Agenda Item 9

Policy and Resources Committee
10 July 2017

Proposed Amendments to the Covert Surveillance Policy

Purpose of report

To ask Members to approve amendments to the current Covert Surveillance Policy to provide guidance limiting the covert use of social media in investigations in accordance with Information Commissioner best practice.

Attachment

Appendix 1 – Current Covert Surveillance Policy

1.0 Background

1.1 The Protection of Freedoms Act 2012 changed the procedure for the authorisation of local authority surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA), As a result of the Act, local authorities may only authorise directed surveillance (covert surveillance on individuals in public places) or use a covert human intelligence source (CHIS) when the following conditions are met:

- The authorisation is for the purpose of preventing or detecting conduct which constitutes a criminal offence; and
- The criminal offence is one which is punishable by a maximum term of at least six months' imprisonment or is an offence under:-
    - s146 of the Licensing Act 2003(a) (sale of alcohol to children);
    - s147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
    - s147A of the Licensing Act 2003(b) (persistently selling alcohol to children);
    - s7 of the Children & Young Persons Act 1993 (c) (sale of tobacco etc to persons under 18)

In addition to restricting the use of directed surveillance and CHIS, both types of activity will require subsequent authorisation by a JP.

1.2 The Council updated its policy in 2013 to reflect these changes. Also as a consequence the Council ceased undertaking covert surveillance and instead relies on overt activity such as investigation of fly-tipped material to identify the offenders.

1.3 However the Council is still subject to periodic RIPA Inspections and is therefore required to continue to training officers in the provisions of RIPA and keep its policy up to date.

1.4 One area of activity which has the potential to extend into covert surveillance is the use of social media. A number of complaints which require further action by the Council now provide posts gathered from social media sites as evidence to support the complaint. For this reason it is proposed to insert guidance to officers in their use of social media as outlined below.

2.0 Revisions to the approved Covert Surveillance Policy

2.1 It is proposed to insert the following sections into the policy as follows (with subsequent paragraphs renumbered:

2.2 **4.27 *Covert surveillance of Social Networking Sites (SNS)***

4.28 Occasionally officers may be alerted to information on social media which may be pertinent to an investigation. When using social media sites for gathering evidence to assist in enforcement activities, officers should note that 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 specific SNS being used works, particularly in relation to privacy settings.

4.29 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 routinely regard it as "open source" or publicly available. The author has a reasonable expectation of privacy if access controls are applied. In addition 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.

4.30 To ensure compliance with regulations:

- *Officers must not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA. If it necessary and proportionate for the Council to covertly breach access controls, an authorisation for Directed Surveillance will be required. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer.*
- *Officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute their investigation.*
- *Legal advice should be taken in advance as to whether repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status for a specific investigation will require RIPA authorisation and approval by a Magistrate. This advice and the justification report for the monitoring should be retained for future reference in case of challenge.*

4.31 Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

3.0 Equality and Diversity Implications

3.1 Applying the investigatory powers given to the Council in accordance with the legislation noted above is designed to ensure that there should be no equality and diversity implications to the use of the powers.

4.0 Legal Implications

4.1 Failure to obtain a RIPA authorisation where a person's rights under the European Convention of Human Rights are interfered with may leave the Council open to civil action for damages under the Human Rights Act 1998.

5.0 Risk Management

5.1 As noted in the legal implications above, the Council could be open to civil action for damages if the appropriate authorisation is not sought

6.0 Resource and Financial Implications

6.1 There are no resource and financial implications arising directly from this report. If the Council does make use of the RIPA provisions in future, there will be resource implications involved in seeking a magistrate's consent to an authorisation but these are have been previously found from existing legal budgets.

7.0 Constitutional Implications

7.1 Part 3.2 of our Constitution identifies the officers with delegated powers to apply the policy. No amendments to this are required at present.

8.0 Implications for Our Customers

8.1 The proposed changes are unlikely to significantly affect the council's relationship with its customers although they will provide clarity on how the Council will view social networking sites.

9.0 Corporate Outcomes

9.1 The revised policy links to the corporate outcome of Councillors and staff with the right knowledge, skills and behaviours

10.0 Recommendation

10.1 The Committee is recommended to approve the insertion of the additional text outlined in section 2 of this report into the council's covert surveillance report.
Reason – to ensure that East Northamptonshire Council is compliant with the Protection of Freedoms Act 2012

Legal	**Power:**	Regulation of Investigatory Powers Act 2000; Protection of Freedoms Act 2012			
	Other considerations:	the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010; to the Protection of Freedoms Act 2012; and the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.			
Background Papers:	• **Policy & Resources Committee 9 September 2013 – Covert Surveillance Policy**				
Persons Originating Report:	Sharn Matthews, Monitoring Officer ☎ 01832 742108 ✉ smatthews@east-northamptonshire.gov.uk				
Date: 27 June 2017					
CFO		**MO**		**CX**	