Appendix A

Authorisation and Protocol Requirements for Review of Work Activities

Contents

Authorisation and Protocol Requirements for Review of Work Activities

Application

1. This procedure (authorisation and protocol requirements) applies to all Council officers, and is commended to all Schools for consideration and adoption by their respective Governing Bodies. In respect of Schools, the authorising officer for monitoring activities should be the relevant Chair of Governors, in consultation with the Audit Manager, who will coordinate the associated professional considerations.

2. The procedure is aligned to upholding the principles of Council Codes of Conduct, the Counter-Fraud and Corruption Strategy, and to the Council's Disciplinary Policy.

Scope

3. The Council is involved in everyday functions of law enforcement ('core functions'). The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for regulating the use of those investigatory powers ensuring that any covert surveillance activities are consistent with the duties imposed upon public authorities by the Human Rights Act.

4. The regulation of employees (e.g. employment issues, contractual arrangements etc.) is a factor common to all public authorities and may be considered to be an 'ordinary function.' These 'ordinary functions' are covered by the Data Protection Act 2018 and the Information Commissioner's Employment Practices Code. A public authority may only seek authorisations under RIPA when in performance of its 'core functions'.

5. This procedure does not apply to cases which relate to the Regulation of Investigatory Powers Act 2000. Any such cases should be progressed in accordance with the Council's RIPA Operational Policy and Guidance. In each case advice should be obtained as appropriate, from the OM Principal Solicitor (Litigation), or other representative as directed by the Monitoring Officer.

Introduction

6. The Council has adopted an Employees' Code of Conduct, embedded in the Constitution and incorporated into the contract of employment of all Council employees.

7. The public are entitled to expect the highest standards of conduct from all Council employees. The role of employees is to serve the Council by providing advice, implementing its policies, and delivering services to the local community.

8. Where the employer is a public authority, that authority has a duty to the tax payer to ensure that employees are doing what they are paid to do. The Council demands a very high standard of conduct from employees whilst they conduct their duties, and official positions must not be used to further private interests, or the interest of others.

9. Officers in a supervisory role are responsible for ensuring that employees under their control adopt high standards of conduct whilst undertaking their duties. All employees have a duty; to be honest; to act with propriety and integrity at all times; and to adhere to legal requirements, rules, policies, procedures and practices.

10. Many employees spend time working in the community, reporting direct to site or job. Occasionally the Council will want to undertake management checks to ensure that employees comply with appropriate rules and working practices. This supervisory action is to ensure compliance with the contractual arrangements between employer and employee. Such checks can be conducted as to the whereabouts and actions of employees during hours of paid employment, and as such are outside the scope of this procedure.

11. From time to time managers may receive an allegation or suspicion that the conduct of an employee they manage has fallen short of the expected standards, and would require investigation, for example; falsification of time sheets. It is important that before monitoring is undertaken, a preliminary investigation is undertaken and if monitoring is considered appropriate, an impact assessment will need to be completed.

12. It will be rare for covert monitoring (surveillance) of employees to be justified; it should therefore be used in exceptional circumstances.

> - *"The covert monitoring of workers can rarely be justified. Do not carry it out unless it has been authorised at the highest level in your business. You should be satisfied that there are grounds for suspecting criminal activity or equivalent malpractice, and that telling people about the monitoring would make it difficult to prevent or detect such wrongdoing.*
>
> - *Use covert monitoring only as part of a specific investigation, and stop when the investigation has been completed. Do not use covert monitoring in places such as toilets or private offices unless you suspect serious crime and intend to involve the police."*
>
> *Information Commissioners Office*

13. The authorising officer, graded Assistant Director / Chief Officer or above, should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice and notifying individuals about the monitoring would prejudice its prevention or detection.

14. The Council's Disciplinary Policy and Fraud, Bribery & Corruption Policy help to ensure that when a suspicion or allegation of misconduct by an employee comes to the attention of the Council, an adequate investigation, conforming to the rules of natural justice, is carried out as quickly as possible. The Council must also ensure that it meets its counter-fraud obligations in accordance with a range of legislative requirements, including corporate criminal offence legislation (Criminal Finances Act). Support and guidance is available from Internal Audit (fraud@cardiff.gov.uk).

Data protection and monitoring at work

15. A number of the requirements of the Data Protection Act will come into play whenever an employer wishes to monitor its employees. It is important to note that the Act does not prevent an employer from monitoring employees, but such monitoring must be done in a way which is consistent with the Act.

16. The Employment Practices Code under the Data Protection Act deals with the impact of data protection laws on the employment relationship. The Code has been issued by the Information Commissioner and aims to give guidance and promote good practice.

17. Employers especially in the public sector must also bear in mind Article 8 of the European Convention on Human Rights, which creates a right to respect for private and family life, home and correspondence. In broad terms, what this Act requires is that any adverse impact on employees is justified by the benefits to the employer and others.

18. The procedure has been subject to an Equality Impact Assessment, to meet the responsibilities of Section 149 of the Equality Act 2010. Those tasked with administering the procedure require adequate equality / unconscious bias training to ensure fairness throughout the process.

The Council's monitoring arrangements

ICT Services

19. Access to, and use of ICT services, such as internet, email, mobile devices, electronic file store (networks and storage devices) and printing is subject to the scrutiny of the employer.

Tracking systems

20. The Council uses vehicle tracking systems to manage its vehicle fleet using real time information to improve operational practice and service delivery. It also enables the Council to comply with legal duties in relation to Health & Safety. The system gathers GPS (geographical / speed) data and time information in respect of each vehicle.

CCTV

21. The Council reserves the right to view CCTV images where it is considered necessary and proportionate to do so, following suspicion or receipt of an allegation of misconduct.

Impact assessments & process

22. The Data Protection Act does not prevent monitoring, and in some cases monitoring might be necessary to satisfy its requirements. However, any adverse impact of monitoring individuals must be justified by the benefits to the employer and others. The term "impact assessment" describes the process of deciding whether this is the case.

23. An Impact Assessment form has been designed to ensure that the relevant factors are taken into account when deciding if monitoring is justified and to ensure that the exercise is properly authorised.

24. As an employer, managers are likely to find it helpful to carry out an 'impact assessment' to decide if and how to carry out monitoring. This is the means by which it is established whether a monitoring arrangement is a proportionate response to the problem it seeks to address. It should assist employers in identifying and giving

appropriate weight to the other factors they should take into account as outlined in the Impact Assessment Form.

25. The Impact Assessment Form (Appendix A) should be completed by the relevant officer in respect of each monitoring exercise and emailed via a Cardiff Council email account for professional advice from the Audit Manager and the Information Governance OM. The advice / comments received will be included on the Impact Assessment Form, for consideration by the Authorising Officer.

26. Where the monitoring relates to ICT systems, if the form appears to identify an appropriate request, contact will be made with the ICT Security and Compliance Manager, to ascertain if proposed monitoring is achievable before forwarding to the Authorising Officer.

27. The Authorising Officer will discuss the Impact Assessment Form with the OM Principal Solicitor (Litigation) or an equivalent representative, as assigned by the Monitoring Officer. The Authorising Officer will require the agreement of the representative in Legal services to counter-sign the Impact Assessment Form in order to proceed with the monitoring exercise.

28. The Authorising Officer, will make the final decision to authorise / not authorise the monitoring exercise, and will sign the Impact Assessment Form, which will be counter-signed by the representative in Legal Services. The decision will be communicated within 5 working days of their receipt of the form. The Authorising Officer will keep authorised requests under regular review.

29. Each request will be dealt with on a case by case basis taking into account the requirements of the Data Protection Act, and the Employment Practices Code. Officers will be asked, as part of the request, what considerations have been taken into account in respect of an adverse effect on others and what other action has been considered prior to requesting the monitoring of an employee.

30. This information will be held securely by the Authorising Officer for a period of time as specified within the Council's Retention Schedule and securely destroyed when no longer required. Information will be kept confidential at all times as set out in employee's contract of employment and the Council's data protection policies and procedures.

31. The Monitoring Officer will retain a copy of each Impact Assessment for a period of time as specified within the Council's Retention Schedule.

32. Questions in relation to this process should be directed to the Audit Manager (fraud@cardiff.gov.uk).

33. It is intended to review this process every two years.

Appendix A

Cardiff Council
Review of Work Activities – Impact Assessment

Applicant		**Section**	
Place of work			
Contact number			

PURPOSE OF MONITORING

1. Describe the conduct to be authorised
Explain what is being investigated, for example: • Investigate allegation of misuse of email/internet • Investigate allegation of employee falsifying timesheets • Investigate allegation of theft of fuel

2. Describe in detail the operation (include duration, vehicles, equipment, subject(s), resources etc)
The key phrase is "in detail." Therefore a response which merely states **"**Video camera and recording equipment will be installed at a fixed point" will not be adequate. Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it, how they are going to do it and also: • How long will the monitoring last? • Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times? • Which premises are to be used and/or targeted? • Which vehicles are to be used? Are they public or private? • What type of equipment is to be used? e.g. covert cameras • What is the capability of the equipment to be used? e.g. zoom lens, remote controlled, audio etc. • Who else will be involved in the operation and what will be their role? e.g. Internal Audit, ICT, Police It may be appropriate to attach plans/maps showing where and how the surveillance will be conducted and indicating where any surveillance equipment will be installed.
3. What do you expect to obtain as a result of monitoring
• Internet usage logs to establish if the Council's system was used in order to undertake personal, business activities • Evidence to determine if the employees are leaving work at a time different to their time sheet entries • Evidence to determine if the employee is undertaking secondary employment which has not been declared and may be detrimental to their recovery.

INDIVIDUAL SUBJECT TO MONITORING

4. Employee details			
Name		**Address**	State N/A if not relevant
Job title		**Directorate**	
Place of work		**Address of monitoring**	State N/A if not relevant

ADVERSE IMPACT

5. Identify any likely adverse impact as a result of monitoring
Mutual trust and confidence should exist between an employee and their employer, what impact could this activity have? If you undertake monitoring you may also identify information relating to others, for example, members of the public or work colleagues. List here all potential collateral intrusion and negative impacts of this proposed activity. If the employee is already aware that their use of a system will be recorded, please state so here (e.g. attended tool box talk – aware that vehicle has a tracker).

ALTERNATIVES

6. What alternative actions have been considered
Whilst the only other alternative may appear to be speaking to the employee, you must still show that you have considered that and any other alternatives, setting out why you have chosen not to take that course of action. • Can you get information using less intrusive means/overt methods? • What other means have you tried to obtain the same information/evidence?

OBLIGATIONS

7. How will you ensure that you comply with the Data Protection Act
This involves balancing the seriousness of the intrusion into the employees privacy (or any other person who might be affected) against the need for the activity in investigative and operational terms. Ensure that officers who undertake the monitoring are clear on the subject of the exercise. Document how evidence will be gathered, retained, disclosed, stored, destroyed. Demonstrate how you have balanced the size and scope of the proposed activity against the gravity and extent of the perceived misconduct.

DECISION

8. Considering the impact assessment, is the proposed activity justified
The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

9. Professional Advice			
Name Job title	Audit Manager	Name Job title	Information Governance OM
Comments Received			
Date			

10. Authorising Officer			
Name		Job title	*(Assistant Director / Chief Officer or above)*
Comments			
Date		Time	
Signature		To be reviewed:	E.g. within 30 days

11. Counter-Signing Officer			
Name		Job title	*(OM Principal Solicitor (Litigation) / equivalent)*
Comments			
Date		Time	
Signature			

** This authorisation if approved will be effective on signing.

Review1	
Officer	
Date	
Comments	

Review2	
Officer	
Date	
Comments	