.

(iii) *Establish a corporate training programme to include regular refresher training and to engage both likely applicant and authorising officers. This to include instruction in relation to the issues raised in this report especially those of necessity, proportionality and* CHIS.

Such a programme has not been established and the only training undertaken since the last inspection has been in 2016 and concerned only six officers. (See **Training** below). This recommendation has not been discharged.

See recommendation

(iv) *Amend the* RIPA *Policy and Code of Practice.*

Appropriate amendments have been made. This recommendation has been discharged.

***RIPA* Management**

16. Mr Walker has been appointed as *SRO* since 2014. When he came to the role he had some previous experience of *RIPA* having been responsible for benefit fraud investigation which came within his previous remit as Director of Finance. His knowledge of the subject depends in part upon that experience and later training by Mr Eccleston though he has not received formal corporate training by an external provider. He regards himself as having prime responsibility for the oversight of the *RIPA* process within the Council. He and Mr Eccleston are in close touch and he is informed if any issues arise. Mr Eccleston has been *RIPA Co-ordinating Officer* for a number of years and is very experienced in the field. He is regarded as the officer who "runs" *RIPA* within the Council. He received external professional training in 2016 and he keeps himself well abreast of *RIPA* developments, delivering some training to other officers. He performs a gate keeping role in the sense that applicants would be expected to first approach him for advice before making an application and seeking authorisation. Once an authorisation is granted it returns to Mr Eccleston and will also be reviewed by Mr Curtis for the purpose of completing the Central Record. Arrangements will be made by Mr Eccleston for attendance on the magistrate for approval and a protocol is in existence with the Magistrate's Court for the making of such applications. A prosecuting solicitor from the Council will attend with the applicant and if the magistrate raises questions to which only the authorising officer could provide an answer an application would be made for an adjournment for the officer to attend.

17. Mr Eccleston is aware that his responsibilities include the organisation of training and that little training has taken place in the previous inspection period. He recognises that no formal *RIPA* training programme exists at the Council and that steps must be taken to establish one. He is alert to the fact that a recommendation to this effect in the last report has not been addressed.

18. In addition he has responsibility for **raising *RIPA* awareness** within the Council although this, in future, will be undertaken by Mr Curtis who is ideally placed for the role in relation to his responsibilities for information governance. It is recognised that a risk faced by public authorities who engage little in covert surveillance is that of unauthorised surveillance. This is best prevented by ensuring a good degree of awareness of the requirements for authorisation within the Council staff. Some awareness raising actions have been taken by Mr Eccleston since the last inspection including the provision of inspection feedback to officers, the circulation of new *RIPA* information to officers and holding regular meetings with Trading Standards (now regarded as the Department most likely to engage covert surveillance). He has

discussed with Mr Curtis means of disseminating information and it is felt that the Information Governance Working Group will be a useful body for this purpose since it exists to disseminate information within the Council. The simple means of such dissemination could include the cascading down of information from management and the utilisation of Council newsletters to contain the basic information to recognise that authorisation may be required if surveillance is being undertaken and where to get advice on the subject.

See recommendation

19. It was noted, however, that within the Trading Standards Department, Mr Ashmore was able to observe that officers had not lost interest in covert surveillance and that he had been approached by officers considering making applications. In those cases, following discussion with the officer, Mr Ashmore has tendered advice, which had been accepted, that the application should not proceed.

Authorising Officers.

20. Five officers of appropriate rank, including the CEO and *SRO*, are designated to undertake authorisation for the Council. The CEO or, in his absence, whoever deputises for him (probably Mr Walker) are likely only to authorise the acquisition of *confidential information* or the employment of juvenile or vulnerable *CHIS*. The *SRO* should otherwise only authorise in exceptional circumstances and thus provide some extra resilience.

21. It is of some concern that of that number only Mr Ashworth and the SRO have received any recent training.

Training

22. No significant training has been undertaken since the last inspection. It is to be noted that the last authorisation was now some two years ago and demonstrated some weaknesses, particularly on the part of the applicant. It is impossible to say what the standard of authorisation would be at the present time but unless officers receive regular training they become stale and there is an inevitable fall in quality. These issues were discussed with the officers and it was recognised that more training must be undertaken and embrace a wider audience. The institution of a training programme would provide some discipline to the process and should allow for refresher training at least at about 12/18 monthly intervals. This could be provided initially by an external professional trainer with follow-up sessions organised internally. Alternatively the already existing e-learning programme at the Council could be extended to include a *RIPA* module for all likely to engage in the obtaining and granting of authorisations. The training recently undertaken in May and September 2016 concerned the attendance of Mr Eccleston on a course run by an external provider followed by the later delivery of training by Mr Eccleston, based on that experience, to the *SRO*, Mr Ashmore, two Heads of Service and a prosecuting solicitor who would normally attend applications for judicial approval. It follows that three authorising officers have received no recent training and none has been delivered to likely applicants. Mr Ashmore observed that a considerable time had elapsed prior to his 2016 training since he had last received corporate *RIPA* training.

23. The Trading Standards Department has had the advantage of *RIPA* training within the aegis of its professional training, with a Training Standards Manager and other staff being the beneficiaries. In addition the large Regional Trading Standards Group, covering Sheffield and all other regional local authorities within Yorkshire and Humberside, provided training.

See recommendation

CHIS

24. The Council does not employ *CHIS* in the usually understood sense of informants. Stringent authorisation provisions apply and only the CEO or the Director of Legal and Governance is permitted to authorise the employment of *CHIS*. Officers considered it unlikely that such sources would be employed in the normal course of events. Nevertheless the Council has to be prepared to manage a *CHIS* if one appears suddenly in circumstances where the Council has a duty to act. The extension of social media investigation(see **Social Media** below) may also lead to the employment of officers as *CHIS* particularly within the Trading Standards Department if that Department follows the example of some sister departments within the country. To do so it needs officers able to act as a controller and handler and training needs to be given to ensure that those officers understand and are competent to carry out those responsibilities. This does not mean training to the standard expected of police officers acting in those capacities who have to absorb the "tradecraft" required in highly sensitive situations.

See recommendation

Social Media.

25. The Council publishes for its staff a *Social Networking Guidance* document which provides both direction and guidance on the usage of social media for Council purposes. It deals comprehensively with most forms of usage but is not directed to the issue of surveillance save in one short paragraph which advises that *"any monitoring or surveillance of a customer or employee is strictly controlled and you must be authorised to carry out this activity. For example, you must never become a "friend" of any service user or employee for the purpose of obtaining information, unless authorised."* Whilst this provides good guidance to the staff in general, somewhat more comprehensive guidance is required to those likely to be engaged in covert surveillance. This should be provided as a section of the Council's *RIPA Policy and Code of Practice*. A "rule of thumb" guide, which may not cover all social networking sites, may be expressed thus:

> Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case *directed surveillance* authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example, a "friend" on the Facebook site, with the investigating officer utilising a false account concealing his/her identity as a Council officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at the minimum, as *directed surveillance*. If the investigator engages in any form of relationship with the account operator then s/he becomes a *CHIS* requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created.

See recommendation

26. It was noted whilst discussing the issue of social media investigation that within the Childcare Department, where officers are dealing directly with families, those families are told at an early stage of their engagement with the Department that Facebook accounts may be looked at by officers and they are also told that other individuals may be spoken to including schoolteachers. The Department never considers going beyond the open source material on such sites and would never

breach privacy controls by seeking to become a "friend". On rare occasions, where there is urgency in the initial stages of an enquiry with no time to contact families, an approach to Facebook would be considered and an individual's account may be viewed on the same basis as above. If there are repeated visits to the site in those circumstances, unlike the situation where families have been warned in advance and hence the viewing of a site becomes overt, this latter procedure would require authorisation for *directed surveillance* unless the "immediate response" provisions of *RIPA*, section 26(2)(c) apply. Ms Senior-Wadsworth indicated that there had been no incidents of urgent actions in the last 12 months and where viewing had occurred concerning previously warned families it had been on only two occasions in the same period. She and her Department were well aware of the Council's general guidance and there was some awareness of *RIPA* within the Department, but that did not extend to considering authorisation when examining social media. She emphasised the importance of transparency with families dealt with by the Department and would be concerned if any actions were undertaken that may breach the building of trust.

27. The Trading Standards Department did engage in viewing suspected websites and was well aware of the risks of examining social media. Officers followed a practice of viewing the open source material on a website only once and perhaps taking a screenshot. There was awareness of the risks of requiring *directed surveillance* authorisation on repeated visits or if the privacy controls were breached with appreciation that if a relationship were formed with the site operators that would require *CHIS* authorisation. The Department does not operate covert social media accounts. Officers within the Department have received training from Trading Standards trainers on these issues.

Policy and Procedures

28. The Council's *RIPA* policy and procedures are to be found in its *RIPA Policy and Code of Practice* document, last edited in December 2016. It has previously been described as "thorough and well constructed" and continues to remain so, though it may benefit from some further effort to ensure that the procedures for *directed surveillance* are clearly differentiated from those for *CHIS*. Well constructed flowcharts are to be found to assist officers in making applications and authorisations. It is kept under review by Mr Eccleston. It may benefit from a small number of amendments to include:

    - Revising the name of the *SRO* to reflect the change of officer;
    - adding to the list of *RIPA Co-ordinating Officer* responsibilities those for organising *RIPA* training and for ensuring *RIPA* awareness is high throughout the Council;
    - clarify within the sections "General Rules on Authorisations" and "Authorisation Process" that *CHIS* authorisations last for 12 months (one month for a juvenile *CHIS*) and that the duration of all authorisations commences at the time of a magistrate's approval;
    - add to the requirements for a Central Record of Authorisations reviews and magistrates appearances;
    - introduce a section regarding the investigation of social media.

See recommendation

Councillors

29. For the past two years reports have not been provided to Elected Members on the basis that there has been no covert surveillance activity. The importance of informing Councillors even when there was no such activity was discussed with the officers. Attention was drawn to the *Code of Practice for Covert Surveillance and Property*

Interference,3.35 and the *Code of Practice for CHIS,3.27* which require an annual report supported by other regular reports to be delivered to Elected Members during the year. The officers undertook to deliver such reports to the Council's Audit Committee.

See recommendation

CCTV

30. A CCTV system continues to cover the city centre as described in the previous report. If the police require using the system for covert surveillance an authorisation, suitably redacted, must be produced and this is retained and filed. On occasions when the police have sought access without authorisation such access has been refused.

Conclusions.

31. Sheffield City Council has moved from a situation of being a moderate user of *RIPA* to to one where such activity is rare and authorisation is therefore rarely sought. As a result it may be felt that less attention has been paid to ensuring the maintenance of good standards than has hitherto been the case. It was disappointing to note that the recommendation of the last inspection report that a "corporate training programme to include regular refresher training" should be established has effectively received no attention. It is only by regularly refreshing officers' knowledge that some confidence can rest in their capacity to make good quality applications and authorisations. Failure to do so means that officers are likely to make errors in the application/authorisation process which may ultimately cause considerable embarrassment to the Council in the course of litigation and possibly in the media.

32. Whilst both Mr Walker and Mr Eccleston impress as conscientious officers with a good knowledge of the subject who are determined that *RIPA* compliance must be maintained by the Council, nevertheless more robust attention should be paid to those practices which have to some extent fallen into abeyance in recent times.

33. It has not been possible on this occasion to assess the current quality of authorisation since none has been undertaken in the last two years. One of the two authorisations examined related to a Department which no longer exists at the Council. Nevertheless some concern continues including the articulation of *necessity* and *proportionality* in the most recent forms examined, issues which are at the heart of the *RIPA* process.

Recommendations

34.

(i) Raise *RIPA* awareness throughout the Council. (Paragraph 18).
(ii) Establish a corporate training programme to include regular refresher training and to engage both likely applicant and authorising officers. This to include instruction in relation to the issues raised in this report especially those of necessity, proportionality and *CHIS*. (Repeat of last report)(Paragraphs 15(iii) and 23).
(iii) Ensure officers are trained to manage *CHIS*. (Paragraph 24).
(iv) Establish a social media policy for covert surveillance. (Paragraphs 25 and 28).
(v) Amend the *RIPA Policy and Code of Practice*. (Paragraph 28).
(vi) Ensure annual and regular *RIPA* reports are submitted to Elected Members. (paragraph 29).

His Honour Norman Jones, QC,
Assistant Surveillance Commissioner.

INFORMATION MANAGEMENT BOARD

Report Title: Regulation of Investigatory Powers Act 2000: Social Media & Surveillance Policy

Reporting Officer: Steve Eccleston & John Curtis

Officers and Boards Consulted:

Eugene Walker, Executive Director Resources & SRO RIPA, John Curtis, Information Management, Linsey Linton Head, of HR, Gill Duckworth, Director Legal & Governance & Monitoring Officer, Ruth Bastin, Principal Social Worker: all on 20.10.17

Date: ** October 2017

1. Purpose

1.1 To seek the approval of the Information Management Board to the attached policy governing and guiding how staff can lawfully interact with customers in their social media

2 Recommendations

2.1 That the attached policy is approved

2.2 That the policy be placed before the Audit Committee for information and to ensure that there is proper visibility of the policy

3 Background and Update

The Council makes occasional use of covert surveillance as part of criminal or other investigations. The use of surveillance is governed by the Regulation of Investigatory Powers Act 2000. Organisations using surveillance are answerable to the Office of the Surveillance Commissioner (OSC) which inspects on a periodic basis.

Surveillance is a council wide issue with central advice and governance provided by Information Management (IM) and legal input by Legal Services.

For information, the role of IM with regard to RIPA is relatively new. The sense is that RIPA, as a legal regime, sites coherently alongside Information Security, FOIA & DPA. It is a procedurally based regulatory regime. Legal Services will continue to provide expert legal input, including applications to eth Magistrates Court and the triennial inspection. It seems right however that responsibility for policy and procedure oversight, record keeping, data and governance of process should sit with IM.

On 23 January 2017, SCC received the report of the Office of The Surveillance Commissioners (OSC) triennial inspection. It was critical of what it identified as an insufficiency of training generally and also, specifically policy and training in the use of social media which could inadvertently slip into surveillance. The inspection report is attached for information.

To remedy this, training on surveillance internally, and use of social media specifically, was commissioned. This was aimed at both EMT and operational investigators and took place over a whole day on the 5th September 2017, delivered by Act Now, a nationally recognised provider in this field.

The inspection also required a policy to be drafted controlling and giving guidance in the use of social media to avoid the risk of it slipping into Directed Surveillance or Covert Human Intelligence Sources (CHIS). This policy has now been prepared in draft and is attached for the board to consider. Feedback has already been obtained from a number of stakeholders including Eugene Walker, executive Director Resources and SRO for RIPA. It has also been tested with a small project group in Children & Families, including the Principal Social Worker.

Once the Information Governance Board has approved the policy it is proposed that it is submitted to the Audit committee for information. This delivers a level of visibility of surveillance related issues which the OSC required.

Documents attached

1. Draft policy
2. OSC report

REF: <INSERT FILE REFERENCE>

Social Networking Guidance: Covert Social Networking Checks and Surveillance Policy

Why read this note?

Although you may think that anything placed out on social media is fair game for anyone to read, this is not the case in law for public authorities such as councils. As council employees, you are not free to simply scan or read the publics social media posting such as FaceBook, Twitter or Instagram.

You have to comply with good practice and the law in order to do that safely and lawfully. This note tells you how to do that.

Status of this guidance

1. This guidance is issued as an annex to the Councils Social Networking Guidance published on July 2013, authored by HR and accessible at https://myteam.sheffield.gov.uk/HRPoint/PublicLibrary/Forms/Conduct.aspx

Purpose of this guidance

2. The council encourages the use of social media (SM) as a way of interacting and engaging with customers. Detailed guidance and policy is available through the *Social Networking Guidance* outlined above. There is a risk, however, that visits to an individuals social media pages e.g. Facebook, Twitter, Instagram, Pinterest, Snapchat, Linked In, Google +, You Tube etc ***without the customers knowledge*** could amount to ***covert surveillance***, something which can only be permitted in strictly limited and controlled circumstances.

3. **The key issue is whether the visit is covert.**

4. Social media content is also sometimes referred to as "Open Source Material". In this guidance the phrase "Social Media" or "SM" will generally be used for simplicity.

5. There may be occasions when, as part of a criminal investigation, covert observations of social media are necessary and appropriate. This guidance also applies to those situations. In short however, in those situations, Regulation of Investigatory Powers Act (RIPA) authorisation must be obtained. See http://www.sheffield.gov.uk/home/your-city-council/ripa.html and http://intranet/managers/surveillance-investigation. This guidance is therefore intended to support employees when using social media or internet open source information in furtherance of investigations as to when authorisation for surveillance activities should be sought.

Top Tips & Easy Read version

- **Let the customer know if you visit their social media page. Just tell them!**
- **Don't keep repeatedly visiting a customer's social media profile just to see what they are up to**
- **Don't use council profiles / accounts to "friend" individuals' social media accounts, so that the council could end up interacting with them in their personal timeline**
- **Speak to your manager if you're unsure about how you're using social media**
- **Always be careful about how you refer to your work or the council when using your own personal social media accounts**
- **Make sure you complete the online Learning Hub training on social media *(in the process of preparation*).**
- **Your manager can take expert advice from Legal Services or from Information Management**

How to use Social media confidently and without risks

6. Occasional (e.g. once or twice) visits to an individual's SM page e.g. their Face Book feed, without them knowing that you have done so, will not normally amount to covert surveillance (thus requiring authorisation under RIPA). Occasional (e.g. once or twice) visits might be necessary to identify someone for further overt communication. Or it might be justified as part of the preparation in order to decide whether an investigation is required which would then be authorised under RIPA. You must always record your visit, the reason for it and the nature of the information seen.

7. You must always be prepared to justify the reason for your visit to the page/website etc if asked.

8. Overt visits are acceptable. It is only covert (or "secret") visits amounting to directed surveillance which require formal authorisation. **Overt means you tell the customer that you are visiting.**

9. **You can make your visit to a SM site/page/feed overt by**

    a. **Telling the person you have visited their site/page/feed and may do so again in the future**

b. Including the fact that you may visit a SM profile in your consent forms when you first come into contact with a customer

10. In an investigation, any warning or communication should make it clear that the target's activities will be monitored and potentially investigated (if relevent) should the conduct continue. The warning, the reason for it, and a screen shot of any web page should be saved on the relevent case file.

Guidance on covert observation of social media

11. Before any covert investigation takes place using the internet or social media, the investigating officer should have regard to the potential need for a directed surveillance application or a covert human intelligence source CHIS) application in accordance with the councils RIPA policy http://www.sheffield.gov.uk/home/your-city-council/ripa.html

12. The key considerations are to show that the surveillance is necessary, in that there is no other way of obtaining the information, and also proportionate – taking into account the following:-

- 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

Open source material

13. Authorisation is not normally necessary for general open source investigations unless there is some ongoing monitoring of an individual. A case may require reconsidering if there is systematic retention, review and analysis of the information so as to profile the individual. Continued regard should be had to the right to respect for private life (Article 8 Human Rights Act 1998).

Covert Social Media Surveillance

14. There may be circumstances where it is decided that it is inappropriate to send an overt warning to an individual: For example:

- where the individual has a previous history of the behaviour complained of,

- where it is intended to carry out more detailed investigations into the social or business links which the individual has,

- because serious issues are involved e.g. where the activity is clearly carried out with a deliberate intention to defraud, or

- Where the activity is on such a scale, or linked with other illegal activity, that it is thought robust action is necessary.

- Where vulnerable individuals are at serious risk of harm from the behaviour.

15. In these situations, a RIPA authorisation should be applied for and no further monitoring should take place until it has been granted.

Guidance on "friending" a customer

16. Council SM accounts shouldn't be generally used to "friend" or interact with a customer's timeline. If such interactions are necessary then

    - **the starting point is that they should be overt**: identify who you are, your role and why you are interacting with the customer in this way

    - remember to send periodic reminders of the fact that you are interacting in this way

    - ensure you have manager approval to interact in this way

    - discuss your interactions in supervision/1:1's

    - record your interactions with screen shots in the case file

17. Any interactions in this way which are covert (or anonymous) can **only** take place if authorised through the CHIS routes (below)

Covert Human intelligence Sources (CHIS)

18. A "CHIS" is, in simple terms, an undercover source. Anonymously or covertly "friending" a customer on SM is highly likely to amount to a CHIS. Thus, where a covert relationship which is more than merely transitory, is entered into with an individual then authorisation under RIPA for a CHIS should be sought. This applies to social media. An overt and explicit SM relationship cannot amount to a CHIS (thus requiring authorisation) but must still comply with all other council policies.

Law and Official Guidance

The Data Protection Act 1998

Please note that this may be revised in due course post implementation of the General Data Protection Regulation (GDPR). In the meantime:

- Only collect and process appropriate personal data to the extent that it is required to fulfil operational needs or to comply with legal requirements.
- Ensure the quality of the data we use.
- Apply retention schedules to determine the length of time we hold information and dispose of information securely when it has reached its disposal date.
- Ensure that individuals, about whom we hold data, can fully exercise their rights under the DPA 1998.
- Take appropriate security measures to safeguard personal information.
- Ensure that we do not transfer personal data outside the country without suitable safeguards.
- If in doubt seek advice from the Information Governance Team.
- Be aware that content you share and actions you take may show up on pages other than your own and could be re-shared by other users.

Home Office Guidance

19. The Home Office has published a statutory Code of Practice, pursuant to s.71 RIPA, on Covert Surveillance and Property Interference ("the Home Office Code"). By s.72(1), the Council must have regard to the Home Office Code when exercising any powers and duties to which it relates. In relation to investigation using the internet, the Home Office Code states:

> *2.29 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and*

> *proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. […]*

22. In relation to material in the public domain, it states:

> *2.5 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.*

20. The Office of the Surveillance Commissioner (OSC) has published guidance on Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources ("the OSC Guidance"). In relation to monitoring of social media, the OSC Guidance states:

> *289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.*
>
> *289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.*
>
> *289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a*

member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

21. In relation to activity taking place in public, the OSC Guidance states:

124. Section 26(2) RIPA does not differentiate between current and historical surveillance product. Sections 48(2) of RIPA and section 31(2) of RIP(S)A define surveillance as including "monitoring, observing or listening" which all denote present activity; but present monitoring could be of past events or the collation of previously unconnected data. Pending judicial decision on this difficult point the Commissioners' tentative view is that if there is a systematic trawl through recorded data (sometimes referred to as "data-mining") of the movements or details of a particular individual with a view to establishing, for example, a lifestyle pattern or relationships, it is processing personal data and therefore capable of being directed surveillance.

125. The checking of CCTV cameras or databases simply to establish events leading to an incident or crime is not usually directed surveillance; nor is general analysis of data by intelligence staff for predictive purposes (e.g. identifying crime hotspots or analysing trends or identifying criminal associations). But research or analysis which is part of focused monitoring or analysis of an individual or group of individuals is capable of being directed surveillance and authorisation may be considered appropriate.

The Human Rights Act 1998

22. Article 8 of the European Convention on Human Rights provides as follows:

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

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