BARGAINING ON MONITORING AND SURVEILLANCE WORKPLACE POLICIES

Why branches need to negotiate on monitoring and surveillance workplace policies

The increasing number of checks on workers by their employer such as the monitoring of emails, phone calls and computer use, or using cameras and other technology to keep an eye on their activities, is becoming a worrying issue for many.

The TUC’s report on workplace monitoring ‘I’ll be watching you’ (https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you) found that over half of workers think it is likely that they are being monitored at work.
and two-thirds of workers are concerned that workplace surveillance could be used in a discriminatory way if left unregulated.

Of course there may well be valid reasons for workplace surveillance and monitoring, not least for the protection of staff members. Under their duty to protect the health and safety of their staff, UNISON would expect employers to put in place systems for ensuring they know where their staff are, particularly those working in the community and alone. But as the UNISON health and safety leaflet on Lone Working (https://www.unison.org.uk/content/uploads/2018/02/24845-1.pdf stock number 3878) states: “any device is only as good as the systems that support it. New technology should work in conjunction with robust procedures so that lone workers can easily keep in touch and get help should they need it.”

Therefore the best way of preventing risks or concerns is through robust risk assessment and by employers working in partnership and consultation with staff and their trade unions, rather than relying on technology alone, particularly if it could be abused by some employers or could give a false sense of security to employees.

Other examples that employers may have to justify the use of monitoring may be their concern over excessive use of work telephones for personal calls or the accessing of pornographic websites at work, or because of the theft of the organisation’s equipment.

Additionally, employers may introduce automation within the workplace in order to reduce the strain of repetitive work. However, as highlighted in the UNISON guide, ‘Bargaining over Automation’ (www.unison.org.uk/content/uploads/2018/04/Bargaining-over-Automation.pdf) "numerous examples attest to the way employers can utilise the possibilities opened up by the technology to intensify pressures.

Data generated by automation can lead to much more detailed tracking of workers’ performance and complex algorithms can be utilised by computer technology to increasingly dictate the intensity of work schedules. The tracking of time a call centre operator spends in responding to calls and on that basis setting minimum number of call responses per hour is just such a system.

Such tracking of performance can then feed into performance related pay systems.”

Without a doubt, there is increased surveillance, tracking of activity and automation at work, often without a clear and reasoned justification given by the employer. Of particular concern to UNISON members is how it impacts on their privacy and, as suggested in the automation guide, sometimes unfairly used for performance related purposes.

Sometimes the justification given by employers is disproportionate to any need and too often new monitoring and surveillance is introduced in the workplace by employers outside of any collective bargaining process.
It is important to negotiate on this issue of monitoring and surveillance in the workplace because:

i. Use of monitoring and surveillance in the workplace can raise serious concerns around personal privacy.

ii. There may be fears that the information accumulated by employers can be misused.

iii. Branches are reporting that more monitoring evidence is being used in disciplinary cases.

iv. The number of cases requiring steward representation may be reduced, freeing up steward time, particularly if good monitoring and surveillance policies and procedures are agreed.

v. It highlights how UNISON values its members and recognises the need for personal privacy, which could result in an increase of your branch’s activist base.

vi. Agreeing successful policies for workers can be a useful recruitment tool, advertising the benefits of joining UNISON for all, as well as how UNISON reps have expert negotiation skills when dealing with employers.
How to use this guide

The guide has the following sections that you can dip into as relevant in your workplace.

1. The law affecting monitoring and surveillance.................................page 5
   This section outlines the legal issues that an employer must consider in relation to any monitoring and surveillance at work – this would be the starting point for branches or reps in their preparations for any negotiations.
   Do current policies and procedures take full account of the law, in particular the General Data Protection Regulation (GDPR)?

2. What sort of workplace monitoring takes place and what are some of the issues to look out for?.........................................................page 11
   This section sets out the different types of monitoring and surveillance commonly being used in the workplace. It highlights some of the issues that branches and workplace reps should consider and provides quick checklists as a focus for negotiations.

3. Putting the case to employers for negotiations..............................page 33
   To assist the branch or reps in their negotiations, this section provides the argument to put to the employer alongside the legal requirements in section 1, to improve or introduce policies and procedures relating to monitoring and surveillance.

4. Model policy ..................................................................................page 39
   An example policy covering monitoring and surveillance in the workplace is included for branches and reps to use for negotiations with employers.
1. The law affecting monitoring and surveillance at work

Human Rights Act

The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (www.echr.coe.int/Documents/Convention_ENG.pdf) into domestic British law.

More information:

Equality and Human Rights Commission (ECHR)

Article 8 provides individuals with the right to respect for private and family life, home and correspondence, subject to being “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country… or for the protection of the rights and freedoms of others.” This right includes an individual’s personal privacy within the workplace balanced against the legitimate business interests, although the Act is mostly used to legally challenge the intrusive behaviour of public bodies or governments.

As well as the human right to privacy under Article 8 of the European Convention of Human Rights, in the UK the use and processing of personal data is regulated by the General Data Protection Regulation (GDPR) and enforced by the Information Commissioner’s Office (ICO).

The basics of the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) came into effect from 25 May 2018, replacing the 1998 Data Protection Act (DPA). The principles of the GDPR are very similar to the principles of DPA – the laws aim to do the same thing. However the GDPR places a greater emphasis on transparency and the rights of the individuals in relation to personal data held on them.

More information:

ico. (Information Commissioners Office)
https://ico.org.uk/

Personal data is any information about a living individual which enables them to be identified. If data is ‘obviously about’ a person, then it is personal data. Examples of personal data include (but is not limited to):

- Pay roll number
- Date of birth
- National insurance number
• Bank details
• Email address
• Telephone number
• Home address
• Photographs
• Telephone recordings
• CCTV recordings

Records of opinions about an individual, or intentions towards them, are also classed as personal data.

Some personal data is classed as ‘special category’. This data includes information relating to an individual’s:

• race
• ethnic origin
• politics
• religion
• trade union membership
• biometrics i.e. the measurement and analysis of unique physical or behavioural traits such as fingerprint or voice patterns (where used for ID purposes)
• health.
Personal data can be held in any form. This could be on electronic media (such as USB sticks, CDs, computer drives, mobile phone apps and cloud computing) or hard copy files.

Under GDPR there are six lawful bases for processing personal data. Everything an employer does with personal data must fall under one of those lawful bases otherwise it is unlawful and must cease – these are:

(a) **Consent**: the individual has given clear consent for the employer to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract they have with the individual, or because they have asked the individual to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for the employer to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone’s life, or in some cases someone’s property.

(e) **Public task**: the processing is necessary for the employer to perform a task in the public interest or for their official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for the employer’s legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks – the public task basis applies in this circumstance.)

To be able to use special category personal data there are further conditions (additional to those highlighted above) which an employer must meet. The most common are:

- The person involved has given explicit consent for the data to be used in this specific way
- The data is needed to fulfil the employer’s obligations under employment law
- The data is needed in relation to legal claims.

Under the GDPR employers have to be more transparent about what they are collecting data for and how they use it. The GDPR also includes a new obligation to conduct a Data Protection Impact Assessment for types of processing likely to result in a high risk to individuals’ interests.

Employers should now report data protection breaches to the ICO within 72 hours of becoming aware of them. Fines for getting it wrong have increased to 20 million Euros or 4% of the total annual worldwide turnover (whichever is greater).
Anyone is entitled to see the data that an organisation holds on them under the right to subject access. That means that workers can request the data held on them by their employer and they will have a legal duty to provide it. This includes for example the evidence used in a grievance or disciplinary hearing such as the witness statements, photographs or emails, if reasonable in the circumstances. The organisation cannot charge a fee and it only has a month to respond to the individual’s request.

Additionally, individuals will have the right to have their data deleted by an organisation if it is no longer needed, under the right to erasure.

The ICO has an employment practices code on data protection that aims to help employers comply with the Data Protection Act (DPA) and to encourage them to adopt good practice. Although it does relate to the DPA rather than the requirements of the GDPR, the key principles are the same. It is hoped that updated guidance will be produced by ICO in due course. Whilst the existing code is not legally binding, it sets out the Information Commissioner’s recommendations as to how the legal requirements of the DPA can be met.

More information:

Information Commission’s Office ‘Employment Practices Code’
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

The Privacy and Electronic Communications (EC Directive) Regulations 2003

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications. The EU is in the process of replacing the
e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR. However, at the time of writing, the new Regulation is not yet agreed.

Although most particularly aimed at organisations that provide a public electronic communications network or service and those that undertake marketing by electronic means, it does have a wider application.

The rules in the Regulations in relation to the use of ‘cookies’ can also cover other types of technology, including apps on smartphones, tablets, smart TVs or other devices. They will be relevant to any app if it is designed to:

- send email, SMS text messages, or voicemail messages
- make phone calls
- set cookies or other tracking elements
- or engage in ‘viral’ marketing campaigns.

These rules also outlaw spyware or any similar covert surveillance software that downloads to a user’s device and tracks their activities without their knowledge.

Subscribers and users must be provided with “clear and comprehensive” information about the purpose. With apps, this is likely to be within the sign-up stage. Consent must be freely given, specific and informed.

More information:

Information Commission’s Office What are PECR? (Privacy and Electronic Communications Regulations) [https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/](https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/)

Protection of Freedoms Act 2012

This legislation aims to help safeguard civil liberties and reduce the burden of government intrusion into the lives of individuals. Although it applies to public authorities it is also recommended for other types of organisations.

The Act includes a statutory code of practice on the use of surveillance cameras and a surveillance camera commissioner was appointed with responsibility for reviewing and reporting on the operation of the code. Therefore it is of relevance in relation to CCTV surveillance in workplaces.

The code sets out guiding principles that should apply to all surveillance camera systems in public places.


1. always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. take into account its effect on individuals and their privacy
3. have as much transparency as possible, including a published contact point for access to information and complaints
4. have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
5. have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
6. have no more images and information stored than that which is strictly required
7. restrict access to retained images and information with clear rules on who can gain access
8. consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. be subject to appropriate security measures to safeguard against unauthorised access and use
10. have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
11. be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim
12. be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.
2. **What sort of workplace monitoring takes place and what are some of the issues to look out for?**

Employers may have many legitimate reasons for their monitoring and surveillance of staff, for example to prevent theft, enhance the security of a building or to make sure there is compliance with health and safety regulations.

However for any monitoring arrangements to be successful, employers should first consult with workers giving clear reasons for the monitoring. And these reasons should be legitimate and in proportion with the need.

**Quick checklist**

- Is the data to be collected really needed by the employer?
- What data is to be collected – could the process mean that additional personal data that is not required by the employer is also collected?
- Is the reason for monitoring given valid and reasonable in the circumstances?
- How much will the monitoring and surveillance systems cost? Do they represent good value for money?
- Do the benefits of collecting the data really outweigh the potential costs or consequences if the data security and confidentiality is breached?
- Do our members know how and why the data is being collected?
- How secure is the data held?
- How can the employer be certain that the data held is accurate and up-to-date?
- How long is it held for? Just as needed and relevant?
- Is it shared unnecessarily?

Over the next pages are listed some of the more common forms of monitoring and surveillance currently found in workplaces.

The TUC’s report on workplace monitoring ‘I’ll be watching you’ ([https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you](https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you)) found that the most common types of surveillance include:

- “Monitoring work emails, files and work computer browsing history (49 per cent of people think it’s fairly likely or very likely to be happening in their workplace)
- CCTV (45 per cent)
- Phone log and calls, including the recording of calls (42 per cent)

... 23% of workers think that handheld or wearable location-tracking devices are very or fairly likely to be being used in their workplace, while 15% find it fairly likely or very likely that their employers are using facial recognition software.”
Pre-employment information gathering

Before workers start a job, they may be asked for personal details and for references. The employer may also check their criminal background in certain circumstances, for example if the job involves working with children or vulnerable adults. This is known as pre-employment vetting and is different from standard data collection because employers may be asking third parties for 'special category personal data' and 'criminal offence data' about individuals. The GDPR recognises this type of data is more sensitive, and so needs more protection.

Job applicants and new employees may also be asked other sensitive information about themselves such as racial or ethnic origin, or sexual orientation. This may be part of equality and diversity monitoring to help identify possible patterns of inequality amongst job applicants and to help measure the effectiveness of equality and diversity policies.

These details should be kept separately and anonymous from any applications so that it cannot influence the selection process. Applicants should be free to decide whether they want to provide this information or not without being adversely affected. Certain sensitive personal data such as racial or ethnic origin data is ‘special category’ under the GDPR so requires a specific lawful basis for processing. The full list of ‘special category’ data is on page 6 of this guide.

Employers may also want to collect some health information from workers. For example an employer may keep information provided about a disabled candidate’s impairment in order to make appropriate reasonable adjustments. Some job roles
may require certain levels of fitness but an employer has no right to ask a job applicant about their physical health before offering them a position. Even when they do ask for health information or medical checks from new employees, reps should be wary of employers in case they discriminate against disabled workers rather than make reasonable adjustments.

Under the GDPR, “personal data related to the physical or mental health of a natural person… which reveal information about his or her health status” is ‘special category personal data’ whatever the reason for collecting it.

Increasingly employers are also reviewing job applicants’ digital ‘footprints’ such as checking on social media sites for public postings and images, and using this information to screen possible candidates.

Although websites like Facebook and Instagram are in the public domain, basing employment decisions on material uncovered on such sites may be not only unfair but potentially discriminatory. In some circumstances it could also lead to victimisation, for example if it influenced the employer’s decision in relation to what it revealed about a candidate’s ethnicity, sexual orientation or trade union membership.

Whenever ‘special category personal data’ is collected, applicants and employees should be informed of what that information is to be used for, and employers should destroy the documents when they are no longer needed.

Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought. In general this means destroying the information six months after the recruitment process has been completed (to cover the time limit for discrimination claims and taking account of any potential extensions).
Quick checklist

☐ Does your employer have a recruitment policy?

☐ Does it make appropriate reference to the General Data Protection Regulation (GDPR) and relevant workplace policies on data protection and equality?

☐ If the employer uses a recruitment agency do they comply fully with these policies?

☐ Is the recruitment policy clear about what personal information is collected for applicants, candidates and newly appointed staff members and why this information is needed?

☐ Are job applicants provided with a privacy policy containing information on the purposes for which all the data they provide will be processed, the legal basis for processing (i.e. legitimately needed for the recruitment exercise) and how long the data will be kept?

☐ Are job applicants told that equality and diversity monitoring information collected is separated from any personal information and is kept anonymous, and is this always done?

☐ Does your employer have a data retention policy?

☐ Is it clear about how the personal information is stored and that it is kept secure?

☐ Is it clear about how long the personal information is kept and how it is safely destroyed?

☐ Are applicants, candidates and newly appointed staff members made aware of why and how their personal information is collected and used?

More information:


Information Commission’s Office ‘Employment Practices Code’  
[https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)

Although it relates to the Data Protection Act, and this has been replaced by the General Data Protection Regulations, the principles still apply. It is hoped that updated guidance will be produced by ICO in due course.
Drugs and alcohol testing

Employers have a legal responsibility to look after employees’ wellbeing, health and safety. A good employer will want to help employees including those who misuse drugs or alcohol. A policy on drugs, alcohol and other substances developed in consultation with staff or health and safety representatives can be helpful in protecting workers from the dangers of substance misuse and to encourage those with a drug or alcohol problem to seek help.

However employers who decide to adopt alcohol or drug screening as part of their alcohol and drugs policy should ensure this is done lawfully and fairly. Screening is the way of testing whether employees have alcohol, drugs or other substances in their body. This may involve providing a urine sample.

Some employees, such as those who work in a safety critical area, may be automatically or randomly tested for alcohol or drugs due to the nature of their work. However UNISON has some concerns about the testing of workers. Screening is a sensitive matter. And while it is fairly straightforward to test for alcohol consumption and measure this against a legal limit, drug testing can be more complex.

Employers need the permission of employees to undertake screening and should only carry it out when they have a clear reason for testing under health and safety policy.

Medical records should be kept confidential. The screening test used should be as least intrusive as possible and take account of the fact that many people have conditions or impairments that require prescribed drugs.

Employers should ensure that:

- no-one is singled out during random testing
- if a search for alcohol or drugs is carried out then it must be by someone of the same sex, with a witness present
- employees are made aware of any possible disciplinary action they may face if they refuse a test.
However branches and reps should be aware that it is illegal if:

- an employee, under the influence of excess alcohol, is knowingly allowed to work (Health and Safety at Work Act)
- controlled substances are produced, supplied or used on an employer’s premises (The Misuse of Drugs Act)
- drivers of road vehicles and transport system workers are under the influence of drugs while driving or unfit through drugs while working (The Road Traffic and the Transport and Works Act).

**Quick checklist**

- Does your employer have an alcohol and drugs policy?
- Does it make appropriate reference to the General Data Protection Regulation (GDPR) and refer to relevant policies on data protection and health and safety?
- Has the employer undertaken a data protection impact assessment?
- Is any screening clearly related to the specific needs of the job such as working in a safety critical area?
- Is this need for screening of specified substances made clear to all staff?
- Is the alcohol or drugs policy used to ensure problems are dealt with effectively, and consistently and early on in the process?
- Do they protect workers and encourage sufferers to seek help?
- Where screening is being used to enforce the employer’s rules and standards, have these rules and standards been clearly set out to workers, along with any consequences of breaking them?
- Are the tests the least intrusive as possible?
- Are they provided by a professional service? And will workers have access to a duplicate sample so that independent analysis can take place if required?
- Is random testing genuinely random, without singling out any individuals?
- Is random testing necessary, or would post-incident testing be better justified?
- Does your employer have a data retention policy?
- Are medical records kept confidential and stored securely?
- Is it clear about how long the personal information is kept and how it is safely destroyed?

**More information:**

Phone, email and internet usage monitoring

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.

An employer has the right to specify which websites can or cannot be visited by staff and to introduce e-mail usage policies that prevent or limit personal use. They also have the right to access employees’ emails and voicemail while they are away from work to deal with matters of business, so long as staff have been informed that this is going to happen. Where the law becomes more complicated is where employers seek to actively monitor and intercept or even spy on the electronic communications of their staff.

Case law

_Halford v United Kingdom (1997)_
The European Court of Human Rights (ECHR) found that the employer breached Article 8 of the European Convention on Human Rights on privacy when it intercepted the phone calls made from work by an employee, a senior police officer. No warning was given that her phone was tapped and so it was considered that the employee would have had a reasonable expectation of privacy in relation to her calls.

_Copland v UK (2007)_
The ECHR found that the employer breached Article 8 because of the way in which it monitored the employee’s telephone calls, email correspondence and internet use.
The employer wanted to check if she was making excessive personal use of them but failed to warn her of the monitoring.

**Simpkin v The Berkeley Group Holdings plc (2017)**

This case went to the High Court of England and Wales where it was decided that the employee should not reasonably expect privacy when he used his work computer system for personal emails. This was in part because the employee had seen and signed a copy of the employer’s IT policy, which clearly stated that emails sent and received on the employer’s computer system were the property of the employer.

**Barbulescu v Romania (2017)**

The Grand Chamber of the European Court of Human Rights’ found that a sales employee had his human rights under Article 8 breached (reversing the Chamber’s earlier decision). The employee had not been notified by his employer that his work instant messaging account would be monitored, although the employer’s internal regulations did prohibit use of company resources for personal purposes. The employee was dismissed for using the messaging system to contact his brother and fiancée after his messages were extensively monitored without any warning.

Employers are now using a range of sophisticated computer monitoring packages easily available on the market, which can monitor the 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. 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.

Employers may also be opening mail or e-mail, using software to access emails, checking phone logs and numbers called, recording phone calls, checking logs and computer ‘histories’ of websites visited etc.

**UNISON cases**

**UNISON Scotland utilities service groups (energy & water)** undertook a survey of members in customer facing jobs in call centres and similar workplaces in 2004. Results showed “a high level of electronic monitoring by e-mail, phone and other electronic measurement, the latter mostly in contact centres using performance monitoring software. For the majority of staff this included private communications. Several respondents gave examples of calls from family members being listened into even when they were clearly of a highly personal nature. One respondent gave an example of her team manager printing e-mail from a relative describing an urgent family crisis including medical details…

“…The most worrying results from the survey came when respondents were asked what impact the monitoring had on them. ‘Demeaning’ was the most common response with more than half finding monitoring stressful. More than half suffered from different levels of anxiety with 17% suffering from depression. A number of staff
explained that monitoring caused a loss of sleep and extended sickness absence.” Additionally 52% of respondents considered resigning as a result of electronic monitoring.

The survey follows an Incomes Data Services (IDS) report in 2003 which showed more than 60% of Scotland’s call centres had problems retaining staff, compared to 25% across the UK.

**UNISON reps across the UK** have reported cases where staff have been disciplined for forwarding on offensive jokes / emails and copyrighted 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. **UNISON activists** have also been investigated under their employers’ disciplinary procedure for receiving a **UNISON newsletter** about LGBT equality.

It is important that UNISON reps raise issues about unfair and unreasonable monitoring with the employer to make sure there is an agreement so that, for example these type of legitimate emails are not blocked and that staff are not investigated.

Use of social media can also get workers into trouble, particularly accessing sites such as Facebook or Twitter during work time. Any ‘Acceptable Use Policy’ should highlight how social media is a legitimate form of communication which is used at work and that, as long as it it’s not interfering with business it can be accessed.

If a branch is concerned that an employer is monitoring union reps, for example by checking their union business emails, they should speak to their regional officer and make sure this is raised at a staff-side meeting with management.

Employers should strike a balance in their monitoring between what is a legitimate need of the business against the employee’s right to privacy, and workers should be notified about the monitoring undertaken. 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.
Quick checklist

☐ Does your employer have a clear policy on the use of the employer's phones and computers and Wi-Fi for personal use, and are employees clearly made aware of this policy?

☐ Does it make appropriate reference to the General Data Protection Regulation (GDPR) and fulfil its requirements?

☐ Does the employer make clear as to what counts as a reasonable amount of personal emails, personal phone calls and internet access for personal use, including clarification on any restrictions on material that can be viewed or copied, or when they are not allowed?

☐ Does the employer have a privacy policy that all employees know about?

☐ If there is monitoring, screening or recording of phone, email or internet use, have all staff been notified that it is taking place?

☐ Is monitoring clearly not excessive and fully justified?

☐ Is it really necessary to monitor all IT facilities at work and can some areas within the system or through free Wi-Fi be made available for private use?

☐ Rather than monitor individuals, can access be blocked, for example to certain websites?

☐ How is the issue of monitoring addressed where workers can use their own or other organisation’s equipment such as when they are working from home?

☐ Does the employer have a data retention policy?

☐ Are staff told what information is recorded and how long it is kept?

☐ Is storage sufficiently secure?
CCTV monitoring and audio recording

Increasingly CCTV and other types of cameras are being used in the workplace for surveillance of workers and of customers or service-users. Nowadays there may also be wifi cameras, ‘dash cams’ in drivers cabs or on courier bikes. Body worn cameras are also being used such as by police officers and within the NHS. These can be particularly intrusive as they can pick up audio recordings as well as images.

Usually the use of such devices is to protect the safety of people (e.g. as part of a preventative measure where staff assaults have previously been recorded or to provide evidence where there are accidents) and to enhance the security and safety of premises and property.

The Information Commissioner’s Office ‘In the picture: A data protection code of practice for surveillance cameras and personal information’
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf covers the use of CCTV and is based on data protection principles. The code also covers “the use of camera related surveillance equipment including:

- Automatic Number Plate Recognition (ANPR);
- body worn video (BWV);
- unmanned aerial systems (UAS); and
- other systems that capture information of identifiable individuals or information relating to individuals.”

Although it relates to the Data Protection Act, and this has been replaced by the General Data Protection Regulations, the principles still apply. It is hoped that updated guidance will be produced by ICO in due course.

Although the code of practice is not legally binding, by following it employers ensure that they operate within the requirements of the law. It also highlights good practice. Similarly the Surveillance Camera Code of Practice under the Protection of Freedoms Act
ment_data/file/157901/code-of-practice.pdf) provides a basis for good practice, although it only applies legally to public authorities.

A key issue stressed by the ICO guidance is that video or audio monitoring of individuals is “only likely to be justified in rare circumstances.”

It should be noted that the code also describes “the use of audio recording, particularly where it is continuous, will, in most situations, be considered more privacy intrusive than purely visual recording. Its use will therefore require much greater justification.”

More information:

Information Commissioner’s Office ‘In the picture: A data protection code of practice for surveillance cameras and personal information’

Employees may be unconcerned about the use of most standard monitoring (CCTV) in the workplace if the areas are signposted and the reasons for any monitoring and surveillance are transparent and set out to staff. It should also be made clear to them who is able to watch footage and when it will be watched. Cameras should not be placed in areas where employees would normally expect privacy – for example private meeting rooms. In addition, staff should be reassured about the company operating the CCTV system and their security and handling of the data, if not done by the employer directly.

However in some workplaces such as care homes, the use of CCTV cameras may have a place as a short-term reassurance measure or to deter or detect abusers, but
should not be introduced as a means of papering over underlying problems and poor practices.

For example, if the particular problem is about providing reassurance to absent relatives, perhaps Skype and webcam facilities can be made available so that they keep in touch visually as well as by phone; if the problem is about deterring abusers, could the provider instead improve their training, vetting and supervision procedures, as well as consider increasing staff numbers and providing trusted ways for staff to raise concerns about standards of care?

**Care homes**

Incidents of abusive or neglectful care in care homes and hospitals (Winterbourne View, Orchid View and mid-Staffordshire NHS Trust) have led to increased use of surveillance cameras to deter and detect poor care.

Inspectors at the [Care Quality Commission (CQC)](https://www.cqc.org.uk/) issued guidance in 2014 (updated in 2015) on using surveillance to monitor service.

The guidance states “The decision whether to use surveillance is for care providers to make in consultation with the people who use their services, and with families, carers, trade unions and staff… However, there are other, less intrusive steps a provider can take to ensure that care is high quality and safe… We would be concerned by an over-reliance on surveillance to deliver key elements of care, and it can never be a substitute for trained and well supported staff.”

As UNISON’s general secretary, Dave Prentis pointed out in 2015 “Cameras might go some way towards reassuring people that their relatives are being well looked after but CCTV will do nothing to address any of the fundamental problems that can lead to poor and abusive care.

“Many care homes have a high turnover of staff, do not provide enough training, and low wages and unsocial hours make it difficult for many to recruit enough staff to provide proper care to the residents. Without substantial investment in the care sector, these problems will simply worsen as the UK’s population ages.”

**Use of smart phone apps**

UNISON reps have also reported the increased use of mobile phone apps in particular by social care employers. For example, apps used to access individual workers’ rota details and service users' information will be covered by the General Data Protection Regulations if they include access to personal data (and perhaps not only of the worker, but also of the service user), and therefore the data needs to be processed lawfully and fairly.

This would mean that potentially both the worker and the service user would need to have informed consent for use of the apps. As the Information Commissioner’s
Office (ICO) guidance ‘Privacy in mobile’ (https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf) warns: “Personal data is not limited to information typically considered a traditional identifier, such as an individual's name or a photograph of their face. A good example in the mobile environment would be a unique device identifier such as an IMEI number: even though this does not name the individual, if it is used to treat individuals differently it will fit the definition of personal data.”

With apps it would also be important to identify the data controller and data processor, which could include consideration of not only the employer but the app developer, ‘cloud’ provider etc.

The ICO also point out: “You should only collect and process the minimum data necessary for the tasks that you want your app to perform... You should aim to use the least privacy-intrusive data possible.” It would also be essential to ensure that any data collected is stored securely.

In addition, in order to comply with the Privacy and Electronic Communications Regulations (PECR) if relevant (see above), the ICO also states that “app developers should ... provide clear information to users about what the app does, and exactly how it uses their information, before users click to install the app. It is also important to consider user privacy controls and avoid switching optional features on by default. This ties in closely with the requirements of the Data Protection Act and the GDPR.”

**UNISON Case**

A UNISON community branch reported concerns about how social care employers were requiring staff to download the PeoplePlanner app to their personal mobile. The app downloads and stores personal details varying from employer to employer, but can include address and other contact details, sickness, availability for rota scheduling, pay information, training and development information and client/service user’s contact details and care plans.

In addition to concern about the personal data being collected by the app, the workers were particularly concerned that they were being asked to download it on their personal mobiles thereby blurring the line between work and private. Not only could this impact on the type of data being collected, it meant that the employer passed on any related mobile data usage costs to the worker. It could also put the personal data of service users at a greater security risk.

The issue was raised via a grievance with the employer in the community sector. On hearing the concerns, the employer agreed to provide staff with work mobiles and issued guidance to staff on how to delete the app from their personal phones.

**Use of other tracking devices**
Audio recording, radio-frequency identification (RFID) tracking, mobile phone apps and many other types of tracking systems are also increasingly being used by employers. For example, some employers have a legal obligation to track business vehicles over 3,500kg or more and tachographs need to be fitted.

UNISON branches have been reporting an increase in the use of vehicle monitoring especially in some home care and private sector 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. Cameras pointed at drivers that can monitor every aspect of the driver’s behaviour are particularly controversial. Difficulties particularly arise when the purpose given is for security or health and safety and then the footage is also used for performance management.

**UNISON Cases**

UNISON’s 2016 water, environment and transport conference heard from delegates that many employers in this sector have introduced tracking or ‘telematics’ technology in some form. This technology can track the location and movement of both vehicles and individuals in real-time, providing statistical and geo-locational information.

Although the conference acknowledged that there can be some benefits regarding health and safety when this technology is used in a sensible way on liveried vehicles, it had serious concerns about the way in which telematics has become routinely part of disciplinary and performance procedures.

In some circumstances this has led to employees being disciplined for accelerating a vehicle to avoid a collision; employees becoming distracted by monitoring telematic information, leading to road traffic accidents; employers inappropriately accessing private information about the lives of their employees.

Like CCTV monitoring, these types of surveillance are covered by the General Data Protection Regulations. It should only be introduced by agreement and staff should be made aware of the purpose of collecting the information and how it will be used, stored and deleted.

But where a vehicle is being used for private use as well as business use, it is hard to justify vehicle tracking devices unless the opportunity for privacy has been addressed and there is a facility for the employee to switch a button on the device to disable the monitoring.

Even more worryingly, in November 2018 there were news reports that some major UK companies were preparing to microchip their employees using the same technology implanted in household pets. The TUC commented that: “Asking people to be microchipped at work is a sinister step too far. And there’s an obvious risk that this sort of technology could be misused and put workers in danger... So instead of
microchipping their workforce, bosses need to start engaging with staff and unions to make new technology work for everyone.”

**Covert monitoring**

Covert monitoring is rarely used in the workplace as it is extremely hard for the employer to justify the secret recording of 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.

**Case law**

*Lopez Ribalda and others v Spain (2018)*

The European Court of Human Rights (ECHR) decided that a fair balance between a supermarket wanting to protect their property from employee theft and the workers’ right to privacy was not met when the supermarket installed hidden cameras unknown to the staff. The ECHR found that the shop workers’ right to privacy under Article 8 of the European Convention on Human Rights had been breached. Use of the hidden surveillance was found to be disproportionate, being over a long period and suspecting all staff, rather than following on from investigations so that any covert surveillance could be targeted.

*City and County of Swansea v Gayle (2013)*

The Employment Appeal Tribunal (EAT) decided that the covert video surveillance of an employee suspected of regularly leaving work early was not a breach of their right to privacy. This was because the filming took place in a public space and done during working hours when the employer is entitled to know where their staff members are and what they are doing.

Employees need to be aware that covert surveillance without knowledge and consent may constitute a breach of the individual’s privacy under Article 8 of the Human Rights Act. The recording will be considered as personal data under the General Data Protection Regulation and therefore needs to be processed lawfully and fairly.

The Information Commissioner’s Officer’s ‘Employment Practices Code’ states that employers should “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.”

They should “deploy covert monitoring only as part of a specific investigation and cease once the investigation has been completed.”
Use of monitoring and surveillance information in a disciplinary case

In some workplace investigations and disciplinary cases, emails, CCTV and other surveillance data have been used as part of the case. Employees should be made aware that most workplaces have the capacity to access even deleted emails for a considerable time after they were sent.

ACAS guidance on conducting workplace investigations for disciplinary and grievances at work makes reference to the use of monitoring and surveillance methods in cases, but does also state:

“Policies and employee contracts should clarify whether or not an employer may use CCTV recordings and/or personal employee data as evidence in disciplinary and grievance matters.

“Where this is not the case, an employer should only use such evidence where it is not practicable to establish the facts of the matter through the collection of other evidence only.”

Further information:

Acas guidance: Conducting workplace investigations
http://www.acas.org.uk/media/pdf/e/h/Conducting_Workplace_Investigations_Feb_191.pdf

Where CCTV and other surveillance evidence is 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.

If an employer wants to record a meeting so that they can keep full details of what was discussed, such as a disciplinary hearing, they must ask the consent of all present at the meeting. They should respect the rights of all the individuals present if they refuse to give consent. Such recordings should be disclosed in response to a subject access request.

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 in the use of some of these practices as a way of monitoring staff time-keeping and sickness absence.
The Deputy Commissioner for Policy at ICO recently highlighted some key points for organisations planning to use new and innovative technologies that involve personal data, including biometric data, to consider:

“1) Under the GDPR, controllers are required to complete a DPIA [a data protection impact assessment] where their processing is ‘likely to result in a high risk to the rights and freedoms of natural persons’ such as the (large scale) use of biometric data. A DPIA is a process which should also ensure that responsible controllers to incorporate ‘data protection by design and by default’ principles into their projects. Data protection by design and default is a key concept at the heart of GDPR compliance.

2) When you’ve done your DPIA, make sure you act upon the risks identified and demonstrate you have taken it into account. Use it to inform your work.

3) Accountability is one of the data protection principles of the GDPR - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance by putting appropriate technical and organisational measures in place.

4) If you are planning to rely on consent as a legal basis, then remember that biometric data is classed as special category data under GDPR and any consent obtained must be explicit. The benefits from the technology cannot override the need to meet this legal obligation.”

Case studies: Biometrics

UNISON’S City of Westminster branch 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.

In spring 2018, employees of Community Integrated Care (CIC), a national care charity expressed concern at the introduction of a new sign-in system, and have sent a collective letter to the employer questioning the legitimacy of its use under GDPR. This hi-tech clock-in machine identifies staff by their fingerprints and photographs them each time they sign in or out. Staff who work through the night are required to sign in every hour, which they say can interrupt them attending to people in their care.

UNISON assistant general secretary Christina McAnea said:“Staff want to be able to respond to the needs of the people they care for, not the requirements of a machine. CIC should have more trust in their employees and allow them to get on with their work.”
Workers were not asked for consent for their biometric data to be used by CIC and were not advised why they need to be repeatedly photographed. As reported in a *Left Foot Forward* article, a spokesperson for CIC justified the use of the biometric data under the General Data Protection Regulation without consent “as the data is used to pay our colleagues, which is for the purposes of us carrying out our obligation as stated in contracts of employment.”

However a spokesperson for the Information Commissioner's Office expressed some concern: “Biometric data, including fingerprints, are classed as special category personal data… Organisations are prohibited from processing special category data unless they can satisfy one of 10 conditions, including obtaining individuals’ explicit consent.”

UNISON North West regional office has made a complaint to the ICO about CIC on the basis that:

- The employer has not been transparent about how they will be using the data.
- The employer does not have employee consent, nor have they evidenced a different lawful basis for processing.
- The employer has not provided a data protection impact assessment (required if the employer is going to rely on a lawful basis other than consent) to the union, despite us requesting it.
- There is a less privacy intrusive way of achieving the same aim.

At the time of writing, a response to the complaint from ICO is still expected.

There may be circumstances in which biometric monitoring of staff could be justified on the grounds of security. Each case should be judged on its own merits with the need to avoid excessive monitoring balanced against security concerns. For example, there could be a case for introducing biometric monitoring for staff accessing hazardous materials or extremely sensitive information.
Nevertheless, an exceptional case would need to be made for any new system using biometrics. This should be focused on security rather than monitoring staff and should only be introduced after full and comprehensive consultation with staff and their trade unions.
Quick checklist

☐ If CCTV, audio recording, tracking devices, smart phone apps, use of biometrics or covert surveillance is taking place or is planned to be used, has the employer undertaken a data protection impact assessment?

☐ Has the employer fully considered the requirements of the General Data Protection Regulation, the Human Rights Act and if relevant the Privacy and Electronic Communications Regulations and codes of practice such as on use of CCTV?

☐ Has the employer consulted with workers and their trade union representatives on the use of surveillance, its purpose and how it will be carried out?

☐ What problem is the employer trying to solve and how does this particular type of monitoring address this problem?

☐ What evidence of the problem do they have and is it sufficiently serious such as criminal activity or malpractice?

☐ Is the surveillance solely restricted to the specific investigation or area of risk, and occurring within a strict time frame? The employer cannot use the footage for another reason if it is different than the given reason.

☐ Who is covered by the monitoring, is it all staff or just certain departments? If used, are the CCTV cameras going to be in public areas?

☐ Who is responsible for monitoring the cameras or other tracking device or smart phone, and for storing the information? For phone apps, is a specific work mobile provided to workers?

☐ Is there an agreed written policy covering the use of CCTV and/or tracking device or app in the workplace, how the information is to be securely stored and for how long?

☐ Does the policy also outline agreed procedures for staff to have prompt access to data recorded as is their right under GDPR?

☐ If covert surveillance is proposed, why is it not possible to ask the employee/s consent and is this reasonable?

☐ Are no alternative measures possible, indeed preferable (less intrusive, less costly, less controversial)?

☐ How much will introducing the new monitoring or surveillance system or procedure cost? Could this money be more effectively spent on staff training and increasing staff numbers for example?

☐ What other measures has the employer considered?

☐ Have individuals given explicit consent for the use of ‘special category personal data’ or, if not, (as in the use of covert surveillance) can the employer demonstrate that they fulfil other data protection conditions?
☐ Are there obvious signs for all to see warning of the CCTV or other monitoring and do these signs also explain why there is surveillance and who to contact about the scheme?

☐ Do staff know where the cameras (if used) are located? Are they situated in suitable and appropriate areas (and not in areas where a higher level of privacy is expected such as near toilets or break areas).

☐ Do they know when they are being watched or monitored – is it only because of a particular concern or will they be constantly monitored?

☐ If monitoring is to be used to enforce rules and standards, do workers clearly know what these are?

☐ Has the employer been explicit about who has access to the information collected and that any information collected is deleted if it is not relevant to the specific investigation or when the worker leaves the organisation.

☐ Does the employer collect, store and destroy data collected in line with GDPR? Digital data is particularly vulnerable to a breach of security – is this sufficiently considered by the employer?

☐ If any data is removed or deleted, is it done in such a way that it is not recoverable? For example, there are several organisations that will forensically clean a computer hard drive and provide a data destruction certificate to prove that it has been done.
Releasing information to prevent or detect crime

The police or other crime prevention / law enforcement agencies (e.g. Benefit Fraud Office and local authority functions) sometimes contact data controllers and request that personal data is disclosed in order to help them prevent or detect a crime. UNISON does not have to comply with these requests, but the data protection regulation does allow organisations to release the information if they decide it is appropriate.

Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This includes considering:

- The impact on the privacy of the individual/s concerned
- Any duty of confidentiality owed to the individual/s
- Whether refusing disclosure would impact the requesting organisation’s ability to detect, prevent or prosecute an offender.

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for UNISON to release the information.
3. **Putting the case to employers for negotiations**

It’s imperative that any monitoring or surveillance undertaken in the workplace should be proportionate and necessary, and should be carefully considered as to how intrusive it is on the individual and their privacy.

**Why is it important for employers to take this on board?**

**i. To keep within the law**

Employers need to fully consider and comply with the General Data Protection Regulation (GDPR) and Article 8 of the European Convention on Human Rights. Other legislation may also be relevant – further details in section 1.

It is also worth pointing out to employers that under the old Data Protection Act, they just had to comply with the law. Under GDPR, they now have to be able to actively demonstrate to the regulator that they are complying with the law, with a lawful reason for collecting the information and transparency about its collection and use.

Fines for getting it wrong have increased to 20 million Euros or 4% of the total annual worldwide turnover (whichever is greater).

So a starting point for any branch or rep is to look at the employer’s data protection policy and to ask for the data protection impact assessment. Assuming they exist (and they should) can the employer demonstrate that they are being followed and in doing so they are being compliant with GDPR?

**ii. To avoid an adverse impact on your workers**

The Information Commissioner’s Office ‘Employment Practices Code’ warns that:

> “Monitoring may, to varying degrees, have an adverse impact on workers. It may intrude into their private lives, undermine respect for their correspondence or interfere with the relationship of mutual trust and confidence that should exist between them and their employer. The extent to which it does this may not always be immediately obvious. It is not always easy to draw a distinction between work-place and private information. For example monitoring e-mail messages from a worker to an occupational health advisor, or messages between workers and their trade union representatives, can give rise to concern.”

Overuse of monitoring and surveillance in the workplace can be considered as oppressive or demeaning. Inevitably it will create an environment of distrust and suspicion, and it could even lead workers to want to sabotage or trick surveillance systems.

The TUC’s report on workplace monitoring ‘I’ll be watching you’ ([https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you](https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you)) found that “a strong majority of workers (65%) believe that the introduction of a new type of surveillance would have a damaging impact on their relationship with their
Monitoring and surveillance in the workplace

Employers need to be reminded that it is impossible to completely stop the private lives of workers from extending into the workplace. Monitoring will also inevitably mean that information that is confidential, private or sensitive (not only to the individual but also perhaps to the business) is seen by those who do not have a business need to know, such as IT workers involved in monitoring emails.

Monitoring can erode the relationship of mutual trust and confidence that should exist between workers and their employer. This can then lead to a lack of loyalty by workers, high staff turnover and the high cost of recruiting replacement staff. Then there is the knock-on effect on customer service, customer retention and output.

**What impact can it make on staff morale, performance levels and the relationship with the employer?**

2011 research (‘Employee perception towards electronic monitoring at workplace…’ undertaken by Viraj Samaranayake and Chandana Gamage) showed that the greater the perception of invasion of privacy, the lower the job satisfaction was. Workers feel less in control of their work and this can lead to increased stress and a reduction in productivity.

2015 research (‘An Investigation of Attitudes toward Surveillance at Work and Its Correlates’ undertaken by Adrian Furnham and Viren Swami) found that higher scores on negative aspects of surveillance were significantly associated with lower job satisfaction, lower job autonomy, greater perceived discrimination at work and more negative attitudes to authority.

**iii. To let staff get on with their work**

Excessive monitoring and surveillance systems can not only inhibit staff in their day-to-day work, but also use up too much of their time unnecessarily (for example having to regularly sign in with tracking or biometric devices) which should be spent on the actual work responsibilities.

In contrast, employers can raise productivity and improve loyalty and job satisfaction by ensuring staff are able to focus on work whilst at work, without constantly worrying about being watched.

**iv. Because it’s expensive**

We all know that money is tight in the public sector and highly sophisticated, technological monitoring and surveillance systems can be very costly, not only to set up but also to operate and maintain. Can the employer really justify purchasing such a system for the workplace?
Consult members and highlight the particular impact it could have in your workplace

- The branch could organise meetings, send around a member survey on the issue, and report the finding back to the members, and to the employer perhaps in the form of a collective letter.

- Raising awareness of GDPR issues and individual privacy rights as well as how an employer could potentially be operating outside of the law, could provide a valuable recruitment and organising focus for a workplace.

- A survey of all staff at a particular workplace, could not only provide necessary feedback for the employer, but be a useful recruitment tool. Employers may not understand what the strength of feeling is on this issue, particularly the storage of personal data such as those collected from CCTV, biometric monitoring and other tracking devices and smart phone apps.
Other information:

**Information Commissioner’s Office** [https://ico.org.uk/for-organisations](https://ico.org.uk/for-organisations)
Information on data protection for organisations about their obligations and how to comply, including protecting personal information and providing access to official information.


**Data protection: the employment practices code** [https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)
Now archived by ICO, the code aims to help employers comply with the Data Protection Act (DPA) and to encourage them to adopt good practice. Although it does relate to the DPA rather than the requirements of the GDPR, the key principles are the same. It is hoped that updated guidance will be produced by ICO in due course.

**What are PECR?** (Privacy and Electronic Communications Regulations) [https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/](https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/)

**Cookies and similar technologies** [includes smart device apps] [https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies](https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies)


Working with the Home Office, the aim of the Commissioner is to encourage compliance with the surveillance camera code of practice.


**UNISON’s Privacy Policy** [www.unison.org.uk/privacy-policy/](www.unison.org.uk/privacy-policy/)


**TUC’s I’ll be watching you: a report on workplace monitoring** [https://www.tuc.org.uk/research-analysis/reports/%E2%80%99I%E2%80%99ll-be-watching-you](https://www.tuc.org.uk/research-analysis/reports/%E2%80%99I%E2%80%99ll-be-watching-you)

UNISON’s health and safety guide on lone working, Working Alone

Contact your regional education teams and / or LAOS to find out what training and resources are available to assist you with negotiating with your employer or promoting the issues in this guide with your members https://learning.unison.org.uk/
4. **Model monitoring and surveillance in the workplace policy**

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

These policies should always make reference to the General Data Protection Regulation (GDPR) and how the employer is fulfilling its requirements.

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.

The following model policy can be used in the workplace to help ensure excessive and unnecessary monitoring and surveillance does not take place. However it will need to be adapted as relevant to your workplace.

Please note that the text in square brackets [...] indicates where you need to complete information specific to your workplace, or else are notes for you to consider in relation to your negotiations.

**Policy Statement**

*Name of employer* is committed to developing a workplace culture where there is a respect for the private life, data protection, security and confidentiality of personal information, and *name of employer* complies with the requirements of the General Data Protection Regulation (GDPR) and Information Commissioner's Office (ICO) Employment Practices Code.

*Name of employer* is committed to treating all staff members fairly and this policy aims to provide consistency in the treatment of all staff. Serious infringement of data protection rules including in relation to the collection, content inspection, use and storage of data through the monitoring and surveillance systems in the workplace, will be treated as a serious disciplinary matter.

More details can be found in the ‘Data protection policy’ and/or ‘Privacy notice’ [amend as appropriate] at [include links or signpost to the appropriate policy]. *Name of employer* has appointed [name and contact details] as its data protection officer.
Scope of Policy

This policy applies to all staff who are employed at [name of employer].
This policy is supported by and developed with the trade unions representing the employees.

Purpose

[name of employer] recognises that there is a need to balance staff privacy in the workplace along with ensuring the health and safety of staff and that [name of employer] is complying with regulatory and statutory obligations.

This policy sets out how [name of employer] aims to provide this balance in the monitoring and surveillance undertaken in the workplace.

Telephones and ICT acceptable use

[This is a very basic example of acceptable use policy details. Details will always be specific to individual workplaces as appropriate to the type of work undertaken and as negotiated with the trade union. But as Acas guidance points out, “the policy should aim to ensure: employees do not feel gagged; staff and managers feel protected against online bullying; and the organisation feels confident its reputation will be guarded.”]

[name of employer] recognises that employers will need to access telephones, mobile phones, ICT devices, services and software for [name of employer]’s emails and the internet (including for social media) for business use and that they provide an integral part of how [name of employer] communicates with our service users/customers, the general public and stakeholders, and between staff.

[name of employer] allows employees reasonable, limited, occasional and brief access to telephones, mobile phones, computers and other devices (including for internet, emailing and social media) for personal use during working times, as long it does not interfere with staff members’ work. Employees are encouraged to limit such usage during their official rest breaks such as their lunch break/times.

[name of employer] does not provide any guarantees regarding the privacy or security of any personal use of [name of employer]’s telephones, mobile phones, computers and other devices and employees do so at their own risk. Any material and information for personal use that is stored on [name of employer]’s telephones, mobile phones, computers and other devices can be accessed by [name of employer] in the same way as it can access other material and information.

Unacceptable use of [name of employer]’s telephones, mobile phones, computers and other devices includes (but is not limited to) usage involving:

- unlawful or illegal activity
- creating, transmitting, downloading, displaying or storing offensive, obscene or indecent data or material
• creating, transmitting, downloading, displaying or storing of material that deliberately discriminates, bullies, harasses, victimises or encourages discrimination, bullying and harassment or victimisation
• creating or transmitting defamatory material
• creating or transmitting material that brings the [name of employer] into disrepute
• obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper authority
• creation or transmission of material with the intent to defraud or which is likely to deceive a third party
• commercial uses unrelated to the interests of [name of employer]
• uses that are likely to cause annoyance or inconvenience, e.g. sending unsolicited email chain letters
• inappropriate or careless use of data e.g. sharing information when not authorised to do so (especially special category personal data), or emailing information to the wrong recipient
• corrupting or destroying another user’s data or violating their privacy
• deliberately introducing, executing or transmitting malware
• deliberately disabling or compromising [name of employer]’s security systems
• physical or other damage to [name of employer]’s telephones, mobile phones, computers and other devices.

[Amend this list as appropriate.]

Unacceptable use will be treated as a disciplinary matter.

[Name of employer] has specifically blocked use of [state any particular website or social media site that is blocked] on its computers. [Delete this paragraph if not relevant.]

[Name of employer] recognises that employees may wish to use their own mobile phones, computers and other devices (including for internet, emailing and social media) while they are at work. Employees are encouraged to limit such usage during their official rest breaks such as their lunch break/times.

Excessive use of [name of employer]’s telephones, mobile phones, computers and other devices or the employee’s own mobile phones, computers and other devices for personal use during work time, so that it interferes with the employee’s duties, may be dealt with through the disciplinary process.
Where employees make reference to [name of employer] on social media in their personal life, it should not:

- bring the organisation into disrepute
- breach confidentiality
- breach copyright
- deliberately discriminate, bully, harass or victimise others or encourage discrimination, bullying, harassment or victimisation

[Amend this list as appropriate.]

Such inappropriate use of social media may be dealt with through the disciplinary process.

**Monitoring of telephones and ICT usage**

[name of employer] reserves the right to monitor the use of [name of employer]'s ICT, telephone and mobile phone services, and access any information stored on the ICT and telephone and mobile phone infrastructure (including apps), in line with relevant legislation and guidance provided by the Information Commissioner’s Office, to fulfil legitimate business needs, such as (but not limited to):

- complying with regulatory and statutory obligations
- assessing compliance with the health and safety and security policies [include links or signpost to the appropriate policy or amend as appropriate] and acceptable use as outlined above
- preventing and detecting unauthorised use or other threats to the ICT systems
- preventing and detecting crime
- monitoring system performance.

All monitoring will be conducted in accordance with a data protection impact assessment that [name of employer] has carried out to ensure that monitoring is necessary and proportionate, and details will be shared with the trade union. Further details can be found in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

Systematic monitoring (i.e. monitoring arrangements as a matter of routine) will not be person specific.

Occasional monitoring of an individual may be introduced in response to a particular problem or need. Normally the member of staff will be told that such monitoring is to take place and the reasons for the monitoring, as well as being provided with a start and end date for monitoring. However any monitoring of individuals will not normally take place during official rest breaks such as lunch break/times, unless this has been identified as relevant to the investigation.
Content inspections can only happen after permission has been granted by the Head of Human Resources [amend as appropriate] or higher.

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 is to be viewed, the reason for the access and who it is to be disclosed to.

Requests for access to the telephone, mobile phone, email account or restricted folder of a member of staff must be made in writing to the Head of Human Resources [amend as appropriate]. The request must detail the reason for access and the information to be viewed.

Upon receipt of an approved request from the Head of Human Resources [amend as appropriate], a member of the ICT staff will undertake a content inspection and will record:

- what information was inspected
- the computer or telephone on which the monitoring took place
- the start and the end time of the monitoring
- the identity of the person performing the inspection.

The information collected may only be shared with the individual being monitored, and the Head of Human Resources and/or Head of Security [amend as appropriate]. It will only be shared with the line manager if appropriate and identified as not excessively intrusive.

Those who have access to the information will always be kept to a minimum and they must comply with the ‘Data protection policy’ at [include links or signpost to the appropriate policy]. They must receive training on data protection principles that arise when carrying out monitoring.

The information collected will be stored securely and only for a limited time in order to complete an investigation. In normal circumstances it will be securely deleted after 7 [amend as appropriate] days.

[Name of employer] will regard any attempt to conduct a content inspection that is not in accordance with this policy as gross misconduct.

Staff members have a right to access the ICT and telephone data held on them and to have data rectified or erased in some circumstances. Requests should be made as a subject access request, details included in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

CCTV (and/or other tracking or audio recording or biometric monitoring arrangements)
Monitoring and surveillance in the workplace

The use of CCTV [and/or other tracking or audio recording or biometric monitoring arrangements] is in line with relevant legislation and guidance provided by the Information Commissioner’s Office and the Surveillance Camera Commissioner, to fulfil legitimate business needs, such as (but not limited to):

- complying with regulatory and statutory obligations
- assessing compliance with the health and safety policy
- preventing and detecting crime.

All use of CCTV [and/or other tracking or audio recording or biometric monitoring arrangements] will be conducted in accordance with a data protection impact assessment that [name of employer] has carried out to ensure that monitoring is necessary and proportionate in order to address a specified problem, and details will be shared with the trade union. Further details can be found in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

Cameras [and/or other tracking or audio recording or biometric monitoring arrangements] will be located in [specify locations] and signs will be displayed notifying staff members of the CCTV [and/or other tracking or audio recording or biometric monitoring arrangements] use and purpose, and who to contact about their operation.

Intrusion of staff privacy will always be kept to a minimum and surveillance will not normally take place during official rest breaks such as lunch break/times.

CCTV footage [and/or tracking or audio recordings or biometric monitoring data] will be stored securely and only for a limited time in order to complete an investigation. In normal circumstances it will be securely deleted after 7 [amend as appropriate] days.

Requests for access to the footage [and/or recordings or biometric monitoring data] must be made in writing to the Head of Human Resources [amend as appropriate]. The request must detail the reason for access and the information to be viewed.

The information collected may only be shared with the Head of Human Resources and/or Head of Security [amend as appropriate]. It will only be shared with the line manager if appropriate and identified as not excessively intrusive.

Those who have access to the footage will always be kept to a minimum and they must comply with the ‘Data protection policy’ at [include links or signpost to the appropriate policy]. They must receive training on data protection principles that arise when carrying out monitoring.

[Name of employer] will regard any attempt to use CCTV [and/or other tracking or audio recording or biometric monitoring arrangements] that is not in accordance with this policy as gross misconduct.
Staff members have a right to view images of themselves recorded by the CCTV [and/or audio recordings or biometric records] and to receive a copy of these images [and/or audio recordings or biometric records], and to have data erased in some circumstances. Requests should be made as a subject access request, details included in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

Covert Monitoring

Where [name of employer] has good reason to suspect that a member of staff is engaging in criminal activity or equivalent malpractice, it may in very exceptional circumstances introduce covert monitoring of the individual.

All such monitoring will be conducted in accordance with a data protection impact assessment that [name of employer] has carried out to ensure that monitoring is necessary and proportionate, and details will be shared with the trade union. Further details can be found in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

Covert monitoring will take place within a very strict timeframe and will only be targeted at gaining evidence. This type of monitoring and surveillance can only be authorised by the Chief Executive [amend as appropriate].

The information collected may only be shared with the Head of Human Resources and/or Head of Security [amend as appropriate]. It will only be shared with the line manager if appropriate and identified as not excessively intrusive.

Those who have access to the information will always be kept to a minimum and they must comply with the ‘Data protection policy’ at [include links or signpost to the appropriate policy]. They must receive training on data protection principles that arise when carrying out monitoring.

Staff members have a right to access the data held on them and to have data rectified or erased in some circumstances. Requests should be made as a subject access request, details included in the ‘Data protection policy’ at [include links or signpost to the appropriate policy].

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

If, following covert monitoring, evidence of criminal activity is recorded, this must be referred to the appropriate body such as the police to press charges.

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

Responsibilities of managers
Line managers should ensure that all staff members are aware of this policy and understand their own and the employer’s responsibilities. Training on data protection and privacy issues will be provided to all managers.

[Name of employer] should remind staff members at regular intervals of this policy and related policies and where to find them. [Name of employer] will provide induction and refresher staff training on the policy and compliance with the General Data Protection Regulation.

Trade union involvement

Consultation will take place with the recognised trade union on the implementation, development, monitoring and review of this policy.

Union reps will be given training equal to that of managers and supervisors and sufficient time to carry out their duties.

Privacy

[Name of employer] recognises 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 workplace. Therefore this monitoring policy will always be used in a way that is consistent and compliant with the General Data Protection Regulation, the UK Information Commissioner’s Office (ICO) Employment Practices Code and the Human Rights Act and any other relevant legislation in place.

[Name of employer] guarantees the privacy of emails sent to and from designated trade union e-mail addresses, and phone calls to and from designated trade union telephones numbers.

Review and monitoring

[Name of employer] will ensure that all new staff members, supervisors and managers will receive induction training on the policy.

Adequate resources will be made available to fulfil the aims of this policy. The policy will be widely promoted, and copies will be freely available and displayed in [name of employer]’s offices and through the staff intranet [amend as appropriate to your workplace].

This policy will be reviewed jointly by unions and management, on a regular basis.

Further information

Information Commissioner's Office (ICO) [www.ico.org.uk]

Signatories

This agreement is made between [name of the employer] and UNISON, a registered trade union.

This agreement comes into force on:
DATE:……………………………….. 
This agreement will be reviewed on:

DATE:………………………………..

SIGNED: …………………………… for [name of the employer]

DATE:………………………………..

SIGNED: …………………………… for UNISON

DATE:………………………………..