Report to the Cabinet
Meeting to be held on Thursday, 19 January 2017

Report of the Director of Governance, Finance and Public Services

Electoral Divisions affected:
All

Regulation of Investigatory Powers Act 2000: Annual Report to Cabinet
(Appendices A, B, C and D refer)

Contact for further information:
Ian Young, (01772) 533531, Director of Governance, Finance and Public Services
ian.young@lancashire.gov.uk

Executive Summary

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for certain public bodies, including local authorities, to use "covert surveillance" to gather information about individuals without their knowledge for the purposes of undertaking statutory functions in connection with the prevention or detection of crime. The use of RIPA by a public authority provides protection against a claim of infringement of the right to respect for a private and family life, home and correspondence.

RIPA activity and authorisations are governed by Home Office Codes of Practice and Guidance issued by the Office for Surveillance Commissioners (OSC).

Local authorities are subject to regular inspections from the OSC.

Members are required to review the use of RIPA and set the policy (attached as Appendix A) at least once a year. Elected members cannot be involved in decisions on specific authorisations, but have oversight of the process via the reporting requirement to the Overview and Scrutiny Committee.

This year three additional policies linked to the use of covert surveillance are submitted for approval, in relation to non RIPA surveillance (Appendix B); the use of social media and the internet in investigations (Appendix C); and a new draft CCTV Policy incorporating the codes of practice issued by the Surveillance camera Commissioner and the Information Commissioner (Appendix D).

Recommendation

The Cabinet is asked to
i. note the content of this report
ii. approve, with immediate effect, the updated corporate policies on:
    a. Non-RIPA surveillance

Lancashire County Council

b. The use of Social Media and the Internet in investigations
c. Use of CCTV

iii. Agree that the role of CCTV Manager be undertaken by the Head of Service, Legal and Democratic Services

Background and Advice

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for certain public bodies, including local authorities, to use "covert surveillance" to gather certain information about individuals without their knowledge for the purposes of undertaking statutory functions in connection with the prevention or detection of crime.

RIPA is permissive legislation, that is to say that it is not mandatory for a local authority to authorise covert surveillance under RIPA but if it does so then authorisation of surveillance in accordance with the RIPA regime, provides the local authority with a defence if the individual brings a claim against the local authority alleging that the surveillance breaches their human rights, specifically Article 8, the right to respect for private and family life, home and correspondence.

RIPA covers directed surveillance, for example the use of recording devices, photography or video to record persons suspected of being engaged in criminal activity, where there is a possibility of gaining of private information, and the use of a Covert Human Intelligence Source (CHIS), for example an informant, where the surveillance involves developing a relationship in order to obtain information.

Within the County Council, covert surveillance authorised pursuant to RIPA is used very infrequently and only in connection with Trading Standards activities, typically against rogue traders, counterfeiters or individuals engaged in selling tobacco or alcohol products to children. It is used in cases where it is important to obtain information to support potential criminal proceedings, and only where that information cannot be obtained by any other means.

RIPA activity and authorisations are governed by Codes of Practice and Guidance Issued by the Office for Surveillance Commissioners (OSC) and the Home Office.

Applications for authorisation of covert surveillance are submitted using standard home office forms, to designated authorising officers, currently the Head of Trading Standards and three Trading Standards Managers. The managers assess the information provided and need to be satisfied that the surveillance is both necessary for the prevention of crime, and proportionate – i.e. not a sledgehammer to crack a nut. If authorised, the application must then be put before a magistrate for approval before the activity can take place.

Directed surveillance authorisations last for 3 months and apply where there is a possibility that private information may be obtained as a result of the activity.

CHIS authorisations last for 12 months, and cover activity where a relationship may be built up by a source in order to gain information.

Both need to be regularly reviewed to ensure that the surveillance remains necessary and proportionate.

The OSC inspect local authorities every 3 years and examine a sample of authorisations which have been granted in the period since the last inspection. The OSC are due to inspect the authority on 28 February 2017.

Members are expected to oversee the use of RIPA and set the policy at least annually. A copy of the Corporate Policy and Guidance on the Regulation of Investigatory Powers Act is attached as Appendix 'A'.

RIPA Activity

Since the last cabinet report in February 2016 there have been 6 authorisations for the use of surveillance. 4 of these were for the use of a CHIS in connection with the supply of counterfeit goods over the internet, and two were for directed surveillance: one in connection with unsafe goods and one into motor vehicle fraud.

Non RIPA Surveillance

Although the focus of the OSC inspection is primarily on covert surveillance undertaken to prevent or detect crime, the authority may also be involved in surveillance activity for other purposes, for which authorisation is not permitted to be sought under the RIPA regime.

Such surveillance could leave the authority open to a claim of infringement of the right to privacy and family life, and therefore in such cases the approach of the authority has been to utilise what are called "shadow authorisations", to be put before the Director of Legal and Democratic Services for approval.

Such activity may include surveillance in relation to child protection work, and use of social media to obtain information, both in relation to internal investigations and those involving clients. Shadow surveillance may also be thought necessary where serious allegations of employee misconduct are received – for example employees carrying out inappropriate activity in work's time.

Shadow authorisations are rare. Brief reference is already made in the Corporate Policy and Guidance on the Regulation of Investigatory Powers Act to the potential need to use the principles of RIPA when surveillance **not** for the purposes of the prevention and detection of crime is being undertaken. However, it is believed that a more detailed separate policy will provide valuable guidance for employees who may need to seek shadow authorisations for covert surveillance. The draft policy submitted for approval recommends that these should only be approved by the Director of Legal and Democratic Services.

A copy of the Shadow RIPA Surveillance Corporate Policy is attached as Appendix B.

Shadow RIPA Activity

One authorisation has been granted, in September 2016, in relation to covert surveillance carried out by the Trading Standards Service, for the purposes of conducting a social experiment in relation to public attitudes to the proxy sales of alcohol.

Social Media and Covert Surveillance Policy

Increasingly the use of social media means that a wide range of personal information posted by individuals is available online. Some of this is available as "open source" material, some can only be accessed once the individual has accepted a "friend" request.

Individuals posting such material may be considered to have no or a reduced expectation of privacy in respect of the information they have posted. However, where the authority intends to search for information and use it in connection with either the prevention or detection of crime, or for the purpose of other investigations connected with employee misconduct or child protection matters for example, it is important that regard is given to guidance issued by the Home Office and by the Office of Surveillance Commissioners.

Accordingly a Covert Social Networking Checks and Surveillance Policy has been drafted which Cabinet are asked to note and approve A copy of this is attached as Appendix C.

CCTV Policy

The Information Commissioner issued its first code of practice governing the use of CCTV in 2000. This was updated in 2008.

In the past the Council has employed CCTV cameras to monitor its premises to prevent theft and vandalism, although use of such technology has not been as extensive as by district councils who help with the policing town centres through sophisticated CCTV systems.

The technology itself has developed significantly since first introduced. CCTV is no longer a simple camera device that records images to video. Most CCTV devices currently in use by the Council are digital and used both inside and outside Council premises to monitor activity. In addition, the Council uses Automatic Number Plate Recognition (ANPR) systems to enforce traffic and parking regulation and this includes body worn cameras that record both the images of and audible interactions with members of the public. The Council has on occasion also employed unmanned aerial devices (drones) to carry out building surveys to limit danger and disruption.

Reference to "CCTV systems" extends to all devices that capture images or sounds of either individuals or which are used for the purpose identifying individuals.

The increased use of such systems which either deliberately or inadvertently monitor the conduct of individuals has led to heightened concern as to the extent of surveillance, the use to which it is put and whether or not it is justified. Local authorities have been a particular target of media criticism highlighting surveillance being used, for example, to check whether applicants for school places live in the relevant area, capturing dog owners who do not pick up faeces and using camera devices embedded in wheelie bins to monitor waste.

The perceived unwarranted use of surveillance systems has led to the strengthening of the regulatory landscape through the introduction of the Protection of Freedoms Act 2012. The first Surveillance Camera Commissioner was appointed under this Act alongside the introduction of a new surveillance camera code. As surveillance activities record personal data, the Information Commissioner also strengthened its stance on surveillance by publishing "A data protection code for surveillance cameras and personal information" in 2015.

The surveillance camera code established twelve basic principles that apply when any CCTV system is used. These are repeated in the data protection code.

The twelve principles are as follows:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only

take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

The present Council policy on the use of CCTV does not take account of the recent expansion of regulation and codes of practice and fails to address any of the twelve principles set out above; it simply refers to earlier guidance offered by the Information Commissioner.

Whilst a Surveillance Camera Commissioner has been appointed, he does not play any direct role in the enforcement of the guidance. Contraventions of the code(s) which amount to breaches of the Data Protection Act 1998 would be enforced by the Information Commissioner. However, the Office of the Surveillance Commissioner (OSC) has been given a role in the general overview of CCTV systems and this now forms part of the three yearly inspection carried out by that office. The Council's inspection of its RIPA actions by the OSC is due to take place on 28 February 2017 and the Inspector has asked to see our CCTV policy.

The current policy is not fit for purpose against the existing regulatory framework and what is expected of local authorities. A group was formed in September 2016 with a remit to review and update the Council's CCTV policy to ensure that it embraces the twelve principles. Representatives of Facilities Management, Information Governance, Legal and Democratic Services and Audit have therefore produced a new draft policy which is attached to this report at Appendix D.

This draft policy addresses each of the twelve principles and seeks to ensure that those services responsible for introducing and operating CCTV systems give due consideration and weight to the matters set out in the code(s) particularly privacy, security, technical competence and accuracy and information governance.

Further work is required to identify all relevant CCTV systems, to compile a central register, to ensure that those operating CCTV systems are aware of the new policy and what is required of them thereunder. It is proposed that the Head of Service for Legal and Democratic Services act as the CCTV Manager under the policy as part of his role and further meetings of the group will be held to plan how the policy will be rolled out.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

The use of RIPA, where permitted, provides a defence to a local authority where an individual alleges that their human rights have been contravened.

Non RIPA surveillance is subject to a similar process within LCC, which will enable the authority to show that it has appropriately considered necessity and proportionality in any case where there is an allegation that human rights have been breached in a situation not involving the prevention and detection of crime.

Guidance on the use of social media in investigations will ensure that an individual's human rights are considered in the context of the use of information published by the individual online.

The current CCTV policy is out of date and requires updating in line with current regulations and guidance and to ensure it is in line with the technology available and in use.

Financial

If challenged, the Council could be liable to pay a financial penalty in respect of actions held to be an infringement of an individual's right to a private and family life, home and correspondence.

Legal

There is a possibility of legal action against the authority if covert surveillance is held to have breached an individual's human rights.

Equality and Cohesion

The use of RIPA principles requires consideration of the necessity and proportionality of surveillance and as part of this, equality and cohesion issues would be considered.

Human Rights

The use of RIPA and associated principles is recommended in the context of consideration of the impact of surveillance activities on the right to privacy, a family life, home and correspondence.

Crime and Disorder

LCC Trading Standards Service has a statutory duty to investigate criminal offences committed under a wide range of public protection legislation. In a small minority of cases the use of covert surveillance may be the only means of progressing the investigation.

Personnel

All activities are risk assessed to ensure the health and safety of individuals is considered and any mitigating measures are implemented.

List of Background Papers

Paper	Date	Contact/Tel

N/A

Reason for inclusion in Part II, if appropriate

N/A