MONITORING AND SURVEILLANCE AT WORK

Introduction

Due to changes in workplace technologies, increased security threats and counter terrorist surveillance, workplace surveillance and monitoring has become a heightened concern for employees, as it raises questions around personal privacy in the workplace and the misuse of the information accumulated by employers.

UNISON branches are reporting an increase in the use of monitoring and surveillance techniques being used within the workplace, as well as monitoring evidence being used in disciplinary cases. Branches are also being asked to negotiate monitoring and surveillance workplace policies and electronic communication policies with employers. These policies should set out the workplace code of practise when monitoring staff and when and where it is appropriate.

This guide will set out what workplace monitoring is, worker’s rights when they are being monitored and set out the different types of surveillance now being used in the workplace. This guide will also explain the different types of legislation you are covered by when monitoring and surveillance in the workplace takes place.

What is workplace monitoring?

Surveillance and monitoring in the workplace is now commonplace due to the increase of surveillance technology (CCTV) being used for employee safeguarding, enhance security of a building and as a counter terrorism measure. UNISON branches are also reporting that employers are increasing their use of monitoring IT and phone usage. Employers are now using a range of sophisticated computer monitoring packages which are on the market, that monitor what different websites staff are visiting and for how long. Employers are also increasing the use of website blocking software, to prevent staff accessing certain websites and screen emails.

It is important to know your rights in the workplace as employers do have the right to monitor activities in the workplace, but they must tell employees about any monitoring arrangements and the reasons for the monitoring. The information gathered by monitoring must only be used for what it was collected for unless other issues arise from such monitoring, for example a breach in Health and Safety practises. Monitoring in the workplace by the
Data Protection Act 1998

The Data Protection Act (operates in England, Wales, Scotland and Northern Ireland) and legislates how our personal information is used by organisations, businesses and the government. There are very strict guidelines on the use of data including:

- That the information is used fairly and lawfully;
- That the information is used for limited and stated purposes;
- Used in a way that is adequate, relevant and not excessive;
- Kept for no longer than is absolutely necessary;
- Information is kept safely and securely;
- Handled according to data protection rights;
- Not transferred outside of the European Economic Area

There are stronger legal protections for more sensitive data for example health records or criminal records.

Employees also have the right to request what data an organisation might hold on them under section 7 of the Act, however some information can be withheld for example information about the collection of tax, national security or the armed forces.

New Data Protection Regulations Coming in 2018

The General Data Protection Regulation is the new governing legislation for collecting and processing personal data that will come into effect on 25th May 2018. The UK government has confirmed the Regulation will be implemented in the UK as the UK will still be part of the EU on this date.

This regulation will replace the existing data protection directive and carries heavier penalties for employers that breach the regs including a maximum fine of up to £20 million Euros.

Employer is covered by data protection laws but can include: recording on CCTV cameras, opening mail or e-mail, use of software to access email, checking phone logs and numbers and the recording of phone calls, checking logs of websites visited, gaining information from credit reference agencies, collecting information from ‘point of sale’ devices to check performance or money that has been deposited, drug testing, and bag searches.

Employers should have written policies in place to cover all areas of monitoring in the workplace, so that employees know they are being monitored, the reason for it and how the information is being used. It is important to remember that employees are entitled to some privacy at work. Data protections sets down the guidelines in the ways in which monitoring can take place, but if an employer is considering introducing monitoring, they should consider ACAS guidance.

ACAS advises that employers should make it clear why staff are being monitored and, if they are, the benefits it will bring - for example, any monitoring must comply with the ICO’s (Information Commissioner’s Office) Code of Practice (see below) and that the monitoring is being used to safeguard employees. UNISON’s position is that workers should not be subject to unnecessary and intrusive monitoring at work and that the increase in the “surveillance culture” in the workplace is bad for staff morale and productivity.

CCTV monitoring

If CCTV is being used by the employer, the employer must inform employees that it is in use by displaying signs of where the cameras are in the building and inform employees that they ‘may’ be filmed. The employer must also inform the ICO that they are using CCTV in their workplace. Employees do deserve the right to privacy at work and therefore cameras should not be placed in areas where
employees would normally expect privacy – for example private meeting rooms. The ICO has an employer code of practise which covers the use of CCTV and is based on data protection principles. The code of practise is not legally binding but ensures employers operate with the Act and highlights good practise. Images of people are covered by the Data Protection Act, so the information obtained by CCTV (and the use of the images) has to comply with the Act.

**Monitoring electronic communications in the workplace**

ACAS makes clear that there are some legitimate reasons why employers may wish to monitor their workforce, for example to prevent theft or to make sure there is compliance with health and safety regulations. Employers should consider the negative impact of monitoring staff, particularly monitoring electronic communications, as this type of monitoring can cause staff stress, loss of trust and can lower staff morale. It is important to note that your employer does have the right to access your email and voicemail while you are away from work to deal with matters of business, so long as you have been informed that this is going to happen. Workplace unions should always be consulted where monitoring is happening in the workplace and be consulted on any monitoring and surveillance policies.

An employee has no legal right to use their employer’s email, internet or make phone calls for personal use, however most employers allow for some personal correspondence during work time. The Human Rights Act 1998 does extend to the workplace and under this law employees are entitled to access some forms of private communication while at work. This does not mean that an employer doesn’t have the right to monitor electronic communications.

**What can I do about email and web usage monitoring in the workplace?**

If you have concerns about email and web usage monitoring in the workplace then speak with your UNISON rep or branch. It is important that everyone in the workplace knows that this type of monitoring is taking place, and that it is being done with full consultation with the staff unions. It is advantageous to have a written policy in place in the workplace (which has been agreed by the unions) as this sets out very clear guidance on what isn’t acceptable in the workplace. An employer has the legal right to specify which websites can or cannot be visited by staff and to introduce e-mail usage policies that preclude or limit personal use. Where the law becomes more complicated is where employers seek to monitor and intercept or even spy-on the electronic communications of their staff.

**How do I know if my emails are being monitored?**

Most medium sized employers will use software which searches for certain keywords and some offensive language, so that they can monitor usage linked to their business. UNISON reps have reported case work where staff have been disciplined for forwarding on offensive jokes / emails and copyright material (for example music). There have also been cases where employers’ IT firewalls and filters have very basic screening which blocks emails containing words like ‘lesbian’, ‘gay’, ‘bisexual’, automatically quarantining them as offensive, adult or unprofessional and UNISON activists have been investigated under their employers’ disciplinary procedure for receiving a UNISON newsletter about LGBT equality. It is important that UNISON reps raise these issues with the employer to make sure there is an agreement that these emails are not blocked and that staff are not investigated. Use of social media can also get workers into trouble, particularly accessing these sites during work time – It is important that branches argue and include into any Acceptable Use Policy that
social media is a legitimate form of communication which is used at work, and as long as it it’s not interfering with business it can be accessed.

As previously noted your employer has a duty to inform you if they are planning to monitor email in the workplace and the reason why it is being monitored. Employees need to be clear what information is likely to be obtained, why it is being obtained and how the employer wishes to use that information. If a branch is concerned that an employer is monitoring union reps and that their union business emails are being monitored they should speak to their regional officer and make sure this is raised at a staff-side meeting with management.

**Use of biometrics in the workplace**

Biometrics is the use of identifying an individual according to their physical or behavioural characteristics. Examples of commonly used biometrics include iris and retina scanning, fingerprint identification, and face and hand recognition geometry. Many of these forms of biometrics and technology were introduced for identity cards, passports and to enhance counter terrorism surveillance, however UNISON members have reported an increase of the use of some of these practises as a way of monitoring staff time-keeping and sickness absence. This also raises some serious concerns around personal privacy and possible misuse of the information. Biometrics should be focused on security rather than the monitoring of staff and should only be introduced after a full and comprehensive consultation with staff and their trade unions.

**Case Study: Biometrics**

A UNISON branch (City of Westminster) led a successful campaign against the introduction of biometric monitoring by sending out a model letter to their members and asking UNISON members to sign and email the letter back to their employer. As well as campaigning at a local level through their staff side, part of this campaign involved national and local media and drafting a press release. If branches want to involve the media as part of their campaign they should contact their region and seek the advice of their regional press officer contact, who will be able to help with this and set up interviews with their local media contacts.

**Use of monitoring and surveillance information / evidence used in a disciplinary case**

As discussed previously in this guide, employers have the right to access emails and voicemails as long as they have told you they are going to do it. In some workplace investigations and disciplinary cases, emails and CCTV surveillance have been used as part of the case. Employees should remember that even though they may have deleted emails months ago, most work places have the capacity to access emails for up to a year after they were sent. ACAS guidance on discipline and grievances at work makes reference to the use of monitoring and surveillance methods in cases, but does state that where they are used the employer must be sure to view the evidence objectively and in full (particularly evidence based on CCTV footage). UNISON representatives should make sure there is an overarching policy for staff that fully informs them of the location and purpose of these cameras and their use.

**Covert monitoring**

Covert monitoring is rarely used in the workplace as it is often hard for the employer to justify secretly recording their staff. The employer must have genuine suspicions of criminal
activity taking place and be able to justify the covert monitoring as a means of collecting evidence. Even if wrongdoing is recorded during covert monitoring, it would need to be an act of ‘gross misconduct’ rather than a minor offence in which the evidence collected during covert surveillance can be used. The use of covert monitoring is covered by the Data Protection Act. Following incidents of abusive or neglectful care in care homes and hospitals, the call to use covert surveillance cameras in care settings has become an issue faced by many health branches across the UK. UNISON has issued specific guidance for health branches on this issue which includes bargaining advice where cameras are under consideration or where they are already in operation, alongside advice on monitoring in the workplace. Links to this guidance are at the end of this guide.

**Monitoring a work vehicle**

UNISON branches have been reporting an increase in the use of vehicle monitoring especially in some home care and private sector employers. Workplace monitoring can be extended to vehicles especially in employers where their workforce is generally off-site working in different locations. Devices are put into vehicles so that employers can see the location of their vehicles, the distances the vehicle has travelled and any other information about the drivers ‘driving’ habits. Like covert monitoring this type of monitoring is regulated by the Data Protection Act but where a vehicle is being used for private use as well as business use it is hard to justify. Where vehicles are used for private and business use some organisations have had devices fitted that balance the need for privacy and when the vehicle is being used for private use, the employee can switch a button on the device to disable the monitoring. It is important to note that some employers have a legal obligation to track vehicles when tachographs are fitted – e.g. lorries and other vehicles over 5.5 tonnes.

**Case Study – DHL**

DHL has taken a decision to install forward facing cameras to all their insured fleet vehicles. The purpose and business case for the cameras was to:

- Make DHL a safer place to work for their drivers
- Learn more from incidents / near misses to reduce the risk in future
- Reduce cost of vehicle insurance
- Reduce the cost of third party claims by defending vexatious claims against DHL drivers

The cameras also have the ability to be triggered by the drivers to record particular incidents that drivers may find themselves in – to assist with training or insurance claims.

The agreement was jointly agreed with the staff side trade unions and states that the forward facing cameras are not to be used for routine monitoring and as a tool to discipline drivers.

**Organising and Campaigning around monitoring and surveillance issues**

If your employer proposes introducing surveillance, biometrics or monitoring in your workplace your branch should be consulted. Here are some tips on how to organise around this issue:
Find out what is going on
Before you campaign and organise around this issue you need to get the facts. Issues should be raised at local level and reps should try and find out the reasons for why management are seeking to introduce surveillance and monitoring techniques (especially biometric monitoring). Is it for a particular security reason? Is it on advice from counter terrorism police? Or is it just to monitor staff?

Consultation
The branch needs to consider who is going to be covered by the monitoring, is it all staff or just certain departments? Are the CCTV cameras going to be public areas? Who is responsible for monitoring the cameras and storing the information? During the consultation the branch should ask for full costings of how much the monitoring and surveillance systems are, to see if they represent good value for money or if they are unnecessary and expensive.

Risk Assessment / Privacy Impact Assessment
The branch should insist that the employer conducts a full risk assessment and privacy impact assessment of any surveillance and monitoring systems – particularly the use of biometrics, because of the sensitivity of the data which is being kept.

Storage of Information
The branch should ensure that the employer intends to comply with the Data Protection Act and store any information that is collected for monitoring and surveillance purposes securely. If an employer is looking at adopting the use of biometrics, information held on file about employees should be destroyed once they leave the organisation.

Consult members
The branch should organise meetings, send around a member survey on the issue, and report finding back to their members. Employers may not understand what the strength of feeling is on this issue, particularly the storage of personal data involved with biometric monitoring.

Campaigning
If after the members have been consulted, and the branch has ascertained that there is sufficient concern about the introduction of monitoring in the workplace; the branch could campaign around this issue and build up the profile of the union. UNISON branches that have campaigned around monitoring and surveillance in the workplace have used the local JNCC meetings to raise concerns and share the survey results with their employer.

Organising Members
As a branch you will need to take stock of the membership and their views on the introduction of monitoring in the workplace. For most standard monitoring (CCTV) in the workplace, it may be that members are happy if the areas are signposted and the reasons for any monitoring and surveillance are transparent and set out to staff. In terms of biometric surveillance, depending on the circumstances, the branch may take the decision to tell managers that UNISON members will refuse to give biometric data - This should only happen if the branch is clear that this type of surveillance is unwarranted, and only to be
done with full consultation with their members, regional officer and advice from UNISON’s legal sources.

What should an electronics communications policy or a monitoring and surveillance policy look like?

There are many policies that can fall under the umbrella of monitoring and surveillance in the workplace including:

- Information and Communication Technology: Monitoring Policies
- CCTV and Video Surveillance policies
- IT and Email policies
- Acceptable use policy for telephone, email and internet use policies
- Social media policies
- Vehicle monitoring policies

It is important that staff side trade unions are fully involved in the consultation and implementation of any of these policies and that once a policy has been agreed the policy is communicated widely by management so that staff know the types of monitoring and surveillance taking place in their workplace and the reasons for them.

A good ICT monitoring policy should always make reference to the Data Protection Act and compliance of the Act by the employer. It should make clear what the purpose and scope of the policy is, along with a section on employee privacy. There is a draft policy in appendix 1 of this factsheet.

Additional Information on monitoring, surveillance and regulation in the workplace

For more information on monitoring and surveillance in the workplace please see:

- Citizens Advice Factsheet – Monitoring at work
- TUC Worksmart Guidance – Monitoring at work
- ACAS Guidance – Being monitored at work
- Gov.UK Guidance – Data Protection Act
- Personnel Today (Sept 2012) – The implications of placing staff under surveillance
- ICO - In the picture: A data protection code of practise for surveillance cameras and personal information
- Worksmart – Your right to privacy at work
- UNISON – Use of surveillance in health and care settings: Guidance for UNISON representatives
- ACAS Guidance – Internet and E-mail Policies
Appendix 1

Model Monitoring and Surveillance Policy and Procedure

Policy Statement

Both [name of employer] and [UNISON branch] recognise that employees should be treated fairly and this policy aims to provide consistency in the treatment of all staff. This policy sets out the need to balance staff privacy in the workplace along with ensuring the health and safety of employees and that [the employer] is complying with regulatory and statutory obligations.

Purpose

This policy will set out how we will monitor the use of our information and communication technology systems, along with the use of surveillance cameras (CCTV).

Compliance with the Data Protection Act 1998 and the ICO code of conduct on the use of surveillance and monitoring equipment. This monitoring and surveillance procedure complies with regulatory and statutory obligations.

Introduction

1. Our ICT systems support the work of [name of employer] are intended for ‘business’ use. However, we also recognise that there are benefits to be gained by allowing staff to make limited use of our ICT services – including recruitment and retention rates, supports our employees in sustaining a healthy work/life balance, and improve work networking particularly through social media. All usage of our ICT systems (business and personal) must comply and be consistent with our [Acceptable Use Policy].

2. [Name of employer] reserves the right to monitor the use of our ICT services, and access any information stored on our ICT infrastructure, but we will access any information in line with relevant legislation and guidance provided by the Office of the UK Information Commissioner. Impact assessments for all forms of workplace monitoring will be conducted and shared with staff side unions. The monitoring will be undertaken to:

- Comply with our regulatory and statutory obligations
- Workers will be told where monitoring is carried out.
- Assess compliance with our health and safety, security and acceptable use policies
- Prevent and detect unauthorised use or other threats to our ICT systems
- Evaluate staff training - and to ensure standards are maintained
- To prevent and detect crime
- All information will be kept securely
- Monitor system performance
3. Such monitoring will include [delete as applicable] email, internet, telephone, mobile
   telephone, and SharePoint. Such monitoring isn't person specific unless the member
   of staff has been told that such monitoring will take place and reasons for the
   monitoring. As part of this policy personal data may be accessed but only in line with
   legislation. This type of monitoring is defined as ‘systematic monitoring’ in terms of
   the UK Information Commissioner’s Office (ICO) Employment Practices Code.

4. All staff will be trained in this policy and the organisation's [Acceptable Use Policy].

Scope

5. This policy covers all members of staff at [name of employer] and this policy specifies
   our approach to monitoring the usage of ICT devices, services and software including
   printer usage. This policy also includes intercepting communications on our ICT
   systems and how staff and other users of our ICT systems are made aware of this
   policy.

6. This policy has been agreed with staff side trade unions and any updates to this
   policy will be made in agreement with the staff side trade unions.

Communication of this policy

7. It is management’s responsibility to make users aware of this policy by:
   
   - Ensuring all new members of staff are informed of this policy on their induction
   - Informing staff that they are accepting the terms of this policy by logging onto the
     ICT infrastructure
   - Reminding users at regular intervals of this policy, at point of log on, of the
     existence of the policy and where to find it.
   - Staff training once a year on the policy and compliance with the Data Protection
     Act

Privacy

8. This policy has been agreed with the staff side trade unions - We believe it strikes the
   balance between respecting staff privacy, whilst allowing the necessary monitoring
   required to meet our business and legal obligations. No member of staff will be
   individually monitored without informing that member of staff. If a member of staff is
   being monitored, they will be informed as to what type of monitoring will be taking
   place and the reasons for the monitoring. The monitoring will have a start and end
   date communicated to the member of staff.

9. We recognise that staff have a legitimate expectation that they should be able to
   keep their private lives private and that they are entitled to a degree of privacy in the
   work place. Therefore our monitoring policy will always be used in a way in which is
   consistent and with compliance to the Data Protection Act 1998, the UK Information
   Commissioner’s Office (ICO) Employment Practices Code and the Human Rights Act
   1998.

10. [Name of employer] guarantees the privacy of emails sent to and from designated
    trade union e-mail addresses. [Branch Sec to Regional Organiser]

Content Inspections and Authorised Access

12. [Name of employer] has the right to inspect the content on our ICT systems to fulfil business needs, this includes access when a user is unexpectedly absent or is on annual leave. The staff member will be notified before any access is made. In these instances, [name of employer] will inform the member of staff in writing when this access is taking place, what information was viewed and the reason for the access.

13. Access to the ICT system may have to take place to satisfy Compliance of Data Protection and Freedom of Information Requests.

14. Where we have reason to believe that a breach of our information security and information policies is occurring (i.e. where a complaint or concerns have been raised).

15. At the request of law enforcement officers.

16. Content inspection involves viewing information within business files and documents, printer usage, business related email messages, telephone calls, video conference sessions, chat sessions or any other ICT based communications.

17. Business information displayed on VDU screens

18. Content inspections can only happen after permission has been granted by the Head of Human Resources or higher.

19. Requests for access to the email account or restricted folder of a member of staff must be made in writing to the Head of Human Resources. The request must detail the reason for access and the information to be viewed.

20. Upon receipt of an approved request from the Head of Human Resources, a member of ICT will undertake a content inspection and will record:
   - What information was inspected
   - The computer on which the monitoring took place
   - The start and the end time of the monitoring
   - The identity of the person performing the inspection

21. The record may only be shared with the line manager, the individual being monitored, and the Head of Human Resources.

22. [Name of employer] will regard any attempt to conduct a content inspection that is not in accordance with this policy as gross misconduct.
23. If the terms of this monitoring policy or Acceptable Use Policy are seen to have been broken by a member of staff, following a content inspection, the Head of Human Resources can refer the case to the organisation’s disciplinary procedure to be investigated fully.

**Covert Monitoring**

24. Where [name of employer] have good reason to suspect that a member of staff is engaging in prohibited use of our ICT systems – as set out in [the Acceptable Use Policy] – we may in very exceptional circumstances introduce covert monitoring of the individual and only where criminal activity is suspected.

25. We will only undertake such covert monitoring where there are strong grounds for suspecting criminal activity or equivalent malpractice. Covert monitoring will take place within a very strict timeframe and will only be targeted at gaining evidence.

26. This type of monitoring can only be authorised by the Chief Executive. The record of monitoring can only be viewed by the individual’s line manager and the Head of Human Resources.

27. If, following covert monitoring, an individual is cleared of wrong doing; all evidence obtained during the surveillance must be destroyed.

28. If, following covert monitoring, evidence of criminal activity is recorded; this must be referred to the appropriate body to press charges (police).

29. If covert recording is used as evidence in a disciplinary case against a member of staff, the staff side trade unions must have full access to all the covert monitoring information in order to support their member through the disciplinary process.