Policy on Directed Surveillance and use of Covert Human Intelligence Sources

VERSION	Version 6
DATE AGREED	October 2014
NEXT REVIEW DATE	October 2021
AGREED BY	Individual Officer Decision
COVERAGE	This Policy applies to service areas within Bracknell Forest Council
AUTHOR(S)	Borough Solicitor and Assistant Solicitor - Information Management and Corporate Governance

Contents

Amendment Sheet

Amendment Number	Details	Amended By	Date
Version 1	Policy 31.8.04 updated 11.12.06		December 2006
Version 2	Updated	Alex Jack – Borough Solicitor Nicola Thurloway – Assistant Solicitor	March 2010
Version 3	Updated in accordance with Revised Code of Practice	Alex Jack – Borough Solicitor Nicola Thurloway – Assistant Solicitor	April 2011
Version 4	Updated to take into account recent law including Protection of Freedoms Act and various Statutory Instruments and Home Office Guidance	Alex Jack – Borough Solicitor Nicola Thurloway – Assistant Solicitor	November 2012
Version 5	Updated to take account of the Inspector's Report of the 13 March 2014	Alex Jack - Borough Solicitor and Anthony Igbiniyesu – Senior Solicitor	March 2014
Version 6	Reviewed as part of annual review process	Kevin Gibbs – Executive Director of Delivery Sean Murphy - Public Protection Manager	November 2019
Version 7	Executive approval for annual update	Kevin Gibbs – Executive Director of Delivery Sean Murphy - Public Protection Manager	January 2021

POLICY ON DIRECTED SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. INTRODUCTION

1.1 In some circumstances it may be necessary for Council employees in the course of their duties to make observations of persons in a covert manner (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) or to use covert human intelligence sources. By its very nature, that sort of action is potentially intrusive and could expose the Council to a legal challenge as a potential breach of Article 8 of the European Convention of Human Rights, which establishes a "right to respect for private and family life home and correspondence", incorporated into English Law by the Human Rights Act 1998. Also, there is a risk that if covert surveillance and covert human intelligence sources are not conducted properly the evidence obtained may be held to be inadmissible in court on the basis that it is unfair to use it as it was gathered contrary to Article 8 – right to privacy and infringes the defendants right to a fair trial as guaranteed by Article 6 – right to fair trial.

2. OBJECTIVE

2.1 The objective of this policy is to ensure that all covert surveillance carried out by Council employees including any involving covert human intelligence sources is carried out in accordance with the law.

2.2 Indeed RIPA recognises the Council's right to infringe an individual's right to privacy where any covert surveillance can be shown to be both necessary and proportionate and where it has been authorised by an appropriately designated officer within the organisation. Thus, it is important to note that the requirements of RIPA provide protection for both the Council and the individual officers involved and should not be viewed as a mere exercise in bureaucracy

2.3 When carrying out such surveillance or using such sources officers should also bear in mind the **Codes of Practice** on Covert Surveillance and the Code of Practice on Human Intelligence Sources issued by the Home Office.

3. SCOPE AND DEFINITIONS

3.1 This policy applies in all cases where "directed surveillance" is being planned or carried out and "covert human intelligence sources" are used or planned to be used.

3.2 Directed surveillance is defined as surveillance which is covert, but not "intrusive" and undertaken:

- for the purposes of a specific investigation or specific operation
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not the person is specifically identified for the purposes of the investigation or operation).

3.3 Directed surveillance does not include surveillance which is an immediate response to events or circumstances where it is not reasonably practicable to obtain an authorisation as set out in this Policy.

3.4 Directed surveillance does not include intrusive surveillance. Surveillance becomes intrusive if the covert surveillance is carried out in relation to anything taking place on any residential premises or in a private vehicle and involves the presence of an individual or surveillance device on the premises or in the vehicle. The Council does not have the power or ability to authorise intrusive surveillance.

3.5 To fall within the meaning "use of a covert human intelligence source" there must;

- be a source, and
- the use of that source must be covert

A person is a "source" if they establish or maintain a personal or other relationship with someone else for the covert purpose of;

- using the relationship to obtain information or to provide access to any information to another person, or
- covertly disclosing information obtained by the use of or as a consequence of the existence of such a relationship

3.6 In everyday language a "source" is an informant or officer working undercover. The other party to the relationship with the source must be unaware of the use or disclosure of information obtained as a result of the relationship.

4. NEED FOR AUTHORISATION AND JUDICIAL APPROVAL

4.1 Whenever it is proposed to conduct directed surveillance or to use a covert human intelligence source an authorisation should be sought under Part II of the Regulation of Investigatory Powers Act 2000. The authorisation does not take effect until such time (if any) as the Magistrate has made an order approving it

5. GENERAL RULES OF AUTHORISATIONS

Necessity and Proportionality

5.1 An authorisation should not be granted unless the directed surveillance/use of covert human intelligence source is both necessary and proportionate.

5.2 In terms of **necessity**, the directed surveillance/use of covert human intelligence source must be considered to be necessary to the operation on the following grounds:

- for the purpose of preventing or detecting conduct which constitutes one or more criminal offences

and

- the offence is punishable by a maximum term of at least 6 months of imprisonment (this applies only to direct surveillance and not CHIS)

or

- is an offence under:
  - section 146 of the Licensing Act 2003 (sale of alcohol to children)
  - section 147 of the Licensing Act 2003 (allowing sale of alcohol to children);
  - section 7 of the Children and Young Persons Act 1933 (sale of tobacco to persons under eighteen)

5.3 Even if the proposed activity is considered to be necessary, the person considering the application for authorisation must consider whether the activities are also **proportionate**.

5.4 The following elements of proportionality should therefore be considered;

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

5.5 The proposed activity will not be proportionate if;

- the intrusiveness is excessive in relation to the value of the information to be obtained,

or

- the information sought could be obtained by less intrusive means

5.6 Where an individual is suspected of claiming a false address in order to abuse a school admission system operated by the Council it is likely that a RIPA Authorisation is not necessary as less intrusive and overt means could be explored to obtain the information required.

5.7 The Authorising Officer should consider the issue of proportionality with particular care in relation to relatively minor offences, instead, other less intrusive methods such as general overt observation of the location should be used. In rare instances where such offences are especially problematic or occurring with particular frequency and the problem cannot be resolved by overt measures, RIPA authorisations may be considered appropriate but care should be taken to ensure that the amount of private information obtained is kept to the minimum necessary.

Collateral Intrusion

5.8 "Collateral intrusion" means intrusion into the privacy of persons other than those who are the subject of the investigation. Measures should be taken to minimise both the risk of such intrusion and the extent of such intrusion. An application for authorisation should consider the risk of such intrusion and the Authorising Officer must take such risk into account in reaching a judgment as to whether or not the

proposed directed surveillance/use of covert human intelligence source is proportionate. If the investigation unexpectedly interferes with the privacy of persons who are not covered by the authorisation, the Authorised Officer should be informed.

Management of Covert Human Intelligence Sources

5.9 An Authorising Officers should not grant an authorisation for use of a covert human intelligence source unless he/she is satisfied of the following;

(a) that at all times there will be an officer who will have day-today responsibility for dealing with the source on behalf of the Council and for the source's security and welfare

(b) that at all times there will be another officer (senior to the officer having responsibility under (a) above) who will have general oversight of the use made of the source

(c) that at all times there will be an officer responsible for maintaining a record of the use made of the source, and

(d) that records maintained by the Council that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons

5.10 The safety and welfare of the source and foreseeable consequences to others should be taken into account in deciding whether or not to grant an authorisation. A risk assessment determining the risk to the source in acting as a source of information to the Council, and in particular identifying and assessing the risks should the identity of the source become known, should be carried out. The welfare and security of the source after the operation has ceased should be considered at the outset. The officer having responsibility under 5.9(a) above (i.e. the officer with day-to-day responsibility for the source) should report to the officer having general oversight any concerns about the personal circumstances of the source, insofar as they might affect.

- the validity of the risk assessment
- the conduct of the source, and
- the safety and welfare of the source

5.11 If appropriate such concerns should be reported to the Authorising Officer who will need to determine whether or not to allow the authorisation to continue.

6. WHO CAN GRANT AN AUTHORISATION?

6.1 Subject to 6.4 below, the law permits authorisations for directed surveillance and use of covert human intelligence sources to be granted by officers of at least Head of Service status.

6.2 A list of those Officers designated as Authorising Officers is shown as Annex A to this document. Once an application has been granted by the Authorising Officer, the authorisation then requires judicial approval before it can take effect.

6.3 Authorising Officers should not authorise investigations in which they are directly involved.

6.4 In the following instances an authorisation may only be granted by the Chief Executive, and in his absence, by any of the authorising Executive Directors for RIPA surveillance involving the;

a) use of a juvenile Covert Human Intelligence Source (CHIS).

b) surveillance involving the potential acquisition of confidential information. Confidential information means information which is; legally privileged information, confidential personal information or confidential journalistic material.

6.5 An Authorising Officer will receive training and is not able to authorise before then. Thereafter, each Authorising Officer shall receive further training/refresher training on at least a biennial basis.

6.6 The Senior Responsible Officer for RIPA, as recommended in the revised Code of Practice, is the Executive Director of Delivery.

7. THE PROCESS OF OBTAINING AN AUTHORISATION

7.1 The Investigating Officer seeking an authorisation should apply through their own line management structure unless it is impracticable in the circumstances (e.g. because no Executive Director, Director or Assistant Director in the relevant department is available).

7.2 An application for authorisation for directed surveillance or use of covert human intelligence sources should be made in the appropriate standard form which is available via the Home Office website at:
https://www.gov.uk/government/collections/ripa-forms--2

7.3 Both the Investigating Officer seeking the authorisation and the Authorising Officer shall have regard to any guidance notes issued by the Home Office and the Legal Service, on the use of those forms.

7.4 The Authorising Officer shall return the completed form to the Investigating Officer. The Investigating Officer will be using the Judicial Application /Order form at Annex B of the Home Office Guidance, seek judicial approval via a Magistrate in order for the application to take effect:
https://www.gov.uk/government/collections/ripa-forms--2

7.5 The authorisation does not take effect until such a time (if any) as the Magistrate has made an order approving it.

7.6 In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. If the Magistrate refuses to approve an authorisation, the authorisation is quashed.

7.7 A copy of the Form and record of the Magistrate's decision (on the Judicial Application/ Order Form at Annex B of the Home office Guidance) will be provided to the RIPA Monitoring Officer after the hearing for it to be added to the Central Record.

7.8 The Borough Solicitor has already designated (under section 223 of the Local Government Act 1972) that certain Investigating Officers can present RIPA applications in the Magistrates Court.

8. DURATION OF AUTHORISATION

8.1 In the case of directed surveillance, written authorisations cease to have effect after three months (unless renewed). In the case of covert human intelligence sources an authorisation expires after four months if the source is a child and one year if the source is an adult.

9. REVIEW OF AUTHORISATION

9.1 Once granted an authorisation should be reviewed regularly to assess whether or not the investigation continues to be necessary and proportionate. The date of review is event driven, for example a test purchasing application should be reviewed after the date of the test purchase.

9.2 The Authorising Officer should specify how often a review should take place and use the appropriate form from the Home Office (see 7.3 above) to conduct a review (i.e. a review of the use of directed surveillance or reviewing the use of covert human intelligence source.) This information will be held on the Central Record.

10. RENEWAL OF AUTHORISATION

10.1 Judicial approval is required if an authorisation is being renewed. An application for renewal of authorisation should not be made until shortly before the authorisation is due to expire. An authorisation may be renewed more than once for at least three months in the case of directed surveillance or, in the case of covert human intelligence source, one year.

10.2 An application for renewal should be made to the officer who granted the original authorisation unless there is very good reason not to do so (e.g. because the original authorising officer is on annual leave).

10.3 Applications for renewal should be made using the appropriate Home Office forms (i.e. renewal of directed surveillance or renewal of authorisation to use covert human intelligence source). Officers seeking an authorisation for renewal and Authorising Officers shall have regard to Code of Practice issued.

10.4 Once the application has been renewed by the Authorising Officer the completed Form will be provided to the Investigating Officer who will seek judicial approval (see 7.5-7.8) via Magistrate in order for the renewal to take effect. The renewal does not take effect until such time (if any) as the Magistrate has made an order approving it. This information will be held on the Central Record.

11. CANCELLATION AND CEASING OF AUTHORISATIONS

11.1 The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she believes that the investigation is no longer necessary or proportionate. If the original Authorising Officer is no longer available, the duty falls upon the person who has taken on that role. All authorisations should be cancelled or renewed before they cease to have effect.

11.2 Although authorisations cease to have effect after the relevant time expires (see paragraph 8) an authorisation should be reviewed, renewed or cancelled before the expiration of the time limit.

11.3 As soon as a decision is taken to cease the operation an instruction must be given to those involved to stop the directed surveillance/using the covert human intelligence source. A form (see 7.2 above) recording the cancellation should be completed and forwarded to the RIPA Monitoring Officer for inclusion in the Central Record.

12. ROLE AND DUTIES OF SENIOR RESPONSIBLE OFFICER (SRO)

12.1 The Council's SRO is the Executive Director – Delivery (Kevin Gibbs) and has the following responsibilities;

- Central responsibility for quality control of the RIPA process including providing comments/ advice for future applications
- Management of records in accordance with paragraph 13 below.
- Keeping the Central Record (a register of all authorisations) updated.

12.2 Any Authorising Officer seeking guidance in authorisations or any RIPA related matter should contact the Strategic Manager – Case Management Unit.

13. RECORDING AUTHORISATIONS / REVIEWS / RENEWALS / CANCELLATIONS

13.1 There shall be a Central Record which shall be kept by the RIPA Monitoring Officer. The role of the Central Record is to keep a complete record of all authorisations and to monitor the quality of authorisations. There will also be a summary record maintained of all the completed forms.

13.2 A copy of the originals of forms authorising or cancelling directed surveillance or use of a covert human intelligence source should be sent by internal email to the SRO. The SRO shall retain all such forms for a period of not less than three years. A copy of such forms shall be retained by the relevant department for at least three years. The original forms shall be retained by the relevant department together with;

- a record of the period over which the surveillance has taken place
- the date and time when any instruction was given by the Authorising Officer

Relevant departments must ensure that any data is processed in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

13.3 In the case of use of covert human intelligence sources, records should be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source.

Records to be kept in relation to Covert Human Intelligence Sources

13. 4 The following matters must be included in the records relating to each source;

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other that the authority maintaining the records;
(d) the means by which the source is referred to within each relevant investigating authority
(e) any other significant information connected with the security and welfare of the source;
(f) any confirmation made by the person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source
(g) the date when, and the circumstances in which, the source was recruited;
(h) the identities of the persons who, in relation to the source;

I. has day to day responsibility for their security and welfare;
II. has oversight of the use made of the source
III. has responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons specified in (h) above have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him in relation to his activities as a source;
(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
(l) the information obtained by each relevant investigating authority by the conduct or use of the source;
(m) any dissemination by that authority of information obtained in that way; and
(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

14. CODES OF PRACTICE

14.1 Two Codes of Practice have been issued by the Secretary of State relating to Directed Surveillance and Covert Human Intelligence Sources (CHIS) respectively. These came into force on 6 April 2010. The updated version of the current guidance (updated 20 September 2018) is available on the gov.uk website https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

15. TEST PURCHASING AUTHORISATIONS

15.1 By their nature all test purchase operations are covert and conducted for a specific operation. When planning test purchase activities the Officer in Charge (OiC) of the specific operation must consider the application of RIPA, with regard to both Direct Surveillance and CHIS.

15.2 The Assistant Surveillance Commissioners report of 2015 made a number of observations with regard to the application of RIPA to such operations, including:

- The IPCO Procedures and Guidance of 2014 (previously issued by the OSC) make reference to the desirability of obtaining authorisation where covert recording equipment or an observing officer are deployed (repeated at point 244 in the procedures and Guidance of 2016);
- The BRDO Code emphasises the Chief Surveillance Commissioners' guidance on this aspect of operations
- The introduction of the 'Serious Crime Test' clearly indicates the government's view that authorisation is appropriate.

15.3 Test purchase operations relating to alcohol are considered within the relevant RIPA Codes of Practice. These indicate that where a juvenile has been employed other than as a CHIS, and either covert equipment is used or an adult is observing, a Direct Surveillance authorisation must be considered

15.4 The need for a Directed Surveillance authorisation will be determined by whether it is likely that private information will be obtained about a person. The OiC must have regard to this policy above when considering this.

15.5 Where there is to be any prolonged surveillance or repeated attempts at the same premises, an authorisation for a CHIS must also be considered. Officers should note that where a CHIS is used, the meaning of "information" is not restricted to private information.

15.6 Where the OiC does not apply for an authorisation for either Directed Surveillance or the use of a CHIS, their rationale must be recorded and retained on file for a period of three years. These records will be subject to review by the Monitoring Officer and will be available for examination by IPCO.

16. CCTV

16.1 Because CCTV is usually overt (i.e. members of the public are made aware that a CCTV system is in operation) an authorisation is not normally required for the use of CCTV material. However, there may be occasions when a covert CCTV system is used for the purposes of a specific investigation or operation in which case an application for directed surveillance may be required. The advice of the RIPA Monitoring Officer should be sought in such circumstances.

16.2 In the event of a Police request for directed surveillance using CCTV cameras they will need to follow their own internal procedure for obtaining authorisation in the first instance. In such cases a copy of the relevant Police authorisation should be obtained by the Officer receiving the request and forwarded to the RIPA Monitoring Officer to confirm its validity.

17. SOCIAL NETWORK SITES (SNS) – ONLINE INVESTIGATIONS (TO BE READ WITH ANNEX C)

17.1 The Surveillance Commissioner has made a series of comments about local authorities accessing information available on the internet. There was concern expressed that they were doing this without direction, oversight or regulation and reiterated the view that certain activities would require authorisation.

17.2 These concerns were raised again in the report of 20161 and a letter was sent to all local authorities to highlight the matter. The OSC Procedures and Guidance July 2016 (now under IPCO), point 289, Covert Surveillance of Social Networking Sites, is reproduced at Annex B The use of the internet to gather information to profile targets prior to and/or during an operation may be considered Directed Surveillance

17.3 The risk of Collateral Intrusion is also likely to be an issue and must be fully considered as part of any assessment of the application of RIPA prior to the activity taking place. All Officers proposing to access social media must be familiar with the relevant codes of practice and guidance listed at Annex B. They should have particular regard to paragraphs 3.10 to 3.17 of the Code relating to Directed Surveillance and paragraph 4.11 to 4.17 of the Code relating to the use of a CHIS when considering the application of RIPA.

17.4 Where the activity is likely to require an ongoing, covert, relationship with other SNS users, this may come within the parameters of a CHIS. Where such activities are contemplated but no authorisation is sought, the Officer in Charge must record their reason and retain this in compliance with the policy. On-line investigations shall only be conducted on equipment designated for that purpose. Such equipment will not be attached to the Council's network. Officers must not use personal accounts for accessing social media as part of their enquiries.

17.5 Only Officers who have attended suitable training will be authorised to conduct on-line investigations under a RIPA authorisation. Officers must be familiar with, and

[1] *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers 2016 - 2017, https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202016-17.pdf*

have regard to, the Council's policy on the use of Social Media section in the Code of Conduct for Staff.

17.6 Finally, all officers who use social media in their day to day work activities must complete the on-line RIPA course accessed through DORIS. Anyone requiring advice must contact Sean Murphy, Public Protection Manager.

18. NON-COMPLIANCE

18.1 Evidence gathered in breach of the procedures described in this document will not automatically be excluded by a Court. However, the defendant may argue that reliance by the prosecution on evidence obtained in breach of Article 8 – right to privacy denies him his right to a fair trial as guaranteed by Article 6 and that the case should not proceed. In addition, the admissibility of evidence is a matter for the Courts discretion, and they will decide whether the evidence is put forward in such a way that the proceedings are fair as a whole. Therefore, RIPA should be complied with at all times.

18.2 Apart from the above, non-compliance with RIPA may still result in a claim against the Council for a breach of Article 6 and/or 8 of the European Convention of Human Rights a complaint to the Local Government Ombudsman referral to a RIPA Tribunal censure by IPCO.

ANNEX A - RIPA AUTHORISING OFFICERS:

Chief Executive: Timothy Wheadon

Executive Director of People Services: TBC

Executive Director of Delivery and SRO: Kevin Gibbs

Assistant Director – Contract Services: Damian James

Public Protection Manager: Sean Murphy (also Designated Person for Communications Data)

Head of Community Safety: Alison O'Meara

ANNEX B - RIPA GUIDANCE

Guidance for applicants and designated person considering necessity and proportionality.
www.gov.uk/government/publications/guidance-notes-for-chapter-ii-application

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance.
www.gov.uk/surveillance-and-counter-terrorism

IPCO Procedures and Guidance (and previously issued by OSC).
Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources **(**available at www.ipco.org.uk**)**

ANNEX C - INVESTIGATORY USE OF SOCIAL NETWORK SITES (SNS)

Introduction

This document sets out how Services within Bracknell Forest Council (the Council) will use social network sites and should be read in conjunction with other relevant policies including:

ICT Policy and User Usage Agreement
Security Policy
Code of Conduct of Staff

Purposes for using SNS

Services will access SNS in different ways:

- Open and overt exchange of information with users;
- Viewing information about users which is openly available, without any need to log in to the SNS, in order to verify information. This may be done overtly or covertly; and
- Covertly viewing information and/or engaging with a user to obtain information about them another person or a business. These are explained in more detail below.

The purposes for which Services may wish to access SNS will include but is not limited to the following and it will be for the officer to determine which of the methods of accessing the SNS is appropriate according to the circumstances:

- Monitoring activities of licensed premises with regard to irresponsible drink promotions.
- Monitoring the promotion of bands that are known to have caused complaints relating to noise levels.
- Viewing personal areas to verify the details provided by a benefit claimant (living alone, fitness to work, etc)
- Checking residency with regard to school catchments areas
- Gathering information which may later become intelligence used to direct resources.
- Obtaining any information which provides evidence of a prima facia offence.
- Open and overt exchange of information with users

For the purpose of this document ‘overt use’ is defined as the use of a SNS by Services in an open manner with the intent of sharing information with individual stakeholders or groups of stakeholders.

Those individuals or groups will be aware of our presence on their area (wall, space, page, etc) of the SNS. This will include areas used by businesses for advertising their products or services (e.g. the ‘fan’ section on Face Book). Where information is obtained from such areas which may lead to any form of enforcement action, this information must be handled in accordance with paragraph 6 of this document.

When employees of a Service are engaging openly with a business or individual as a representative of the Council they will operate in accordance with the policy. Services should set up corporate accounts which do not supply private information about individual

employees. Access will normally be via networked computers which are operated and maintained in accordance with the Council's policies.

SNS access in this manner will not require Regulation of Investigatory Powers Act (RIPA) authorisation. Officers must still act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

Access will be monitored in accordance with the Policy and other relevant corporate strategies.

Viewing information about users which is openly available

Although users will not be aware of activity undertaken by Officers in viewing their SNS pages, subject to the considerations referred to below, this may not classed as covert surveillance for the purpose of RIPA.

There is unlikely to be a reasonable expectation of privacy by the user who has published this information about themselves and made it freely available for anyone to view.

Information that is considered as being openly accessible is only that which is capable of being accessed without logging on to the SNS as a user. If you need to log on to an SNS to access information about a person, that must be done either overtly or in accordance with the requirements for the covert acquisition of information.

Consideration should be given to the means of recording the information viewed and by what method. This information would also be required in order to comply with the provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) where applicable.

Investigators should refer to their Service procedure notes for the method of doing this. Officers must still act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

Notwithstanding the above, those viewing information that is freely and openly available on an SNS must always consider in each case whether the user who's SNS is being viewed;

might reasonably be aware of just how much of their personal information is openly accessible, and
whether the SNS user might have inadvertently given public access to certain information.

This is not an easy task as it involves trying to guess what the SNS user was thinking. The more intimate or sensitive the personal information is likely to be, the greater the caution that should be exercised in viewing and recording the information. You may be required to demonstrate proportionality and necessity in relation to the user's Article 8 rights and in determine whether such information can properly be used in relation to the matter being investigated.

In circumstances where officers are considering accessing SNS for the purpose of obtaining information which is not required for a criminal investigation, the activity being contemplated would fall outside the scope of RIPA. However, in order to ensure that

proper regard has been had to the Article 8 rights of the individual, consideration should be given to completing a “Consideration of RIPA to Directed Surveillance activities” form.

Covertly engaging with a user to obtain information

For the purpose of this document covert use is defined as the use of SNS by Services to gather information to direct their activities in relation to the prevention and detection of crime, the apprehension or prosecution of offenders or to take any other action in respect of a regulatory breach, except where that information is being obtained either by open and overt interaction with the user or where the information is openly available.

Before accessing an SNS covertly the investigating officer must give consideration to the provisions of RIPA. It is possible that the activity may be classified as Directed Surveillance or that the accessing officer may be acting as a Covert Human Intelligence Source (CHIS). The application for access will record those considerations along with the conclusion. Where it is determined that no RIPA application is required the appropriate paperwork on the case file will be endorsed to that effect by the appropriate officer or manager. If a RIPA authorisation is required then the Councils RIPA procedures together with any complementary Service policy for that process will be followed and access not granted until such time as the activity has been properly authorised in accordance with the legal process.

Where an officer wishes to access an SNS with the intent of gathering information about a business or individual (target) without the knowledge of that target, they will deemed to be acting covertly for the purpose of this document. Covert access will always be considered as an investigation and all officers must act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

For covert operations an anonymous user account will be set up which cannot be traced back to the Service or any individual employed by the Council. These accounts will be maintained by the individual Service who will put in place processes for controlling and monitoring the access and use of the accounts.

Where there is any doubt, advice should be sought from the line manager or the Public Protection Manager.

Access will be monitored in accordance with the Policy and other relevant corporate strategies.

Human Rights and Data Protection Act considerations

During an investigation an important consideration is the right of respect for private and family life (Article 8) and any interference with this right must be lawful, necessary and proportionate. Whilst RIPA provides a framework that enables specific types of interference with this right e.g. for covert surveillance to be lawful, the Human Rights aspects must always be considered even where RIPA is not engaged.

When viewing SNS as described above, officers must consider whether the information that has been published on an SNS attracts any reasonable expectation of privacy. Guidance suggests that if any expectation of privacy is claimed it is unlikely to be

reasonable given the various warnings that are usually contained on the SNS privacy policies.

Interference with any privacy right claimed will require a legal basis, which for investigations undertaken by the local authority will be found in the relevant legislation e.g. Health and Safety at Work Act or trading standards legislation. The carrying out of investigatory work that does not trigger the application of RIPA remains a lawful interference with any right of respect to private and family life, provided activity is both necessary and proportionate.

Any personal information that is collected from viewing SNS must be held and processed in accordance with the Data Protection Act, as well as any investigation and evidential protocols that are in place.

Authorisation

All access to SNSs must be authorised in advance by an appropriate Team Leader/Manager in accordance with the Policy. This authorisation is in addition to any authorisation that might be required under RIPA and it does not detract from the responsibility to keep appropriate records of the SNS access and the information viewed and used.

Equipment

Officers must not under any circumstances use their personal IT equipment or any other IT equipment that is not provided by the Council for undertaking any of the activities to which this document relates.

The Service should provide dedicated standalone computers for covert internet activity. Networked computers must not be used for this type of exercise. Printed information obtained from networked computers will not normally be sufficient for evidential purposes and officers should only resort to using these where there is no other means available to them.

SNS information is primarily transmitted and stored in a digital format and it is important that this is captured in such a way that the integrity of the information is not compromised. There are a number of published guides that are relevant to the capture, storage and production in court of computer based evidence. All officers charged with the production of computer based evidence which may result in legal proceedings should be familiar with these documents.[2]

Criminal Procedures and Investigations Act 1996 (CPIA)

Where officers acquire information which may result in regulatory action they must ensure they secure this information in such a way that the Service can discharges its duties under the CPIA in any future proceedings. Regulatory action includes, but is not restricted to, the following:

[2] Storage, Replay and Disposal of Digital Evidential Images, Home Office Publication 53/07
Digital Imaging Procedure v2.0 November 2007, Home Office Publication 58/07
Good Practice Guide for Computer-Based Electronic Evidence, ACPO 2007

Prosecution, Simple Caution, Administrative Penalties, Written or Verbal warnings relating to criminal breaches
Issuing of Fixed Penalty Notices, Penalty Notice for Disorder or other statutory fines
Suspension or review of any benefits
Review of any licences issued by the Authority
Use of Civil sanctions to prevent future breaches of legislation

Personal use

The Code of Conduct of Staff policy sets out the standards expected of employees of the Council in their personal use of Social Network Sites. Employees should ensure that in their personal use of SNS they do not provide details about their employment that might compromise their health & safety. This is particularly relevant where they are engaged in enforcement activities in their routine work.