Northumberland
County Council

Corporate Fraud Team

Covert Employee Surveillance Guidance

Author:
Amy Hodgson – Corporate Fraud Manager

April 2022

1. Introduction

1.1 Covert employee surveillance by the Corporate Fraud Team in the course of an investigation is not subject to the requirements of the Regulation of Investigatory Powers Act (RIPA) but instead is subject to the provisions of the Data Protection Act and the Employment Practice Code.

1.2 The Information Commissioner has given specific guidance on the monitoring of employees and links to the Employment Practice Code and the supplementary guidance, including case studies, can be found below.

Information Commissioner's Office

https://ico.org.uk/

Employment Practice Code

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Employment Practice Code - Supplementary Guidance

https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf

2 Guidance

2.1 Covert surveillance is the surveillance of employees carried out in such a manner that the subject will be unaware that the surveillance is taking place.

2.2 Covert surveillance can be undertaken inside or outside the workplace and whilst the surveillance itself is not subject to the Data Protection Act once a record is kept of that surveillance the Act will apply to those records.

2.3 Covert surveillance can only be justified in a particular case if there are grounds for suspecting criminal activity or equivalent gross misconduct which would lead to the employee being dismissed and where prior notification to the employee would prejudice prevention or detection.

2.4 A reliable test of whether covert surveillance is justified is to consider whether the activity being monitored is of sufficient seriousness that it would be reasonable for the Police to be involved. This does not mean, however, that in all cases a referral to the Police will be made.

2.5 It will be rare for the covert surveillance of employees to be justified. It should therefore only be used in exceptional circumstances.

2.6 Covert surveillance must only be deployed as part of a specific investigation and must be directed at a specific employee in circumstances where the conduct under investigation would lead to dismissal for gross misconduct or a referral to the Police would be appropriate.

2.7 Any covert monitoring must be strictly targeted at obtaining evidence within a set timeframe and it must be ensured that the covert monitoring does not continue after the investigation is complete.

2.8 The number of staff involved in the covert surveillance operation should be limited and each must be clearly identified on the authorisation.

2.9 Any information obtained through covert surveillance must only be used for the prevention or detection of criminal activity or equivalent gross misconduct. Any ancillary information obtained through surveillance should be disregarded and where feasible deleted unless it reveals other activities that no employer could reasonably be expected to ignore.

2.10 In all cases the disclosure of any information obtained during the course of the surveillance should only be made to those directly involved in the investigation. Under the Data Protection Act the employee also has a right to view any records in relation to the surveillance.

2.11 An Impact Assessment and Application form should be completed in all cases and the Chief Executive or the Corporate Fraud Manager should normally authorise any covert monitoring. In accordance with the guidelines they must satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection.

3 Impact Assessments

3.1 The Data Protection Act does not prevent monitoring. Indeed in some cases monitoring might be necessary to satisfy its requirements. However, any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others.

3.2 An impact assessment involves;

- Identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver
- Identifying any likely adverse impact of the monitoring arrangement
- Considering alternatives to monitoring or different ways in which it might be carried out
- Taking into account the obligations that arise from monitoring
- Judging whether monitoring is justified.

3.3 Adverse impact

3.4 Identifying any likely adverse impact means taking into account the consequences of monitoring, not only for employees, but also for others who might be affected by it, for example members of the public.

3.5 Consider:

- What intrusion or interference, if any, will there be into the private lives of employees and others? Bear in mind that the private lives of employees can, and usually will, extend into the workplace.
- To what extent will employees and others know when either they, or information about them, are being monitored and then be in a position to act to limit any intrusion or other adverse impact on themselves?
- Whether information that is confidential, private or otherwise sensitive will be seen by those who do not have a business need to know.
- What impact, if any, will there be on the relationship of mutual trust and confidence that should exist between employees and their employer?
- Whether the monitoring will be oppressive or demeaning.

3.6 Alternatives

3.7 Considering alternatives, or different methods of monitoring, means asking questions such as:

- Can the investigation of specific incidents or problems be relied on to follow up an allegation of malpractice, rather than undertaking covert surveillance?
- Can monitoring be limited to workers about whom complaints have been received, or about whom there are other grounds to suspect of wrong-doing?

- Can monitoring be automated? If so, will it be less intrusive, e.g. does it mean that private information will be 'seen' only by a machine rather than by other workers?
- Can spot-checks or audit be undertaken instead of using covert surveillance.

3.8 Obligations

3.9 Taking into account the obligations that arise from monitoring means considering such matters as:

- How information about employees collected through surveillance will be kept securely and handled in accordance with the Act.
- The implication of the rights that individuals have to obtain a copy of information about them that has been collected through monitoring.

3.10 Is monitoring justified?

3.11 Making a conscious decision as to whether the current or proposed method of monitoring is justified involves;

- Establishing the benefits of the method of monitoring
- Considering any alternative method of monitoring
- Weighing these benefits against any adverse impact
- Placing particular emphasis on the need to be fair to individual workers
- Ensuring that any intrusion is no more than absolutely necessary
- Bearing in mind that significant intrusion into the private lives of individuals will not normally be justified unless the employer's business is at real risk of serious damage and where gross misconduct sufficient to justify dismissal is suspected

3.12 **Impact Assessment and Application Form**

3.13 In all cases an Impact Assessment and Application Form must be completed by a Fraud Investigator or the Anti Fraud Consultant before the surveillance is undertaken.

3.14 The only exception is where immediate action is required as a result of information received and in these cases the application must be completed and authorised within two working days.

3.15 See below for an appropriate form.

Northumberland
County Council

Covert Employee Surveillance

Impact Assessment & Application

Name of Applicant	
Job Title	
Department	Corporate Fraud Team
Full Address	County Hall, Morpeth, Northumberland
Contact Details:	Direct Dial Telephone: Email address:
Investigation Reference and Title	

Note: Prior to completion of this form please ensure that you have read and understood the Provisions of the Data Protection Act – Employment Practice Code details of which can be found via the following links:

Employment Practice Code

https://ico.org.uk/

Employment Practice Code - Supplementary Guidance

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Reference should also be made to the Corporate Fraud Team – Covert Employee Surveillance Guidance.

Applications should normally be completed by a Fraud Investigator or the Anti Fraud Consultant.

Give full details of the employee who is to be the subject of the surveillance (Name and personnel number, address and other information as appropriate)
Give background details of the investigation and the conduct of the employee that is being investigated.
Describe in detail the purpose of the surveillance and the information that it is expected will be gained.

Describe in detail the surveillance operation to be undertaken and the expected times and overall duration. Provide full details of any equipment to be used, i.e. camera, binoculars or recorders etc. **(Where appropriate please attach a map showing the location.)**
Give justification for why this surveillance is necessary
Give details of any alternative methods of investigation that have been considered with reasons as to why they cannot be used as an alternative.

Explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or others? Why is this intrusion outweighed by the need for surveillance?
Indicate the likelihood that confidential information might be obtained
Supply details of any potential collateral intrusion and why that intrusion is unavoidable. Describe the precautions you will take to minimise collateral intrusion.
I certify that I have read the Covert Employee Surveillance Guidance and make application for authorisation to conduct surveillance as outlined above.

Signature (Fraud Investigator / Anti Fraud Consultant)	
Date	

Authorising Officer's Statement and Authorisation Details **(Give precise justification for the surveillance, i.e. details of why the authorisation is granted, exactly what surveillance is authorised, who is authorised and where it is to be undertaken and over what period.**	
Signature **(Corporate Fraud Manager /** **Chief Executive)**	
Name and Position	
Date & Time Granted	
Expiry Date & Time **(Maximum 3m)**	