

UNCLASSIFIED

Covert Surveillance of Employees Policy and Procedure

Status/Version: 1.0 For Approval
Effective:

1. Introduction

- 1.1 This policy is based on the Information Commissioner's "Employment Practices Code". It sets out the procedure to be followed if Covert Surveillance of Employees is required. Adherence to the policy promotes good practice and ensures compliance with the Data Protection Act 1998 and Human Rights Act 1998.
- 1.2 Employees are made aware of the nature and extent of surveillance via the most appropriate means, e.g. employment contracts, code of conduct, relevant policies.

2. What is covert surveillance

- 2.1 Covert surveillance means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place.

3. When should it be used

- 3.1 Covert surveillance of employees should only be used in exceptional circumstances.
- 3.2 It must be necessary, proportionate and only used if there are grounds to suspect criminal activity or serious malpractice by an employee.
- 3.3 The Council's Monitoring Officer or their nominated representative must authorise all applications for the covert surveillance of employees before such surveillance is commenced.

4. Procedure

- 4.1 Managers should liaise with HR and Internal Audit if they have concerns around employee conduct. Internal Audit will consider whether the use of Covert Surveillance is appropriate.
- 4.2 If covert surveillance is deemed appropriate, Internal Audit will complete an application form (attached at Appendix 1) to be submitted to the Monitoring Officer for consideration. The application must clearly demonstrate:
 - Who will be undertaking the surveillance, the purpose and duration;
 - Details of any proposed surveillance equipment;
 - The reasons for covert surveillance
 - The likely benefits to be gained;
 - Evidence of necessity and proportionality
 - Any likely adverse impact(s) of the surveillance to both the employee concerned and others who might be affected by it, e.g. confidential intrusion;
 - Evidence that all reasonable alternative methods of surveillance (e.g. relevant HR policies have been followed, obtaining statements, interviews etc.) have been duly considered including speaking to the individual(s) concerned;
 - Evidence of appropriate consideration to risk assessment, insurance and health and safety issues, together with any required provisions being put in place prior to the surveillance taking place;

- If a private investigator is employed to carry out the covert surveillance, confirmation that there is a contract in place that requires the private investigator to only collect information in a way that satisfies the employer's obligations under the Act.

4.3 The application form must be marked private and confidential and/or password protected.

5. Authorisation

5.1 Covert Surveillance will only be authorised if the Monitoring Officer/nominated representative is satisfied that it is necessary, proportionate and that there are grounds to suspect criminal activity or serious malpractice. The Monitoring Officer may either sign the application form or use email to convey their decision.

5.2 In considering the application, the Monitoring Officer shall have regard to other relevant council policies procedures.

6. Outcome of the surveillance

6.1 If covert surveillance substantiates the alleged criminal activity/serious malpractice, all evidence obtained must be passed to HR to deal with in accordance with the Council's disciplinary policy and procedures.

6.2 Where allegations are substantiated, the employee must be informed as soon as is reasonably practicable.

6.3 All requests to extend or cancel covert surveillance must be made in writing to the Monitoring Officer.

7. Storage/Retention/Requests for information

7.1 If allegations of criminal activity/serious malpractice cannot be substantiated, all recorded information will be securely destroyed.

7.2 If allegations are substantiated, all recorded information will be stored securely in accordance with the Council's corporate retention and disposal policy.

7.3 Requests from the data subject, or their authorised representative, for details of a covert operation will be managed via the Council's Subject Access Request process.

8. Register

8.1 The Monitoring Officer will keep a register of all applications, authorisations and reasons for refusing any applications for covert surveillance on a rolling 3 year period.

8.2 The Monitoring Officer will review the applications, authorisations, refusals, extensions and cancellations in conjunction with Internal Audit (as appropriate) on an annual basis.

9. Training

9.1 All officers involved with covert surveillance will undertake appropriate training.

Document Control:

The documentation will be reviewed on a biannual basis.

Version History

Version	Status	Date	Author	Summary of Changes
1.0	For Review	September 2013	A Bajaj	Initial document

Reviewers

Name	Role	Business Area
Neelesh Sutaria	Senior HR Officer	Resources Directorate
G Carter	Senior Solicitor, Employment	Resources Directorate
S Mangan	Inter Audit & Risk Manager	Resources Directorate
J Hutchings	Information Governance Manager	Resources Directorate

Management Review

Name	Role	Business Area
C West	Executive Director	Resources Directorate
S Brake	Assistant Director, Policy & Performance/Caldicott Guardian (RIPA Monitoring Officer & Senior Responsible Officer)	People Directorate / Chair of JIST
C Forde	Assistant Director, Legal Services	Resources Directorate
S Roach	Deputy Director, Strategy & Communities	People Directorate
S Iannantuoni	Assistant Director, HR	Resources Directorate
TU Core Group	Trade Union	

Member Approval

Name	Date
Cllr Townshend Cabinet Meeting (Community Safety & Equalities)	
Audit & Procurement Committee	

Distribution

Name	Organisational Department	Format
All	Intranet	Word Document

Enquiries regarding this procedure should be directed to Legal Services.