Information Assurance

Policies and Guidance

Surveillance Policy

1 July 2013

Document Version: v3

Review Date: 1 July 2015

Owner: Information Governance Manager

Document History

Revision Date	Version Number	Summary of Changes
01012013	V0.1	Original draft
12022013	V0.2	Suggestions for amendments by Sarah Khawaja, Legal Services
19072013	V0.3	Suggestions for amendments by Linda Fletcher, Corporate Counter Fraud Team, & presentation comments via IMPB

Index

Chapter	Title	Page
1.	Introduction	4
2.	Scope	5
3.	Aim	5
4.	Applicability to investigations carried out by or on behalf of Leicester City Council	6
5.	Review and Maintenance	6
6.	Legal Requirements	6
7.	Policy Statement	7
8.	Objectives	7
9.	Responsibilities	8
10.	Surveillance Principles	9
11.	Intrusive Surveillance	10
12.	Directed Surveillance	10
13.	Covert Human Intelligence Sources	12
14.	Communications Data	13
15.	Reviews, Renewals and Cancellations of RIPA Authorisations	14
16.	Reporting Errors in RIPA Authorisations	14
17.	RIPA requests from Third Parties	14
18.	CCTV	14
19.	Surveillance of Employees	15
20.	Storage and Destruction of Surveillance Data	16
21.	Compliance with Legislation	16
22.	Complaints	17
23.	Internal Charging	17
24.	Further Guidance	18

1. Introduction

1.1 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of surveillance.

1.2 Part II of the Regulation of Investigatory Powers 2000 Act provides a statutory framework under which covert surveillance activity undertaken by the Council can be authorised and conducted compatibly with Article 8 and the Data Protection Act 1998.

1.3 The Employment Practices Code provides a framework under which surveillance activity of employees can be authorised and conducted compatibly with Article 8 and the Data Protection Act 1998.

1.4 Surveillance, for the purpose of the Regulation of Investigatory Powers Act 2000, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

1.5 Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

1.6 Specifically, covert surveillance may be authorised under the 2000 Act if it is either intrusive or directed:

- Intrusive surveillance is covert surveillance t hat is carried out in relation to anything taking place on residential premises or in any private vehicle

(and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);

- Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under the 2000 Act.

1.7 The grounds on which local authorities can rely on to authorise directed surveillance are narrower than those available to the police or security services. A local authority can only authorise directed surveillance of a member of the public if the designated person believes such surveillance is necessary and proportionate for the purpose of preventing or detecting crime.

1.8 In most cases the crime for directed surveillance must be an offence for which there is a minimum prison sentence of 6 months, and the surveillance must be authorised by a magistrate.

1.9 The Council must have a policy in place to ensure that such directed surveillance is carried out in compliance with the law and does not breach the human rights of any of the surveillance subjects, and that surveillance in or around the workplace is also carried out in compliance with the law.

2. Scope

2.1 The policy applies to all surveillance carried out by The Council, both external surveillance covered by RIPA authorisations and internal covered by the Employment Practices Code

3. Aim

3.1 To provide a framework for the carrying out of covert surveillance of the public and staff by the Council.

3.2 To ensure all legal obligations on the Council are met, in particular, the Human Rights Act 1998.

4. Applicability to investigations carried out by or on behalf of Leicester City Council

4.1 This policy applies to covert surveillance activities carried out by or on behalf of the Council and includes, but is not limited to, the following:

- the taking of photographs of someone in a public place or;
- the recording by video cameras of someone in a public place;
- the use of listening devices or photographic equipment in respect of activities in a house, provided the equipment is kept outside the house and the equipment gives information of less quality and detail than devices which could have been placed in the house itself
- the taking of photographs of staff in the workplace or;
- the recording by video cameras of staff in the workplace;
- acquisition of communications data e.g. email traffic, internet use logs, telephone call logs.

5. Review and Maintenance

5.1 This policy is agreed and distributed for use across the Council by the Information Management Programme Board (IMPB) on behalf of the Operations Board. It will be reviewed bi-annually by the Information Governance Manager, who will forward any recommendations for change to the IMPB for consideration and distribution.

6. Legal Requirements

6.1 The Council is obliged to comply with all relevant UK and EU information legislation. This requirement to comply is devolved to Elected Members, staff, contractors or others permitted to carry out surveillance on behalf of

the Council, who may be held personally accountable for any breaches of Article 8 of the Human Rights Act 1998 (Right to Privacy).

6.2 The acquisition of a RIPA authorisation will equip the Council with the legal protection (The RIPA 'Shield') against accusations of a breach of Article 8.

6.3 The Council shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012

6.4 For more detailed explanations of the above see the Information Governance section of the Staff e-Handbook.

7. Policy Statement

7.1 Leicester City Council supports the objectives of the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, and the Protection of Freedoms Act 2012. This policy aims to assist staff with meeting their statutory and other obligations which covers the issues of Information Governance.

8. Objectives

8.1 The policy is intended to provide a framework for carrying out surveillance activities in compliance with the law by:

- Creating and maintaining within the organisation an awareness of the Right to Privacy (Article 8, Human Rights Act 1998) as an integral part of the day to day business;

- Ensuring that all staff are aware of and fully comply with the relevant legislation as described in policies and fully understand their own responsibilities when undertaking surveillance activities;
- Ensuring that all staff acquire the appropriate authorisations when undertaking surveillance activities;
- Storing, archiving and disposing of sensitive and confidential surveillance information in an appropriate manner.

8.2 The Council will achieve this by ensuring that:

- Regulatory and legislative requirements are met;
- RIPA and surveillance training is provided;
- All breaches of privacy, actual or suspected, are reported, investigated and any resulting necessary actions taken;
- Standards, guidance and procedures are produced to support this policy.

9. Responsibilities

9.1 The Chief Operating Officer, on behalf of the City Mayor and Strategic Directors' Board, is the Senior Information Risk Owner and has overall responsibility for Information Governance within the Council.

9.2 The Information Governance Manager is responsible for:

- Acting as the Council's RIPA Monitoring Officer
- Developing, implementing and maintaining the relevant corporate Information Governance policies, procedures and standards that underpin the effective and efficient surveillance processes;
- Support and advice to staff and managers on Surveillance;
- The production, review and maintenance of Surveillance policies and their communication to the whole Council;
- Provision of professional guidance on all matters relating to Surveillance;

- Oversight management of all privacy breaches and suspected breach investigations;
- Provision of corporate training;
- Provision, via the Intranet, of Surveillance briefing materials and, through City Learning, of on-line training;
- Management and recording of RIPA authorisations;
- Providing annual returns to national inspectors – The Office of the Surveillance Commissioner (OSC) and the Interception of Communications Commissioner's Office (IOCCO);
- Liaising with national inspection regimes, OSC, IOCCO and the CCTV commissioner to organise inspections;
- Production of an annual Information Governance Report.

9.3 The RIPA Authorising Officers will assess and authorise RIPA applications.

9.4 The Director of Finance will authorise all internal intercept requests

9.5 The Corporate Counter Fraud Team will advise and assist in all aspects of staff investigations.

9.6 All Directors will:

- Implement this policy within their business areas;
- Ensure compliance to it by their staff;
- Sign off applications for surveillance of staff;
- Take all reasonable steps to protect the Health and Safety of investigators and where appropriate of third parties involved with investigations. This should include the carrying out of risk assessments.

10. Surveillance Principles

10.1 Leicester City Council is committed to a surveillance framework that ensures:

- Requests for Authorisations are assessed to ensure the privacy of the individual is not breached unless it is necessary and proportionate to do so;
- All requests are monitored and performance indicators made available to demonstrate compliance with the legislation;
- The surveillance process is regularly audited to ensure compliance with statutory requirements and that relevant national codes of practice are followed.

11. Intrusive Surveillance

11.1 Intrusive surveillance is covert surveillance carried out by an individual or a surveillance device in relation to anything taking place on residential premises or in any private vehicle. The Council is not permitted to carry out intrusive surveillance in any circumstances.

12. Directed Surveillance

12.1 Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

12.2 The Council will use Directed Surveillance to acquire information covertly where it is appropriate and legal to do so.

12.3 At the start of an investigation, council officers applying for a RIPA authorisation must satisfy themselves that what they are investigating is a criminal offence and passes the criminal threshold test.

12.4 The appropriate Directed Surveillance application form, which will be available on the Council's intranet site, should be completed and submitted to the Authorising Officer.

12.5 Any officer completing the Directed Surveillance RIPA application form must contact Legal Services so that they can be authorised to attend the magistrate's court on behalf of the Council. This authorisation to act on behalf of the Council at the court remains valid as long as the applying officer is employed by the Council.

12.6 The applying officer must submit the signed Directed Surveillance RIPA application, once it is signed by the Authorising Officer, to the local Magistrate for approval.

12.7 If confidential information or matters subject to legal privilege are to be acquired, the Directed Surveillance may only be authorised by the Head of Paid Service or their deputy in their absence.

12.8 The Information Governance Manager will ensure there is always a minimum of three (3) trained Authorising Officers at the Council. These will be at Divisional Director level or above, and their names published on the Council's intranet.

12.9 Statistical returns for directed surveillance data acquired using RIPA will be submitted to the OSC by the Information Governance Manager upon request.

12.10 The Information Governance Manager will comply with requests from the OSC in relation to the organisation of inspections of the Council.

12.11 A Directed Surveillance RIPA authorisation may also be used if the crime threshold is not met but the offence is a criminal offence under:

(i) sections 146, 147 or 147A of the Licensing Act 2003; or
(ii) section 7 of the Children and Young Persons Act 1933

(underage sales of alcohol and tobacco).

12.12 A RIPA authorisation is not needed when it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance in an immediate response to events.

13. Covert Human Intelligence Sources

13.1 Under the 2000 Act, a person is a CHIS if:
a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

13.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

13.3 The Council may use a covert human intelligence source (CHIS) to acquire information covertly where it is appropriate and legal to do so. A CHIS covertly uses a relationship to obtain information or to provide access to any information to another person.

13.4 The crime threshold does not apply to the authorisation of a CHIS.

13.5 The appropriate CHIS application form, which will be available on the Council's intranet site, should be completed and submitted to the Authorising Officer.

13.6 The applying officer must submit the signed CHIS RIPA application, once it is signed by the Authorising Officer, to the local Magistrate for approval.

13.7 The Council will never authorise the use of a CHIS under the age of 16 to gather evidence against his parents or carers.

13.8 The Council will never authorise the use of a CHIS under the age of 18 without carrying out a special risk assessment in relation to any risk of physical injury or psychological distress to the source that may arise.

13.9 If confidential information or matters subject to legal privilege are to be acquired by the CHIS, or the CHIS is a juvenile or a vulnerable individual, the Directed Surveillance may only be authorised by the Head of Paid Service.

14. Communications Data

14.1 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services or telecommunications services. The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine external to the Council.

14.2 The crime threshold will apply only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS.

14.3 The Council will appoint a Single Point of Contact (SPoC) responsible for the acquisition of external communications data using RIPA. If the National Anti-Fraud Network (NAFN) SPoC system is not used, a trained and accredited member of Council staff must undertake this role.

14.4 If the National Anti-Fraud Network (NAFN) SPoC system is not used, the appropriate application form, which will be available on the Council's

intranet site, should be completed and submitted to the Authorising Officer.

14.5 Statistical returns for communications data acquired using RIPA will be submitted to the IOCCO by the Information Governance Manager upon request.

14.6 The Information Governance Manager will comply with requests from the IOCCO in relation to the organisation of inspections of the Council.

15. Reviews, Renewals and Cancellations of RIPA Authorisations

15.1 The applying officer must review the authorisation on a monthly basis to decide if the operation needs to continue.

15.2 RIPA authorisations must be cancelled as soon as they are no longer required. Cancellations must be authorised by the Council's Authorising Officer.

15.3 RIPA authorisations are only valid for 3 months. If a renewal is required, it must be applied for prior to the three month deadline. Renewals must be authorised by the Council's Authorising Officer and the Magistrate.

16. Reporting Errors in RIPA Authorisations

16.1 All errors in RIPA authorisations must be reported immediately by the applying manager or Authorising Officer to the Information Governance Manager..

17. RIPA requests from Third Parties

17.1 Requests from third parties to use Council equipment, facilities or buildings quoting RIPA authorisations must be made in writing, including a copy of the RIPA authorisation (redacted if necessary) and referred to the Information Governance Manager, or in the case of CCTV, the CCTV Manager.

18. CCTV

18.1 The Council operates CCTV systems, the use of which is subject to the national CCTV code of practice, as adopted by the Council.

18.2 Where CCTV cameras are used covertly as part of an operation to observe a known individual or group, an appropriate authorisation must be applied for.

18.3 The Council will keep its CCTV protocol up to date.

18.4 The Information Governance Manager will comply with requests from the CCTV Commissioner in relation to the organisation of inspections of the Council.

18.5 Any statistical returns required by the CCTV Commissioner will be supplied to him by the Information Governance Manager upon request

19. Surveillance of Employees

19.1 The Council may use Surveillance and the acquisition of internal communications data where there are grounds to do so. Procedures must be followed in relation to its staff where it is appropriate and legal to do so to protect the Council against claims of a breach of Article 8. A RIPA authorisation is not available in these circumstances. It is good practice to apply the same process however to address Article 8 considerations.

19.2 All managers must consider the impact on the human rights of the staff member(s) under formal surveillance and complete one of the appropriate forms which can be found on the Council's intranet.

19.3 The Council will follow the ICO's 'Employment Practices Code' to ensure employees' personal information is respected and properly protected under the Data Protection Act 1998.

19.4 For the acquisition of communications data (including but not limited to cryptag logs, email accounts, computer access, internet use logs and telephone call logs) managers must complete the 'Interception of Communications Form' which can be found on the Council's intranet and submit it to the Corporate Counter Fraud Team.

19.5 For all other directed surveillance of staff, managers must complete the 'Non-RIPA Surveillance Form' which can be found on the Council's

intranet and submit it to the Information Governance Manager once it has been signed by the relevant Divisional Director.

20. Storage and Destruction of Surveillance Data

20.1 The Information Governance Manager will store all paper copies of the signed authorisations centrally in a fireproof and secure manner.

20.2 Signed authorisations will be scanned, and electronic copies will be held securely on the Council's shared drive as back-ups.

20.3 All paper copies of the signed authorisations, and electronic copies, will be retained for three years and then disposed of securely, unless it is believed that the records could be relevant to pending or future criminal proceedings, where they must be retained for a suitable further period, commensurate to any subsequent review.

21. Compliance with the Legislation

21.1 The Council recognises the need to make the contents of this Policy known and ensure compliance by every employee.

21.2 The Information Governance Manager will notify relevant staff of changes to RIPA and surveillance legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

21.3 Elected members will receive an annual RIPA report via the Audit and Risk Committee.

21.4 The Council also recognises the need to make their policies known and accessible to the public. This policy will be published on the Council's website.

21.5 RIPA statistics, suitably redacted as to not reveal specific operations, will be published on the Council's website annually.

21.6 Leicester City Council expects all employees to comply fully with this policy, other information legislation and the Council's Employee Handbook. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following from this policy.

22. Complaints

22.1 Complaints relating to any surveillance matters must be made in writing and addressed to:

Information Governance Manager
Information & Customer Access
Leicester City Council
New Walk Centre
Leicester
LE1 6ZG
info.requests@leicester.gov.uk

22.2 If the complainant is still unhappy following the Information Governance Manager's response they must be advised to write to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ.
Tel. 0207 035 3711

23 Internal Charging

23.1 Costs incurred by the Council as a result of cases which are progressed to the Investigatory Powers Tribunal or the courts, will be charged to the relevant service area.

24 Further Guidance

24.1 Further guidance entitled ‘How to Carry Out Surveillance’ can be found on the Council’s intranet site.