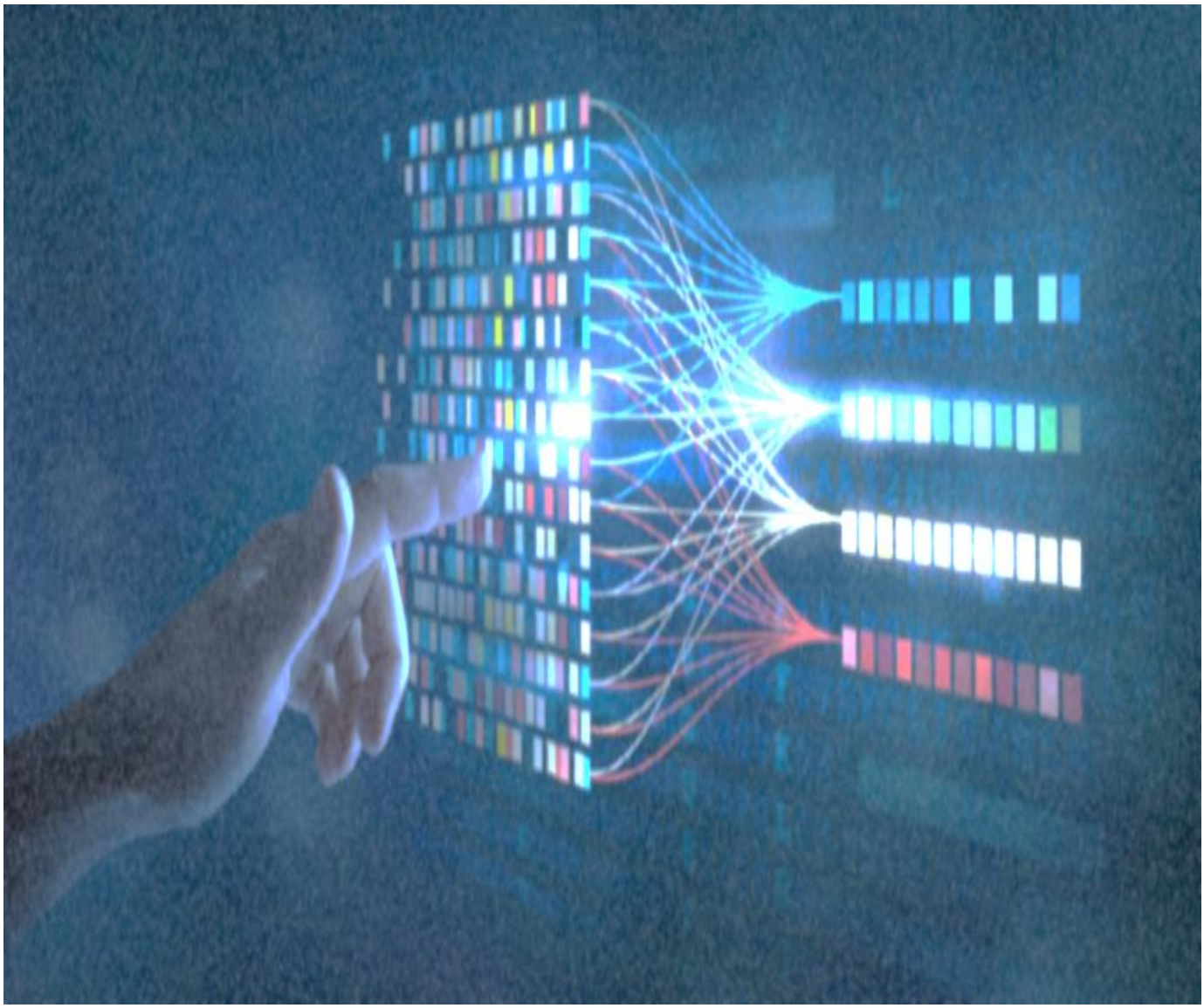
New technology and AI in the workplace

incorporating monitoring and surveillance, and automation guidance

UNISON Bargaining Support Group

UNISON
the public service union



Contents

If negotiators have any comments on this guidance or any experience of negotiations that could be usefully incorporated in the guidance, please contact Bargaining Support at bsg@unison.co.uk

Further guidance is available from bargaining support for branches and workplace reps www.unison.org.uk/bargaining

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

1. Why branches need to negotiate on the use of new technology in the workplace

We live in a technological age. And every day seems to bring some new innovation aiming to make life smarter and easier.

The introduction of new technology in the workplace can help to improve work for staff and make it fairer, safer, faster, less monotonous, more productive.

But new technology in the workplace may put some jobs at risk. It may require many workers to retrain and learn new skills. It's important that this is recognised and action is ongoing so that workers are always prepared and ready.

Headline findings from the 2023 study 'What drives UK firms to adopt AI and robotics, and what are the consequences for jobs?' (part of the Pissarides Review) show an overall picture of around **80% of UK firms having adopted AI, robotic or automated equipment in the past three years, with a similar proportion for physical or cognitive tasks.**

KPMG in their June 2023 report 'Generative AI and the UK labour market' suggest that the adoption of generative artificial intelligence (AI) could add 1.2% to the level of UK productivity, or, in terms of 2022 level of GDP, £31 billion additional output in the UK per year. Overall, they estimate that 40% of jobs are expected to see some impact from the technology.

Whilst some sectors may have expanded as a result of technological innovation, others have found that new technology has replaced labour.

Research by Goldman Sachs suggests that **artificial intelligence could replace the equivalent of 300 million full-time jobs.** Overall, AI could take over around a fifth of all jobs globally.

But too often, reps and branches are left feeling powerless through ignorance.

A January 2024 report from Wales TUC 'A snapshot of workers in Wales' understanding and experience of AI' highlights how "trade unionists reported that they are generally not yet sufficiently empowered with accessible, contextualised, and detailed information to understand these specific forms and effects of AI they encounter. This is a barrier to an effective response by trade unionists.

This is compounded by widespread frustration with the limited means and tools workers have at their disposal to ensure that the AI and digitalisation transition is fair and worker-centric."

Employers expect new technology to increase their productivity and profits. But workers too should be able to share in the benefits of new technology and be assured that their interests are protected.

The TUC has called for a number of protections to be enshrined in UK law including:

- A legal duty on employers to consult trade unions on the use of "high risk" and intrusive forms of AI in the workplace.
- A legal right for all workers to have a human review of decisions made by AI systems so they can challenge decisions that are unfair and discriminatory.
- Amendments to the UK General Data Protection Regulation and Equality Act to guard against discriminatory algorithms.

The TUC also launched an AI taskforce bringing together leading specialists in law, technology, politics, HR and the voluntary sector. Its chief mission is to fill the current gaps in UK employment law by drafting new legal protections to ensure AI is regulated fairly at work for the benefit of employees and employers.

The taskforce aims to publish an expert-drafted AI and Employment Bill early in 2024 and will lobby to have it incorporated into UK law.

An impact on personal privacy and management decisions

The introduction of new technology at work is often made without a clear and reasoned justification provided by the employer. Sometimes the justification given is disproportionate to any need. And too often new technology is introduced in the workplace by employers outside of any collective bargaining process.

The increasing use of new technologies and digitisation – such as the use of artificial intelligence (AI), algorithms and biometrics – often results in a surreptitious collection of personal data. More employers are now able to carry out routine but not obvious checks on their workers through the monitoring of their emails, phone calls and computer use, or using CCTV and other forms of technology to keep a covert eye on staff activities.

Some employers have introduced the use of devices such as body-worn cameras or dash cams, ostensibly to protect the health and safety of employees and deter assaults. But there may be fears that the information accumulated by employers from such equipment can be misused. And branches are reporting that more of this monitoring evidence is being used in disciplinary cases.

All these concerns may impact on the health and wellbeing of staff, not least because the new technology may increase the intensity of work and replace human decision-making with automated instructions and evaluations.

The TUC's November 2020 report 'Technology managing people: the worker experience' found that

- 1 in 7 (15%) say that monitoring and surveillance at work has increased since Covid-19

- 6 in 10 (60%) say that unless carefully regulated, using technology to make decisions about people at work could increase unfair treatment in the workplace
- fewer than 1 in 3 (31%) say they are consulted when any new forms of technology are introduced
- more than half of workers (56%) say introducing new technologies to monitor the workplace damages trust between workers and employers.

The report also notes that

- Some employers have deployed new monitoring technologies as a result of the increase in homeworking created by the COVID-19 pandemic.
- There is a perception that these new technologies are being used in an intrusive way which goes well beyond the type of monitoring that employees would experience in their usual working environments.
- There is a strong feeling, from workers and union representatives alike, that technology is being deployed without their full knowledge or understanding.
- There are concerns that AI-powered solutions can be flawed. For example automated absence-management systems were highlighted, which had wrongly concluded that employees were improperly absent from work leading to performance processes being incorrectly triggered.
- Workers and employees had experienced poor mental health due to perceived unfairness driven by AI-powered technology.
- Trade union representatives perceive that managers often do not understand AI-powered technology and perceive it to be unimpeachable.

An impact on job security

Technological tools will inevitably have a lasting impact on the future of work, making certain jobs obsolete, or deciding on how some jobs should be carried out without valuing the skills of the individual.

Estimates of the proportion of UK jobs that can be feasibly automated vary widely from 10% to 44%, though it is generally recognised that it is much more common for a part of a job to face automation than a job in its entirety.

The think tank, Future Advocacy in their 2020 report 'Automation and Britain's new political landscape' predicts that 8 million jobs in Britain are at risk of automation by the early 2030s.

One example is at Derby City Council who announced in February 2024, the use of AI technology in local government having signed a £7 million contract with developers to deliver the next stage of its project. Staff working in three service areas will soon be using 'AI copilots' to help them carry out their jobs more effectively. By using AI to take on routine tasks, the Council say they will be

enhancing their own skills and freeing up more time to concentrate on the activities and tasks that provide real value to those most in need of support. They will also use AI software to quickly generate information to help them make informed decisions.

However, as Computing magazine reports, a recent Freedom of Information (FOI) request disclosed that two full-time equivalent positions had been eliminated in the customer management department.

Studies suggest that low-paid jobs are five times more likely to include potentially automated work than high-paid jobs. This tendency to hit low-paid work harder means that automation also carries a greater threat to certain parts of the workforce.

In terms of geography, studies have shown that the North East and Northern Ireland are more vulnerable than London and the South East. Similarly, the disproportionate number of women, Black and disabled workers amongst the low-paid, increases the risks that they face. And occupations in transport, retail and admin are among the most exposed sections of the service sector.

The Equality and Human Rights Commission's August 2023 'Future of Work' report found that "the further expansion of alternative forms of employment or automation could exaggerate pre-existing inequalities in the labour market. Moreover, AI could perpetuate biases and discrimination on the basis of sex and ethnicity in workplace practices, resulting in risks of human rights being infringed…

Employment in jobs at high risk of automation has increased by 17% for 50 to 69-year-olds since 2009." This increase was also identified for disabled workers and Black workers.

Many employers will also prioritise cutting costs without regard for the consequences amongst staff or service users from the introduction of new technology.

Transparency from the employer and early consultation with unions is therefore key to safe and trusted use of new technologies in the workplace.

The need for new technology agreements

If good practice technology policies are agreed, the number of cases requiring steward representation may be reduced, freeing up steward time.

Negotiations will also highlight how UNISON values its members and recognises the need for consultation when new technology is introduced, which could result in an increase of your branch's activist base.

In addition, 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.

Organising staff increases bargaining strength

Organising staff around the need for a workplace agreement on new technology will increase bargaining strength over any proposals from the employer.

The introduction of new technological tools and automation can be a strong mobilising issue that draws on well-founded concerns about job security and privacy, the changing nature of job roles and heightened pressures on the workforce.

Every bargaining aim must be seen as an organising opportunity, to build the union and achieve better bargaining outcomes.

The UNISON 5 Phase Plan to Win sets out the 5 phases of successful strategic organising campaigns to support a bargaining aim:

1. Research and development
2. Union base building
3. Launch issue-based campaign
4. Resolve the issue (and go to 5) or escalate and create a crisis (for the employer or ultimate decision maker).
5. Win, celebrate, review and sustain

Ideally, bargaining goals can be achieved without the need to escalate campaigns to dispute. Where there is member support for escalation to deal with employer intransigence, further advice must be sought from the regional centre.

Further detail is outlined in the **5 Phase Plan to Win guide and template**, which is available as one of the resources of the Organising to Win series.

UNISON activists can access the resources via the Organising Space – UNISON's online space for activists. Visit the Organising to Win tile at OrganisingSpace.unison.co.uk or contact your Regional Organiser for guidance and support.

UNISON staff can access the resources via the Organising to Win page on Pearl and can contact the National Strategic Organising Unit for guidance and support.

Had an organising win? Let's learn the lessons and celebrate! Send a summary to WIN@unison.org.uk and we'll be in touch.

Starting a conversation about new technology in the workplace

Employers may have many legitimate reasons for using technology in the workplace, not least for the protection of staff.

For example, 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. New technology may help to achieve this.

But, as the UNISON health and safety leaflet on **Lone Working** (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.”

For any new technological practices to be successful, employers should first consult with workers and give clear reasons for their introduction. And these reasons should be legitimate and in proportion to the need.

QUICK CHECKLIST

- ☐ Undertake a mapping exercise of how digital management systems are used in the workplace. What is being used, for what purposes and where? What information have workers received and what is their experience of the technology? Who is responsible for procuring, deploying and using the technology? What data is being collected? How is it stored and used?
- ☐ Find opportunities to ask the employer how they plan to invest in new technology and AI.
- ☐ Ask them to give clear reasons for their plans – are they legitimate and in proportion to the need?
- ☐ Encourage the employer to set up a joint negotiating committee specifically set up to look at the consequences of the introduction of new technology and AI within the workplace and to allow meaningful consultation. Do existing policies and agreements sufficiently cover the use of new technology?
- ☐ Will the employer agree to bring proposals to introduce new technology to this committee when the proposals are still at a formative stage to enable employees to input into the shaping of proposals and design of systems?
- ☐ Ask the employer to be clear about which managers are accountable and responsible for any new technological systems and what the oversight mechanism will be.
- ☐ Ask that information is shared in accordance with the Acas code of conduct on Disclosure of Information to Trade Unions for Collective Bargaining Purposes as a minimum.
- ☐ Get informed about what technology and AI can do. Reps and branches need to be able to identify the technology being used in the workplace, that could have a significant impact on workers' terms and conditions. What does the technology do; how will it work; what are the potential risks and harms?
- ☐ Do you have the right training and skills to identify issues and represent members' interests? If not, seek this out. A good starting point is the TUC online interactive training TUC's interactive learning for union reps **'Managed by Artificial Intelligence'** www.tuc.org.uk/resource/managed-artificial-intelligence

2. Why should employers develop an agreement with the trade union?

An agreement with the trade union increases the chances of resolving workers' concerns about the introduction of new technological tools, whilst ensuring minimum disruption to services.

Other benefits to the employer:

To keep within the law

As the AI Law Consultancy point out in their 2021 paper for the TUC 'Technology Managing People – the legal implications', "the legislative measures that have been added to define better the legal rights of employers and their employees and workers have not been altered just because new technology is being deployed."

Because a machine or an algorithm or some other form of new technology collects information and makes a decision on behalf of the employer, it does not mean that the employer is not ultimately responsible for that decision.

"For instance" the AI Law Consultancy state, "the employer's statutory obligation to act fairly in terms of process and outcome when dismissing employees with over two years' continuous service remains. It is not watered down in any way just because business has utilised new ways for human resource management."

Other areas of employer responsibility covered by legislation, including health and safety and equality, are not reduced by the use of new technology. Employers must still act fairly in process and outcome. They have a duty to protect the health and safety and welfare of their staff, and an implied duty to maintain trust and confidence as part of the employment contract.

Employers must also fully consider and comply with the **UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and Article 8 of the European Convention on Human Rights.** Other legislation may also be relevant – further details in APPENDIX ONE.

It is also worth pointing out to employers that under the old Data Protection Act, they just had to comply with the law. Under the UK 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.

There are a few places that branches and representatives can look to check on their employer's data protection practices. Employers should have an **employee privacy policy and a data protection policy** that outline what data is collected and why it is collected, as well as their lawful justification for it.

If an employer is processing what is known as **special category data**, they must have completed a **Data Protection Impact Assessment (DPIA)** beforehand.

Special category data is:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

For example, a DPIA would be required if an employer wishes to add a clocking in system that relies on using the employee's fingerprint. Fingerprints are biometric data and fall under special category data, so a DPIA must be completed.

Special category data also requires additional considerations around the lawful basis under which it is processed. While you can request a copy of the DPIA, there is no obligation for this to be provided.

If you believe that your employer is processing special category data unlawfully, contact the **data protection team at UNISON centre** via dataprotection@unison.co.uk.

It is not just data protection legislation that employers need to be mindful of when introducing new technology especially AI. For example, **equality legislation** will be particularly relevant to ensure that AI output does not show any bias or discrimination, and use of new technology does not result in unequal treatment in the workplace.

The case studies presented in the Equal Rights Trust 'Discriminatory by default?' report show that:

- Discrimination can and does occur at every stage in the development and deployment of algorithmic systems, from inception through to use.
- This discrimination can and does occur in all areas of life where algorithmic systems are deployed, from healthcare to employment, and from social security to social media.
- This discrimination has arisen on myriad grounds, from gender to nationality and from disability to race, affecting communities exposed to discrimination because of different aspects of their status, identity or beliefs…

…An analysis of these examples demonstrates that because of the way in which algorithmic systems are developed and designed, trained and evaluated, deployed and used, they are frequently discriminatory by default. Systems which some still believe are inherently objective and fair in fact reinforce existing patterns of discrimination, reflect stereotypical assumptions and replicate bias.

Other legislation may also be relevant such as **copyright law**, for example, if AI chatbots are used in the workplace without consideration of any potential copyright infringement in the information they produce.

The TUC believes there should be a new set of legal reforms for the ethical use of AI at work including:

- A legal duty on employers to consult trade unions on the use of 'high risk' and intrusive forms of AI in the workplace.
- A legal right for all workers to have a human review of decisions made by AI systems so they can challenge decisions that are unfair and discriminatory.
- Amendments to the UK General Data Protection Regulation (UK GDPR) and Equality Act to guard against discriminatory algorithms.
- A legal right to 'switch off' from work so workers can create 'communication free' time in their lives.

To avoid an adverse impact on your workers

The myriad of new technological tools now available for employers to use in the workplace, particularly those that involve monitoring and surveillance of staff, may have unexpected negative consequences on workers that could have a knock-on effect on service delivery.

For example, as the Information Commissioner's Office guidance on 'Data protection and monitoring workers' warns that: "Excessive monitoring can have an adverse impact on the data protection rights and freedoms of workers.

Excessive monitoring is likely to intrude into workers' private lives and undermine their privacy and mental wellbeing. It is not always easy to distinguish between workplace and private information, especially when workers are based at home. Some workers may also use personal devices for work.

Monitoring communications between a worker and their union representative or capturing a worker's personal correspondence both give rise to significant concerns."

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.

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.

Research

2011 research ('Employee perception towards electronic monitoring at work place…' 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.

The TUC's report on workplace monitoring 'I'll be watching you' (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 employer.... Only a quarter (25%) feel that surveillance will have more benefits for workers than downsides."

Employers need to be reminded that it is impossible to completely stop the private lives of workers from extending into the workplace.

Therefore the use of many technological tools will inevitably mean that information that is confidential, private or sensitive (not only to the individual but also perhaps to the business) is seen or collected by those who do not have a business need to know, such as IT workers involved in monitoring emails.

In addition, the use of artificial intelligence in performance management can have a negative effect on worker mental health, increasing the stress and pressure put on workers and leaving them feel powerless.

To let staff get on with their work

Technological systems, particularly those that involve excessive monitoring and surveillance may 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), time that would be better 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.

Because it's expensive

We all know that money is tight in the public sector and highly sophisticated, new technological 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?

In addition, employers need to be mindful of an individual's right to see the data that their employer holds on them under the right to subject access within the UK General Data Protection Regulation. This includes biometric data and health testing information.

More information:

UNISON's **Data protection issues for negotiators: requesting data from employers** www.unison.org.uk/data-protection-issues-for-negotiators-requesting-data-from-employers/

The employer cannot normally charge a fee to fulfil such a request for access to the data held by them, and usually has a month to respond, although in complex cases, this can be extended to three months.

Potentially faced with numerous requests from suspicious, concerned or disgruntled employees could produce a time-consuming and costly exercise for any employers who do not fully consult on proposed new technological tools in advance.

QUICK CHECKLIST

- ☐ Will the introduction of the new technology impact on service users? This could provide a key campaigning opportunity for the union to join force with organisations representing service users or gather support direct from service users such as through petitions. Where the preferences of service users align with staff, demonstrating the opposition of service users can present employers with a much more difficult task to justify their proposals – more information in UNISON's guidance, Effective Campaigning.
- ☐ Encourage the employer to develop a new technology policy that will involve the trade union in key decisions about the introduction, development and use of technology, including how they are experienced and change over time, and identifying options and adjustments for improvement – a model new technology in the workplace policy is available below.
- ☐ Has the employer considered how any third-party developers of new technology produced the algorithms etc used by them? Has the employer taken account of who would be responsible for any data protection, employment law, human rights, equality and employment contract breaches with the introduction of any new technology? Would they be able to identify these breaches?
- ☐ Make sure the union is involved in discussions early in considerations of new technology - in the design, procurement, trial, implementation, review and maintenance.
- ☐ It is important to get the employer to agree in principle that adjustments will be made to any new technology used in the workplace if risks or harms are identified, such as retraining an algorithmic system or adjusting the factors it considers.

3. Key issues for consultation

The key concerns for negotiations with employers about the introduction of new technology are **transparency and consent**.

Any new technological tool should be carefully considered as to how intrusive it is on the individual and their privacy. If it involves any monitoring or surveillance in the workplace, it is imperative that it should be proportionate and necessary.

Research
Workers and trade union reps responding to TUC surveys (as reported in the TUC's November 2020 report 'Technology managing people: the worker experience') wanted employers to be more transparent about the technologies being used in the workplace, and how they work.

Without this transparency, workers and union reps feared they would be unable to understand or challenge decisions made about them by artificial intelligence.

As important as knowing and understanding the new technology being used in the workplace, it is crucial that employees can freely agree to its use before it is implemented.

Ideally there should be an agreed mechanism in place, whereby union reps and the employer can discuss any proposed introduction of new technological tools, such as a specific joint negotiating committee looking at new technology, and an agreed policy and procedure to consult and communicate.

UNISON case study
(as listed in the **Wales TUC's 'Negotiating automation and new technology')**

Scottish housing company, Wheatley Group, introduced new caseload software for housing officers, replacing the need to fill in paperwork on site with the use of iPads. Although the technology was generally seen as an improvement, there were also many challenges with it, particularly around features it lacked and the changes to working practices.

UNISON rep, Paul Stuart was able to feedback on these issues, and suggest further processes that the workers would like to see automated in the future through the union/employer consultative committee.

To be successful, trade union reps involved need to be properly trained to ensure they have all the necessary understanding of the technology and its potential impact on workers.

More information:

TUC's **Dignity at work and the AI revolution: a TUC manifesto**
www.tuc.org.uk/research-analysis/reports/dignity-work-and-ai-revolution
In this manifesto, the TUC highlight the values we should all adopt to make sure that technology at work is for the benefit of everyone, and to reassert the importance of human agency in the face of technological control.

TUC's guidance, '**When AI is the boss: an introduction for union reps'**
www.tuc.org.uk/resource/when-ai-boss
This guide sets outs how AI systems work, what the implications are for workers and unions, and some of the solutions unions can provide.

Wales TUC's **'Negotiating automation and new technology'**
www.tuc.org.uk/research-analysis/reports/negotiating-automation-and-new-technology
Looking at how new technology is reshaping work in positive and negative ways, reviewing any existing agreements, and areas to consider for negotiations.

TUC's interactive learning for union reps **'Managed by Artificial Intelligence'**
www.tuc.org.uk/resource/managed-artificial-intelligence
For union reps and members who want to know about the impact that artificial intelligence is having in the workplace and who would like to support unions in negotiating agreements on this issue.

Institute for the Future of Work's **'Understanding AI at work'**
www.ifow.org/toolkit/ai-at-work
A toolkit for employers and workers seeking to understand the challenges and opportunities of using algorithmic systems that make or inform decisions about workers.

Equality and Human Rights Commission's **'Artificial intelligence in public services'**
www.equalityhumanrights.com/guidance/artificial-intelligence-public-services
A guide providing an overview of what artificial intelligence is, how the Public Sector Equality Duty applies when a public body uses artificial intelligence along with a checklist for public bodies in England (and non-devolved and cross-border public bodies).

Information Commissioner's Office 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.

UNISON's **Data protection issues for negotiators: requesting data from employers**
www.unison.org.uk/data-protection-issues-for-negotiators-requesting-data-from-employers/
Includes information about requesting personal data through subject access requests. Every individual has rights as a 'data subject' including a right to access the personal data that an organisation holds on them under the UK GDPR.

The Why Not Lab – aims to equip workers and their unions with the right skills, know-how and know-what to ensure collective rights in the digital age; puts workers' interests centre stage in current and future digital policies
www.thewhynotlab.com/

Public Services International (PSI) as part of their project **'Our Digital Future'** has online training courses available covering the following key topics:

1. What's all this about data and artificial intelligence?
2. How is digitalisation changing public services and jobs?
3. What rights do workers' have to data and A.I and what needs improving/changing?
4. To limit bias, discrimination and opaque decision-making, unions must demand a seat at the table regarding the governance of algorithmic systems. What should this model look like? What needs to be tabled?
5. How do we use collective bargaining to protect and develop our digital rights?
6. How can unions support one another within and across regions to avoid duplication, support the sharing of best/bad practices and help one another to leapfrog into a strong, sustainable digital path?
7. What coalitions should unions build/participate in to anticipate and limit the negative effects on public services and workers and to become leading actors pushing for the development of progressive governance and pro-public policies of digital technologies?

Courses are currently available for Digital Rights Organisers and Union Leaders. Further training is being developed for shop stewards and union secretariat.
Digitalisation Training - North America, Europe, Caribbean - PSI - The global union federation of workers in public services

QUICK CHECKLIST

- ☐ What new technology and digital systems that affect workers and their working conditions are being used by the employer, and why?
- ☐ Who designed and owns these systems? Who are the developers and vendors and how does their contract with the employer cover data access and control, as well as system monitoring, maintenance, and redesign?
- ☐ Which managers oversee and are responsible for the systems? What mechanisms do they have in place should the systems fail, harm workers or be poorly governed?
- ☐ Consult members and highlight the particular impact the introduction of new technology could have in your workplace.
- ☐ Survey all staff. This could not only provide necessary feedback for the employer, but be a useful recruitment tool for UNISON. Employers may not understand what the strength of feeling is on the issue, for example concerning the storage of personal data collected from CCTV, biometric monitoring and other tracking devices and smart phone apps.
- ☐ The branch could organise meetings and report the findings of the survey back to the members, and to the employer perhaps in the form of a collective letter.
- ☐ What other mechanisms do staff have to challenge actions and decisions taken by management based on algorithms?

4. Impact and risk assessments required

To safeguard workers, it is important that employers agree to undertake various impact assessments to identify potential risks and negative impact when introducing new technology into the workplace.

The assessments should also help identify the action necessary to reduce or remove the risks.

The CIPD asked over 800 employers in 2022 to choose their top three ways for ensuring AI is used responsibly at work.

Requiring employers to conduct impact assessments before and after implementing AI is seen as important as introducing regulation to ensure AI is trustworthy. This is closely followed by requiring vendors to demonstrate that the AI in their software is trustworthy.

The Institute for the Future of Work has developed a specific **Good Work Algorithmic Impact Assessment**, designed to help employers and engineers to involve workers and their representatives in the design, development and deployment of algorithmic systems so that risks are anticipated and managed, 'good work' is promoted, the law is complied with, innovative approaches are unlocked and trust in technology is built.
www.ifow.org/publications/good-work-algorithmic-impact-assessment-an-approach-for-worker-involvement

Equality impact assessments

An equality impact assessment (EIA) is a tool organisations and employers use to make sure they promote equality in policies, practices and services. They help organisations check and record how they have made the best decisions, based on robust evidence. They help make sure that a change or decision does not have an unintended negative impact on particular groups of people.

Equality impact assessments address two key questions:

1. How effective will this initiative be in promoting equality?
2. Could it affect different equality groups in different ways?

Equality groups are set out in the Equality Act[1] as nine ‘protected characteristics’:

- age

[1] In Northern Ireland the relevant legislation includes: the Disability Discrimination Act (DDA) 1995 and subsequent amendments and supplementary laws, Employment Equality (Age) Regulations (NI) 2006 and subsequent amendments, Equal Pay Act (NI) 1970, Sex Discrimination (NI) Order 1976 and subsequent amendments, Maternity and Parental Leave etc. Regulations (NI) 1999, Race Relations

- disability (a disabled person being defined as someone who has a mental or physical impairment that has a substantial and long-term adverse effect on the person's ability to carry out normal day-to-day activities)
- gender reassignment (covering all people considering or undergoing or who have undergone gender reassignment whether or not they have medical treatment)
- marriage or civil partnership
- pregnancy and maternity
- race (including colour, nationality, and ethnic or national origins)
- religion or belief
- sex
- sexual orientation.

The EIA process involves gathering information and consulting people – workers, service users or members of the public who will, or could, be affected by an initiative in order to answer the key questions.

Further information:
UNISON's model equality impact assessment flowchart www.unison.org.uk/unison-eia-guidance-and-flowchart-jan-2022/

Health and safety risk assessments

Risk assessments are part of the risk management process and are included in the Management of Health and Safety at Work Regulations.

A risk assessment is the process of identifying what hazards currently exist or may appear in the workplace. A risk assessment defines which workplace hazards are likely to cause harm to employees and visitors.

By law, every employer must conduct risk assessments on the work their employees do. If the company or organisation employs more than five employees, then the results should be recorded with details of any groups of employees particularly at risk such as older, younger, pregnant or disabled employees.

Further information:
UNISON risk assessment guidance
www.unison.org.uk/content/uploads/2022/02/26694_Risk_assessment_guidance_update_Feb22.pdf

Data protection impact assessments

A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

A DPIA must be carried out when processing involves **special category data**. Special category data is:

- personal data revealing ethnic or racial origin
- personal data revealing to political opinion
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation.

The DPIA must:

- describe the nature, scope, context and purposes of the processing of personal data
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

Further information:

Data protection impact assessments guidance from the ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

'Guidance on AI and data protection' from the ICO including an '**AI and data protection risk toolkit'**, designed to provide further practical support to organisations auditing the compliance of their own AI systems. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/

QUICK CHECKLIST

Equality and fairness

- ☐ When introducing new technology into the workplace, has the employer properly considered the requirements of equality legislation, and relevant workplace policies on equality and diversity? Has the employer carried out an equality impact assessment?
- ☐ Ask for pilots or trials of the proposed changes and ask for the union to be involved in reviews.
- ☐ How does the employer control for and monitor possible worker harms in new systems e.g. health and safety, discrimination and bias, work intensification, deskilling?
- ☐ Are workers fully aware when AI is being used to make important decisions about them? Does the employer ask for their consent beforehand?
- ☐ Do any targets set by technological tools take full account of individual needs, such as the need for toilet breaks and rest periods? And reasonable adjustments?
- ☐ Are staff members and their union reps able to challenge any decisions made by AI? Do they sufficiently understand how the technology operates and can they access appropriate information?
- ☐ Encourage the employer to publish an AI explainability statement. **AI Explainability Statements** explain in a non-technical way how the AI used by the organisation works. The aim is to provide transparency, comply with legal requirements, best practice and AI ethical principles, in order to keep the trust of the public. Further information covering one example of an AI Explainability Statement that has been reviewed by the ICO: www.livehealthily.com/press/releases/explainability-statement
- ☐ Raise awareness of equality issues including any potential discrimination or negative impact on groups with protected characteristics resulting from use of new technology tools amongst staff. This could provide a valuable recruitment and organising focus for a workplace.

Health and safety and data protection

- ☐ When introducing new technology into the workplace, has the employer carried out a health and safety risk assessment to consider impact on workers' wellbeing and working conditions?
- ☐ Has the employer properly considered the requirements of UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and relevant workplace policies on data protection and health and safety?
- ☐ Has the employer carried out a data impact assessment? Will they inform and involve union reps, including when it is reviewed?

- ☐ Ask the employer to follow the **ICO guidance on Data protection impact assessments (DPIAs)** https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- ☐ If data is being collected, do the benefits really outweigh the potential costs or consequences if the data security and confidentiality is breached?
- ☐ Is the employer clear about what personal information is collected from staff members, why this information is needed and how it will be used? Could the process mean that additional personal data that is not required by the employer is also collected?
- ☐ How can the employer be certain that the data held is accurate and up-to-date?
- ☐ Does the employer have a data retention policy?
- ☐ Is the employer clear about how the personal information is stored and that it is kept secure?
- ☐ Is the employer clear about how long the personal information is kept and how it is safely destroyed?
- ☐ Is the data shared unnecessarily?
- ☐ Raise awareness of data protection issues and individual privacy rights amongst staff. Highlight the potential impact of new technological tools or automation on jobs and roles. This could provide a valuable recruitment and organising focus for a workplace.
- ☐ Raise awareness of health and safety issues including the risks of work-related stress and an ‘always on’ culture amongst staff. This could provide a valuable recruitment and organising focus for a workplace.

5. How new technology is being used in the workplace and some of the issues to look out for

The impact of new technology can spin off into almost every aspect of an employee's terms and conditions. For example, it can significantly change the requirements of a job role, shift an employer's capacity to monitor work and control workloads, facilitate 'crowd-work' platforms that change the type of contracts offered, increase remote working or create pressures that intrude deeper into a worker's personal life.

The TUC's November 2020 report 'Technology managing people: the worker experience' lists some examples of how artificial intelligence (AI) is currently being used:

- AI-powered **management practices** are well established in platform-based gig economy work, where algorithms operate to match worker to work, monitor activities, allocate ratings and impose reward or disciplinary measures.
- AI-powered tools are being used at **all stages of the recruitment process**, ranging from sourcing candidates, to screening, interviewing candidates and the formation of job offers based on a predictive model.
- People are not only being recruited by AI, they are being **line-managed** by AI as well with technology making or informing decisions on a variety of issues at work such as absence management, work allocation, timetabling of shifts and time off, ranking of workers (often using points or stars), goal setting and performance assessment.
- AI-powered tools are also being used to undertake analysis of **team dynamics**, personality analysis and coaching and restructuring of teams.
- **Gamified online training** (the use of gaming mechanics and experience, often by way of a simulation) with assessed outcomes is also increasing, replacing face-to-face training.

Using new technology for the management of staff and service delivery

Management tools

As the TUC suggest in their guidance, "When AI is the boss: an introduction for union reps": "Think of all the functions of a manager. There is probably an AI-powered tool on the market for almost every function you list."

This could include using technological tools to:

- Decide who gets access to work on an online platform and scheduling of shifts

- Monitor performance and productivity, such as through keyboard activity, logged time taken to complete tasks or time at work, allocating grades/ratings for performance
- Allocate tasks, deciding on teams and dictating how and when work is completed
- Trigger disciplinary and capability procedures
- Terminate employment – dismissal, making a redundancy selection, withdrawing access to a platform or app.

The use of such tools may also lead to a higher intensity of work. The performance of workers may be tracked against unrealistic expectations that then feed into performance related pay systems. Unsurprisingly, as a consequence service delivery may also be affected detrimentally.

Monitoring workers' activity

The TUC's 2018 report on workplace monitoring 'I'll be watching you' (www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you) found that the most common types of workplace surveillance include monitoring work emails, files and work computer browsing history, CCTV, phone log and calls, including the recording of calls, handheld or wearable location-tracking devices.

The shift to more homeworking or hybrid working has led to a greater use of digital platforms such as Microsoft Teams, Zoom and Slack accounts, and WhatsApp groups that can all be analysed for activity.

AI may be using facial recognition to track attendance, keyboard strokes to monitor computer use, seat or desk sensors to check when workers are at their desk, screening of internet and email use to check on communications, analysis of workers' expressions and tone of voice to monitor behaviour, analysis of time spent to complete tasks to rate performance.

The TUC also warn that "AI might even be used by employers to monitor union activity and put together a union profile. For example, AI might be used to analyse information such as the location of union offices, the activity of union officials, the use of union-related vocabulary in emails, and even union activity on social media."

Research commissioned by the Information Commissioner's Office (ICO) in August 2023 revealed that almost one in five (19%) people believe that they have been monitored by an employer. Over two thirds (70%) of people surveyed by the ICO said they would find monitoring in the workplace intrusive and fewer than one in five (19%) people would feel comfortable taking a new job if they knew that their employer would be monitoring them.

ICO has guidance for employers on monitoring workers lawfully, transparently and fairly and reminds them that any monitoring must be fully compliant with data

protection law.

More information in 'Employment practices and data protection: monitoring workers' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/

So-called 'decision-making' tools

Employers may be using automated (or semi-automated) decision-making tools, people analytics or innovative monitoring or surveillance tools to assess, predict and check on workers. However, they may not realise that they may have a detrimental impact on certain groups of workers and that decisions made using technology are not neutral or unbiased.

"Technology and algorithms do not 'make decisions': they process and use data that was pre-selected by human beings in ways devised by human beings, for purposes determined by human beings.

Human choices about how to build and use data-driven technologies are never neutral. Nor are the outputs of these technologies 'objective' or impartial."

From 'Mind the Gap: the Final Report of the Equality Task Force', Institute for the Future of Work

Automation and restructures

Many proposals for automation are likely to involve the restructuring of job roles. Therefore, an agreement on the use of automation should clearly define any anticipated consequences for job roles.

There needs to be a fair procedure agreed for deciding the allocation of staff to these roles, as with any restructuring exercise.

Where job roles are to change, union reps and branches may recognise there is a benefit of relieving staff of repetitive tasks with the use of new technology. But at the same time, the employer should be encouraged to commit to resourcing training where necessary to expand job roles in other ways, whilst guarding against attempts to establish more demanding roles without the appropriate payment in line with job evaluation.

It's key that unions work with employers to ensure they provide training for employees to ensure that they are properly equipped with the skills needed to fill shifting job roles.

The Wales Union Learning Fund (WULF) has helped establish many hundreds of joint union/employer workplace learning programmes in almost every industry all over Wales… Many unions have already developed programmes through WULF that address retraining for workers whose jobs are under threat, either from decarbonisation or automation.

The amount of funding available to a workplace via WULF is never going to be

enough to address the level of need for skills transition in Wales, but it does allow unions to bring something to table when raising the issue of skills transition.

Wales TUC's 'Negotiating automation and new technology'

Any proposal that suggests a cut in the number of jobs is clearly the biggest worry for staff. Therefore, it is crucial that any new technology policy or automation agreement also carries the maximum level of protections for staff in allowing for redeployment and exploring all options before any redundancies are proposed.

If it can be achieved, a no compulsory redundancy agreement is obviously the most preferable arrangement.

AI and service delivery

Whilst some industries are increasingly using AI and robots to replace certain areas of work, some employers are embracing innovative technology too swiftly within the workplace.

For example, there are reports that school headteachers are being targeted to invest in new 'robots' to help children participate working with their class at home, but without closer consideration of any potential impact on data protection, health and safety, safeguarding issues etc., nor discussion with reps or workers. These robots are placed in the classroom and the child is at home on their device. The robot has a built-in camera and microphone to transmit the lesson back to the child. From home, the child can control their robot, and interact with the class.

AI can be used to identify the training needs of workers, to deliver the actual training or support that influences the service provided by the worker, such a chatbot providing instructions to a call-centre worker telling them to respond in a certain way to a caller.

Issues for the employer and workers to take account of will be similar to those that should be considered when using surveillance and tracking devices (see below).

QUICK CHECKLIST

- ☐ Identify all the AI systems that the employer use in the workplace. How they are they being used to manage workers?
- ☐ Has the employer notified the workers of the nature and scope of the new technology that is being introduced?
- ☐ Is the reason given for introducing the new technology, valid and reasonable in the circumstances?
- ☐ How much will the new technological system cost? Does it represent good value for money?
- ☐ If automated systems are planned, find out about any anticipated consequences on job roles. Could it result in a restructure?

Data concerns

- ☐ Find out if data collected by digital platforms used by workers is being analysed.
- ☐ Find out how this data is being used by the employer.
- ☐ If used for monitoring or surveillance, could a less intrusive form of monitoring be used?
- ☐ Encourage employers to use ICO guidance to help ensure they fulfil their data protection responsibilities when monitoring workers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers/ When following the guidance, steps taken by the employer include making workers aware of the nature, extent and reasons for monitoring; having a clearly defined purpose and using the least intrusive means to achieve it; having a lawful basis for processing workers data – such as consent or legal obligation; telling workers about any monitoring in a way that is easy to understand; only keeping the information which is relevant to its purpose; carrying out a Data Protection Impact Assessment for any monitoring that is likely to result in a high risk to the rights of workers; and making the personal information collected through monitoring available to workers if they make a Subject Access Request (SAR).
- ☐ If the new technological tool involves artificial intelligence, can the employer provide information on how it was trained, on what data and data sources are being used, which factors or 'variables' have been used to build the tool and how they have been weighted or prioritised, how the tool will be evaluated, what will happen if risks or harms are found?
- ☐ Encourage employers to use ICO guidance to help ensure they fulfil their data protection responsibilities when using AI. The ICO with The Alan Turing Institute has developed guidance **'Explaining decisions made with AI'** aiming to give organisations practical advice to help explain the processes, services and decisions delivered or assisted by AI, to the individuals affected by them

https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/

Restructure concerns

- ☐ Make sure there is a fair restructure process and consultation agreed in advance making full use of re-training and redeployment opportunities. More information in the UNISON bargaining guidance on workforce reorganisation www.unison.org.uk/content/uploads/2021/09/Bargaining-on-workforce-reorganisation-v2.pdf
- ☐ Existing organisational change or redundancy policies or agreements may need to be updated to explicitly take account of the introduction of automation and its potential impact on job roles.
- ☐ Where new technology impacts on job roles, is redundancy considered as the very last resort, and ideally with a principle of no compulsory redundancies agreed?
- ☐ Encourage the employer to commit to training of staff to equip them with skills needed for changing job roles.

The right to ‘switch off’

Much of the research looking at the impact of homeworking on workers during the COVID-19 restrictions, found that the blurred boundaries between their work and home lives, much of it made possible with the use of technological tools, could negatively affect their wellbeing.

The CIPD found that “many organisations haven’t been taking effective action to combat the risks of an ‘always on’ culture during the pandemic. Boundaries between work and home life have become increasingly blurred for many people working from home for example, making it difficult for people to switch off.”

The issue about having a right to ‘switch off’ or ‘disconnect’ is increasingly becoming an urgent one for workers, as new technology means that access to/from work is available anywhere, at any time.

Research

The 2021 CIPD/Simplyhealth Health and Wellbeing at Work survey report found that more than 77% of employers had observed ‘presenteeism’ – people working when unwell – in employees who were working from home. Additionally, 30% of remote workers reported working more unpaid hours than before the pandemic.

70% of employers found ‘leaveism’ – working outside of contracted hours or using annual leave to work – was also an issue.

No wonder then that 5% of remote workers said their work-related mental health had got worse during the pandemic, with 42% saying this was at least partly a result of inability to switch off from work.

The CIPD states that “the findings suggest that many organisations haven’t been taking effective action to combat the risks of an ‘always on’ culture. Boundaries between work and home life have become increasingly blurred for many people working from home for example, making it difficult for people to switch off.”

A report (August 2021) from Autonomy on the right to disconnect, looked at existing research on the prevalence and impact of always being ‘on’ for work. They found that, across a number of studies, “findings show that if workers have a chance to mentally ‘switch off’ from their work, they are generally more productive, engaged on the job and convivial with colleagues. On the other hand, if workers do not have the ability to ‘switch off’ mentally from their work, they are more likely to experience symptoms of exhaustion…”

And because “the vast majority of those who work from home are women [as they are] far more likely to shoulder the additional burdens of childcare, housework and care for elderly family members... women are at greater risk of negative health impacts.”

UNISON’s national young members’ forum, has also highlighted this concern affecting younger workers’ wellbeing and work/life balance. They call for employers

to produce clear guidelines and policies on the right to disconnect when working from home.

A call for a legal right to 'disconnect'

The TUC has called for a statutory right for employees and workers to disconnect from work, to create 'communication-free' time in their lives.

French workers have benefited from a right to disconnect since 2017 when a law was passed to ensure that workers had a right to stop taking work calls or respond to emails outside of their normal working hours. The law was introduced to address the 'always on' culture, whereby the line between work and home life had become increasingly blurred.

Since then Italy, Spain, Ireland, Slovakia and Portugal have introduced the right at least in some form. And EU members are currently negotiating a binding directive that will include the right to disconnect from work-related communications outside working hours.

The aim of the Republic of Ireland's right is to help employees strike a better work/life balance while working from home. The Irish government has introduced a Code of Practice for organisations which includes:

- the right of an employee to not have to routinely perform work outside their normal working hours
- the right not to be penalised for refusing to attend to work matters outside of normal working hours
- the duty to respect another person's right to disconnect (e.g. by not routinely emailing or calling outside normal working hours).

Six in 10 UK workers would support a 'right to disconnect' law, according to research from Ipsos.

QUICK CHECKLIST

- ☐ Have you surveyed members and staff about the pressure they may feel under to be available outside their normal working hours, particularly through the myriad of ways available to communicate using new technology?
- ☐ Are staff, particularly those who work remotely working longer hours? Working when sick? Working when on leave? What sort of impact does it have on their health and wellbeing?
- ☐ Does the employer recognise that the lines between personal life and work can become blurred for homeworkers, not least through the use of virtual meetings that intrude into the home space?
- ☐ Will the employer agree to rules about when staff can and cannot be contacted for work purposes outside of normal working hours? Do staff have a right to switch off and disconnect work from home life?
- ☐ Check out UNISON's **Bargaining guidance on workloads.** It is intended to assist negotiators in making the case to employers for controlling workloads, putting in place the means for assessing workload and taking measures to address excessive workloads www.unison.org.uk/negotiating-workload-agreement-employer/
- ☐ Has the employer carried out a health and safety risk assessment that takes account of work-related stress and the impact of always being 'on' for work?
- ☐ Are all staff expected to get the right breaks and to not work beyond contracted hours?
- ☐ Are all staff expected to properly use their annual leave for rest and relaxation and not to work whilst on leave or use it for sickness absence?
- ☐ Are all staff expected not to work whilst off sick?
- ☐ Is the employer confident that they are not directly or indirectly discriminating against certain groups of workers with protected characteristics, such as those with caring responsibilities (predominantly still women) or disabled workers, because of a long hours work culture? Has the employer carried out an equality impact assessment of working practices?
- ☐ Are managers being trained in any agreed change to the work culture where a 'right to disconnect' is introduced to help ensure successful implementation?
- ☐ Is any agreed change to the work culture communicated clearly to all staff?
- ☐ Are any issues that encourage a long hours work culture such as unmanageable workloads, slow recruitment of replacement staff, or the unreasonable expectations of line managers being properly addressed?
- ☐ Remind employers of the Display Screen Equipment Regulations and the need for regular rest breaks for users of DSE (such as PCs, laptops, tablets

and smartphones) – and this should include taking account of the amount of time spent on focusing on virtual meetings. The common experience often referred to as ‘Zoom fatigue’ is being more widely recognised as often causing stress and exhaustion.

Pre-employment information gathering

Vetting and assessment of job applicants

Before workers start a job, they may be asked for personal details and for references and undergo other pre-employment vetting.

In addition, **employee assessment software** is increasingly being used to assess prospective candidates. For example, CVs or application forms may be **'scraped'** or scanned for keywords to decide who progresses. Employers may used **game-based assessments** to assist in their shortlisting and hiring decisions.

Employers may review job applicants' **digital 'footprints'** such as checking on social media sites for public postings and images, and using this information to screen possible candidates.

Data can be drawn from **psychological profiling**, where people live, their social media use, their personal relationships, and even which web browser they use. Data can also be purchased from third-party data brokers.

The aim is to use the data to create a 'picture' of the candidate and to decide whether they would be a good fit for the organisation. But clearly there are potential issues not only with data protection but with equality legislation should the criteria for assessment not be objective and fully justifiable for the post, and the process transparent.

Although websites like Facebook and Instagram are in the public domain, basing employment decisions on material uncovered on such sites may not only be 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.

Acas recruitment guidance warns employers to "avoid using information that's on someone's social media profile to decide whether you interview or hire them.

You might be breaking the law, particularly if either of the following points apply:

- they did not agree to you using the information in this way
- you looked at some applicants' social media profiles, but not others."

AI and interviews

Particularly with the restrictions over meeting in person during the COVID-19 pandemic, employers' use of AI in the interview process itself has accelerated, with the use of the many commercially available video interviewing platforms.

For examples, recruiters may use 'chatbots' (software that simulates human conversation through voice commands or online text chats or both) to conduct interviews and check if applicants meet defined criteria. Algorithms that analyse

biometric data such as appearance, presentation and voice may score interview candidates.

Research

Job Description Library found that prior to the pandemic only 22% of employers were conducting video interviews whilst by early 2022, this had increased by 57%. Applicants reported many concerns about their experiences of video interviewing, including finding it difficult to build rapport over video, worrying about internet connection dropping out, worrying about being judged on the condition of their home, experiencing technology problems, or being interrupted by someone they live with.

Research from the University of Sussex Business School in 'Artificial Intelligence (AI) in the job interview process' found that candidates reflecting on their experiences of AVIs (asynchronous video interviews in which applicants film themselves answering a predetermined set of questions, with no human interviewer present. The recordings are then evaluated later), expressed discomfort compared to when they were interviewed by people. These included feelings of diminished humanity, believing they had to behave like robots, not knowing how they were going to be assessed, and finding it emotionally and cognitively exhausting.

Technology does not mean neutral and unbiased

AI (artificial intelligence), ADM (automatic decision making) and profiling can discriminate. The decisions made may well be biased, so transparency must be guaranteed.

Employers need to remember that the algorithms used have been trained using a set of decisions made by humans, and some of their biases may creep into the technology. But whereas an interview candidate can ask questions or challenge the decisions made by interviewers, it can be so much harder to do this when the decisions are made by algorithms.

QUICK CHECKLIST

- ☐ Does the employer have a recruitment policy?
- ☐ Does it make appropriate reference to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and relevant workplace policies on data protection and equality?
- ☐ Has the employer carried out a data impact assessment and an equality impact assessment covering recruitment practices? Is the employer clear that the technology supports their equality, diversity and inclusion priorities?
- ☐ If the employer uses a recruitment agency, do they also comply fully with these laws and policies?
- ☐ Do job applicants understand how any technology used works? Is there an opportunity to build genuine relationships during the recruitment process and not to rely too heavily on AI decision-making?
- ☐ Is the recruitment policy clear for applicants, candidates and newly appointed staff members about what personal information is collected and why this information is needed?
- ☐ Is any data to be collected really needed by the employer? Could the process mean that additional personal data that is not required by the employer is also collected?
- ☐ Are job applicants provided with a privacy policy containing information on the purposes for which all the data they provide will be processed and by whom, the legal basis for processing (i.e. legitimately needed for the recruitment exercise) and how long the data will be kept?

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.

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.

Simpkin v The Berkeley Group Holdings plc (2017)
This case went to the High Court of England and Wales. In contrast to the cases above, 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.

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. In that way, they can, for example, make sure there is

an agreement that legitimate emails are not blocked, and that staff are not unnecessarily 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 does not interfere 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.

For an example policy covering use of phone, email and internet within the workplace, including monitoring of usage, see APPENDIX TWO.

Workforce analytics

Workforce analytics, sometimes also called people analytics, is something that employers and their HR departments have also used for some time, particularly in the private sector, but appears to be increasing with the introduction of new technology.

It refers to the process of collecting, analysing and using quantitative and qualitative data about the workforce, alongside business performance data. An example would be collecting data to link a staff pay increase with increased productivity or customer satisfaction.

Although much of the data to be collected may be anonymous, reps and branches should be wary if personal data is included, and that staff are aware of the purpose of data collection and processing, as well as having given consent to its use.

QUICK CHECKLIST

- ☐ Does the employer have a clear policy on the use of the employer's phones and computers and internet for personal use, and are employees made aware of this policy?
- ☐ Does it make appropriate reference to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and fulfil its requirements?
- ☐ Has the employer carried out a data impact assessment?
- ☐ 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 is it fully justified?
- ☐ Is it really necessary to monitor all IT facilities at work or could some areas within the system or through free Wi-Fi be made available for private use?
- ☐ Rather than monitor individuals, can, for example, access be blocked 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?

Workforce analytics

- ☐ Does the employer have a data retention policy?
- ☐ Are staff told what information is recorded and how long it is kept and for what purpose? If data is collected for one reason, but then used for workforce analytics, is this made clear to the workers and is their consent sought to use the data in this way?
- ☐ As far as possible, is data to be used for workforce analytics suitably anonymised, with personal data permanently stripped out, or used in a way that may identify individuals?
- ☐ Is storage sufficiently secure?
- ☐ Are staff who handle the data appropriately trained to ensure they follow data protection procedures?

Surveillance, monitoring and tracking devices

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 wi-fi 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.

The main aim of using 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). They are also used to enhance the security and safety of premises and property.

However, they can also present concerns about privacy and consent from both employees and others whose actions may be recorded. Any details that are recorded would be considered as personal data, so how it is stored, used, collected must be properly considered by the employer.

The **Information Commissioner's Office 'Video surveillance (including guidance for organisations using CCTV)'** provides advice for when employers operate video surveillance systems that view or record individuals.

Surveillance systems specifically include, but are not limited to traditional CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Video (BWV), Drones (UAVs), Facial Recognition Technology (FRT), dashcams and smart doorbell cameras.

Some key points include:

- taking a data protection by design and default approach and performing a Data Protection Impact Assessment (DPIA) for any processing that is likely to result in a high risk to individuals
- establishing who exercises overall control of the personal data being processed
- having appropriate measures and records in place to be able to demonstrate compliance with accountability obligations and data protection principles when using surveillance systems.

Similarly the Surveillance Camera Code of Practice under the Protection of Freedoms Act provides a basis for good practice, although it only applies legally to public authorities.

Employees may be less concerned about the use of most standard monitoring (CCTV) in the workplace if the areas are clearly 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.

Surveillance cameras in care homes

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

Whilst the use of CCTV cameras may have a place as a short-term reassurance measure or to deter or detect abusers, they should never 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 or Zoom 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, can the provider improve their training, vetting and supervision procedures? Can they consider increasing staff numbers and providing trusted ways for staff to raise concerns about standards of care as an alternative to the use of intrusive surveillance cameras?

The **Care Quality Commission (CQC)** has issued **guidance** (www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service) on using surveillance to monitor service.

The CQC state in their guidance "The Regulation of Investigatory Powers Act (RIPA) 2000 sets out the powers public bodies have to use surveillance - and when they can tell or give people permission to use it. For this reason we can't authorise you to carry out 'covert intrusive surveillance'. This means using hidden cameras or other recording equipment in residential areas of your service…

If you use surveillance to help keep people safe or monitor their wellbeing, we treat it as part of their care. This means it must meet the regulations under the Health and Social Care Act.

But any recordings you make of people also count as information about them. Collecting information about people is regulated by the Information Commissioner's Office (ICO)."

As **UNISON's former 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."

Surveillance of homecare staff in private houses

The ICO explains that "personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the GDPR's scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the GDPR."

However, this 'domestic exemption' issue means that there is a gap in the current UK data protection legislation. Unfortunately, the law as it stands does mean that consent for filming in this domestic setting is not necessary, and this can include the covert monitoring of homecare staff when visiting service users.

A potential area for branch or workplace rep negotiations would be to ask employers to include a clause in contracts when providing care services within the home, that employees will not be recorded as a matter of routine, and certainly not without consent. This is additionally important to the service user themselves as the monitoring may impact on their dignity.

Use of smart phone apps

UNISON reps have also reported the increased use of mobile phone apps in particular by social care employers.

But these apps, which are often used to access individual workers' rota details and service users' information, are also covered by the UK General Data Protection Regulations if they include access to personal data (and perhaps not only of the worker, but also of the service user. Therefore, the data needs to be processed lawfully and fairly.

This means that potentially both the worker and the service user would need to have informed consent for use of the apps.

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 phones. 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, which would blur the line between work and their private life.

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 through a grievance with the employer. 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, which went some way to reassuring members.

Case law

In the case of *Alsnih v Al Quds Al-Arabi Publishing & Advertising,* the worker, Ms Alsnih had been dismissed for refusing to use a work app on her personal mobile. However, as well as being found in breach of the Acas code on disciplinary and grievance procedures, the tribunal concluded that the dismissal was also unfair on substantive grounds. The tribunal said that no reasonable employer would:

- dismiss an employee for refusing to put an intrusive work-related app on their personal phone; and
- refuse to pay for a separate phone.

The tribunal highlighted how the employer could simply have provided the worker with a separate phone or installed the app on her laptop in a way that did not interfere with her personal phone.

So called 'early pay' apps

Another example of smartphone apps that reps and branches should make their members wary of, although not necessarily because of a data protection issue, are **early pay apps**. These have been reported to be particularly used in the social care sector.

One example of the app on the market describes itself to the worker as "a mobile app that gives you flexibility in how you take your pay. It's instant access to the pay you have already earned." They also state that any money accessed "is not credit, or a loan or an advance. It is simply the money you have earned so far this month and yours to take if you want it. There is a clear and simple fee to use the service."

The final sentence is the particular issue to bring to the attention of members. The app provider gives people access to their wages earned to date before their pay day. It is paid to them by the app provider and not their employer. The app provider therefore makes their business by charging the worker for the service and not the employer.

Reps and branches should check that members fully read and understand the terms before downloading any app. Workers need to fully understand the implications of accessing part of their wages early through such an app, how this will affect their net salary at the end of the month, and how much extra they will be charged and how this will be deducted from their salary for accessing what they have earned early.

In addition, workers should be fully aware of what personal and financial details and data are being collected and held by the app provider, and properly reassured that it they are following the requirements of UK GDPR.

If possible, reps and branches may consider instead negotiating interest-free loans from the employer or advance payments of salary to workers as a workplace benefit for use in emergency situations. PAYE tax and national insurance would have to be applied to the salary amount when paid in advance, but the employer should not charge any additional fee to the employee. A loan from the employer would not be taxable unless it exceeds £10,000 in the tax year.

Use of other tracking devices

Heat and motion sensor devices to monitor the time workers spend at their desk, **'keyboard-stroke' and other software** used to monitor the worker's computer activity, **audio recording, radio-frequency identification (RFID) tracking** and many other types of tracking systems are also increasingly being used by employers.

An accountancy firm was reported as using staff turnstile data to monitor office attendance to crackdown on suspected breaches of its hybrid working policy, with swipe card entry data circulated among their senior managers to show how frequently staff are attending its offices.

The firm also reportedly updated its staff privacy notice to reflect changes to the "collection and further processing" of card entry data which would allow the employer to oversee "flexible work arrangements, including awareness of … working location".

Some employers have a legal obligation to track business vehicles over 3,500kg or more and **tachographs** need to be fitted.

But 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 driver's 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 when the footage is then also used for performance management.

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.

The Labour Research Department (LRD) reported in December 2023 that "the CWU communications union says data-driven surveillance systems for tech workers include key logging, mouse tracking, screen recording and monitoring internet activity. GPS-enabled tracking devices monitor the location of Royal Mail postal workers and collect data on speed and pace of work.

Telemetry systems in vehicles monitor speed, distance, location and driver behaviour, and an Amazon app sets stretching delivery targets based on times achieved by other drivers."

Like CCTV monitoring, these types of surveillance are covered by the UK General Data Protection Regulations and Data Protection Act 2018. Its use 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. There should be a facility for the employee to switch a button on the device to disable the monitoring.

Even more worryingly, there continue to be news reports that some major UK companies are preparing to **microchip** their employees using the same technology implanted in household pets.

The TUC has 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."

Employees would need to give explicit consent to be microchipped and it is unlikely that it could be made a condition of employment. As with other types of monitoring, employers would have to comply with UK data protection legislation and be transparent with employees about the data collected and how it is used, and be able to show they have a lawful basis to justify the processing and retention of such data.

For an example policy on monitoring and surveillance in the workplace using CCTV, body worn cameras or other tracking devices, see APPENDIX THREE.

Covert monitoring

Covert monitoring is rarely used in the workplace as it is extremely hard for the employer to justify any 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 for the evidence collected during covert surveillance to be used.

Case law has also identified the very limited situations where covert surveillance may be acceptable.

Case law

Lopez Ribalda and others v Spain (2020)
The Grand Chamber of 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 had been met when the supermarket installed hidden cameras unknown to the staff. The Grand Chamber found that the shop workers' right to privacy under Article 8 of the European Convention on Human Rights had not been breached, overturning an earlier ruling. If there is no notification of the surveillance the Grand Chamber suggested that employers may be able to justify covert CCTV if:

- they have a reasonable suspicion that employees are committing serious misconduct (such as theft)
- surveillance lasts only as long as it takes to catch the wrongdoers
- the footage is used only for the purpose of finding those responsible
- there appears to be no alternative way of catching the wrongdoers.

The location of the covert CCTV was also significant, with a general expectation of privacy being lower in public places such as shopfloors. However, there would be a very high level of expectation of privacy in some areas that are private by nature, such as toilets, or in closed working areas, such as offices.

Employers 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 unless it can be adequately justified.

The recording will be considered as personal data under the UK General Data Protection Regulation and therefore needs to be processed lawfully and fairly.

The Information Commissioner's Officer's guidance on 'Data protection and monitoring workers' states that employers should be able to justify every decision they make to carry out any covert monitoring.

More information on the use of monitoring and surveillance in disciplinary cases can be found in APPENDIX FOUR.

QUICK CHECKLIST

- ☐ If CCTV, audio recording, tracking devices, smart phone apps or covert surveillance is taking place or is planned, has the employer undertaken a data protection impact assessment (DPIA)?
- ☐ Has the employer fully considered the requirements of the UK General Data Protection Regulation, Data Protection Act 2018, 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?
- ☐ Are individual workers asked for consent to download apps onto personal or work smartphones and are they made fully aware of terms and privacy issues?
- ☐ 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 the UK 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 the UK GDPR and the Data Protection Act 2018? 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.
- ☐ Will staff be notified of the procedures for gaining access to personal data recorded as is their right under UK GDPR, as well as warnings given about the type of surveillance and who to contact about the app?
- ☐ Encourage employers to use ICO guidance to help ensure they fulfil their data protection responsibilities when monitoring workers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/ When following the guidance, steps taken by the employer include making workers aware of the nature, extent and reasons for monitoring; having a clearly defined purpose and using the least intrusive means to achieve it; having a lawful basis for processing workers data – such as consent or legal obligation; telling workers about any monitoring in a way that is easy to understand; nly keeping the information which is relevant to its purpose; carrying out a Data Protection Impact Assessment for any monitoring that is likely to result in a high risk to the rights of workers; and making the personal information collected through monitoring available to workers if they make a Subject Access Request (SAR).

Use of biometrics in the workplace

Biometrics are used to identify 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.

Biometric data is a type of personal data classified under the UK GDPR as likely to be more sensitive, and so should give the individual extra protection.

Many technological tools using biometrics 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.

In 2019, the Deputy Commissioner for Policy at the ICO 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."

Detailed guidance on processing biometric data is expected from the ICO in due course.

Information on **Special Category Data** is available from the ICO https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/

UNISON cases

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 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.

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 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.

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.

Case study - Serco

In February 2024, Serco Leisure, Serco Jersey and seven associated community leisure trusts have been issued enforcement notices by the ICO (Information Commisioner's Office) ordering them to stop using facial recognition technology (FRT) and fingerprint scanning to monitor employee attendance.

The private contractor used biometrics to monitor the attendance of more than 2,000 employees at 38 leisure facilities across the country. But they failed to show why it is necessary or proportionate to use FRT and fingerprint scanning for this purpose, when there are less intrusive means available such as ID cards or fobs.

Employees have not been proactively offered an alternative to having their faces and fingers scanned to clock in and out of their place of work, and it has been presented as a requirement in order to get paid.

The ICO have told Servo that they must stop all processing of biometric data for monitoring employees' attendance at work, as well as to destroy all biometric data that they are not legally obliged to retain. This must be done within three months of the enforcement notices being issued.

The issue has been raised with Serco nationally but branches and regional organisers should alert UNISON's private contractor's team at private.contractors@unison.co.uk if they become aware of any other biometric tracking being used.

More details at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/

QUICK CHECKLIST

- ☐ If biometric identification is being used or planned, has the employer undertaken a data protection impact assessment (DPIA)?
- ☐ Has the employer fully considered the requirements of the UK General Data Protection Regulation and Data Protection Act 2018?
- ☐ Has the employer consulted with workers and their trade union representatives on its use, its purpose and how it will be carried out?
- ☐ What problem is the employer trying to solve and how does this particular type of tool address this problem?
- ☐ Is there an agreed written policy covering the use of biometric identification 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 UK GDPR?
- ☐ Are no alternative measures possible, indeed preferable (less intrusive, less costly, less controversial)?
- ☐ How much will introducing the new biometric 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, can the employer demonstrate that they fulfil other data protection conditions?
- ☐ 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 UK GDPR and the Data Protection Act 2018? 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.
- ☐ Encourage employers to use ICO guidance to help ensure they fulfil their data protection responsibilities when monitoring workers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers/ When following the guidance, steps taken by the employer include making workers aware of the nature, extent and reasons for monitoring; having a clearly

defined purpose and using the least intrusive means to achieve it; having a lawful basis for processing workers data – such as consent or legal obligation; telling workers about any monitoring in a way that is easy to understand; only keeping the information which is relevant to its purpose; carrying out a Data Protection Impact Assessment for any monitoring that is likely to result in a high risk to the rights of workers; and making the personal information collected through monitoring available to workers if they make a Subject Access Request (SAR).

6. Model new technology in the workplace policy

There are many policies that can fall under the umbrella of new technology in the workplace including:

- Automation and digitalisation agreements
- Monitoring and surveillance policies
- Information and communication technology monitoring policies
- CCTV and video surveillance policies
- IT and email policies
- Acceptable use policy for telephone, email and internet use
- Social media policies
- Vehicle monitoring policies

All of these policies should emphasise how the employer is fulfilling its legal requirements. Having established the principle of a new technology agreement, it is important that it sets out the consultation process that will be followed when any proposals for new technology are put forward.

Once the policy and its implementation has been agreed with the trade union, it should be communicated widely by management so that staff know the types of new technological tools being used in their workplace, their impact on their jobs and the reasons for using them.

The following model agreement can be used in the workplace to help ensure that the introduction of new technological tools or automation consider and address the impact on workers. However, it will of course need to be adapted as relevant to your workplace.

It may be helpful to be specific as possible about the type of technology involving algorithms and AI that there are concerns about, whilst at the same time recognising that there may be future technological developments that should be potentially covered.

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

Both ***[name of employer]*** and the trade union recognise that technology has the potential to deliver huge benefits in the delivery of public services, in creating growth, innovation, fairer and more manageable workloads, and improved efficiency and quality of work.

However, the parties to this agreement acknowledge that the introduction of new technology or making changes to the use of existing technologies may also present specific challenges to staff and management.

[Name of employer] recognises the need for new technological tools to be introduced in a way that gains the support of employees.

Both ***[name of employer]*** and the trade union recognise that new technology and automation:

i) may have a disproportionate impact on sections of the workforce defined as possessing protected characteristics according to the Equality Act 2010 ***[for Northern Ireland, replace with "a disproportionate impact on sections of the workforce defined within Section 75 of the Northern Ireland Act 1998"]*** and therefore an equality impact assessment will be considered for all proposals and action identified to address potential inequalities, with regular reviews agreed as appropriate;

ii) can cause distress amongst the workforce about its impact on the number and type of jobs available, which will be addressed through full consultation and fair procedures;

iii) offers opportunities for reducing repetitive aspects of job roles and retraining in more fulfilling dimensions of the role;

iv) will be accompanied by a risk assessment of changing pressures on staff where appropriate and will not be used to dehumanise the workplace or operational decision making.

The adoption of new technology shall not be considered solely as a method for reducing costs but as a means to improving quality of services that takes account of the crucial role that a motivated, well trained workforce has in delivering high quality services. Any cost savings will be reinvested into the organisation to improve services, and to develop and reward the workforce.

The introduction of new technology will not affect contractual pay nor reduce overtime pay ***[if relevant]*** nor benefit one group of workers at the expense of another.

Both ***[name of employer]*** and the trade union are committed to address any issues arising from the introduction of new technology or when making changes to the use of existing technologies through cooperation, consultation and mutual agreement.

Thorough consideration will be given to mitigating any possible negative consequences where a decision is made to proceed.

[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 any technological systems in the workplace, will be treated as a serious disciplinary matter. More details can be found in the 'Data protection policy' at ***[include links or signpost to the policy].***

The introduction of new technology will not impact negatively on the health and safety of staff, and therefore a health and safety risk assessment will be considered for all proposals and action identified to address potential risks.

New technology will not be used to assess or predict workers' performance without express and informed agreement.

Automated decision making will never be used where it may significantly impact on access to work, terms and conditions of work or quality of work.

New technology will not be used for monitoring or surveillance of the workforce without express and informed agreement. More details can be found in the 'Data protection policy' and/or 'Privacy notice' and the 'Monitoring and surveillance in the workplace policy' ***[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.

[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 UK data protection legislation and the Information Commissioner's Office (ICO) Employment Practices Code. Therefore, if appropriate or required as when processing involves **special category data**, a data protection impact assessment will be considered for all proposals and action identified to address potential risks to data subjects' rights and freedoms. Regular reviews of the risks will be agreed as appropriate and trade union safety representatives will be consulted throughout these assessments.

[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 policy will always be used in a way that is consistent and compliant with the UK data protection legislation, the Information Commissioner's Office (ICO) employment practices guidance and the Human Rights Act and any other relevant legislation in place.

Scope of Policy

This policy applies to all staff who are employed at ***[name of employer].*** It also includes job applicants, ex-employees and contractors. It covers the introduction of all forms of new technology, AI or automation or when making changes to the use of

existing technologies that may impact on the workforce whether directly or indirectly, including in their management, service delivery, monitoring and surveillance.

This policy is supported by and developed with the trade union representing the employees.

Purpose

This agreement sets out the procedures that will be observed when the introduction of all forms of new technology, AI or automation, or when making changes to the use of existing technologies, is under consideration.

These procedures will be followed to ensure that the full range of costs and benefits and challenges are understood before deciding whether to proceed with the adoption of the new technology.

Consultation on proposals for the adoption of new technology

[Name of employer] will notify and consult with the trade union at an early stage when they intend to introduce technology or automation that may have a significant impact on work, workers or the workplace.

This is to ensure that the process is transparent and there will be sufficient time to plan how to train up the workforce in the specific skills required for any new activities and tasks.

Details of all technology used within the workplace will be documented including where it is used, the data involved, and any update or change to the system, and these details will be made available to the trade union, as well as all workers and job applicants.

[Ideally there should be a separate new technology joint negotiating committee involving union reps and the employer to discuss the introduction of new technological tools or automation prior to implementation.

This needs to be backed up with time and resources to ensure that reps involved have the necessary understanding of the new technology and potential impact on workers, and that details can be comprehensively communicated to all staff.]

Proposals for the adoption of new technology will be brought before a joint negotiating committee ***[or equivalent mechanism involving the trade union]*** when proposals are still at a formative stage to enable employees to input into decisions.

Information shared through the consultation procedure shall enable the committee to develop a thorough understanding of:

- The rationale for the adoption of new technology;
- The cost impact and a breakdown of those costs;
- Any external providers involved;

- Who is responsible for the technology and key decision-making points;
- The proposed implementation time-line;
- The consequences for customer service and evidence of how these align with customer preferences;
- The consequences for the working arrangements of the staff directly affected;
- The consequences for integrated working across the organisation;
- An assessment of the equality impact and any subsequent reviews;
- An assessment of the data protection impact (if relevant) and any subsequent reviews
- An assessment of any health and safety risks and any subsequent reviews;
- Monitoring mechanisms.

The introduction of any new technology within the workplace, will have a clear aim communicated to all staff, will be appropriately trialled involving trade union reps at all stages, and will have clear criteria for the evaluation of its success, whilst taking account of workers' concerns and any health and safety issues.

No automated decisions will be made by new technology without being reviewed by humans. All workers have the right to respond to their line manager whenever decisions are made about them. All job applicants have the right to respond to HR whenever decisions are made about them.

Wherever possible, pilots of the proposals will be conducted to allow more informed assessment of its likely full impact.

The consultation period will allow staff and union reps sufficient time to consider the proposals fully and to request further information if required.

The joint negotiating committee will have the resources to access independent experts to help it examine and assess the information provided if required.

Meetings will be held with trade union reps to enable staff to provide feedback on concerns throughout the process and facilitate dialogue on solutions to areas of dispute.

In response to feedback and alternative proposals, ***[name of employer]*** will inform the joint negotiating committee of changes made to proposals or the rationale for rejecting alternatives.

Information shall be shared in accordance with the Acas code of conduct on Disclosure of Information to Trade Unions for Collective Bargaining Purposes.

Restructuring of Job Roles

By agreeing plans for the introduction of new technology with the trade union, ***[name of employer]*** aims to protect jobs, create new jobs and avoid any compulsory

redundancies in line with the Redundancy policy ***[amend as appropriate]*** at ***[include links or signpost to the appropriate policy].***

Where the introduction of new technology is expected to lead to the restructuring of job roles, ***[name of employer]*** will provide the joint negotiating committee with a more detailed consultation paper setting out:

- Current and proposed staffing structure;
- Skills required for the new structure and any training opportunities;
- Job descriptions and grading / bandings of posts;
- Method by which employees will be selected for posts within the new staffing structure(s).

More details on the method of restructuring posts can be found in the 'Workforce reorganisation policy' ***[amend as appropriate]*** at ***[include links or signpost to the appropriate policy].***

[More information on the restructuring process can be found in UNISON's bargaining guide on 'Workforce reorganisation' *www.unison.org.uk/content/uploads/2021/09/Bargaining-on-workforce-reorganisation-v2.pdf* ***]***

The introduction of new technology and automation will not be used to reduce the number of job roles within the workforce, nor be used to demote job roles within the workforce.

The introduction of new technology and automation will not be used to expand the use of insecure contracts such as zero hours contracts, carrying inferior employment rights.

Training and reskilling

[Name of employer] recognises the importance of training staff affected by the introduction of new technology, including managers, to ensure that all staff have necessary skills and understanding. Training will include consideration of any related data protection, equality and health and safety issues.

Adequate resources will be provided for retraining and re-skilling of staff including paying all staff at their normal rate whilst being trained.

Training will be made available to all staff, including agency staff, apprentices and those returning from family leave or after any other periods of long-term absence ***[amend and add to as appropriate for your workplace.]***

Training will be carried out in a timely manner prior to implementation of any new technology.

Staff will be appropriately compensated for any new skills learnt as a result of introducing the new technology in the workplace, including the consideration of increased wages, increased flexible working, reduced hours of work.

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, privacy, equality and health and safety issues will be provided to all managers.

Trade union involvement

Consultation will take place with the recognised trade union at the earliest stage when considering new technology into the workplace, including in the design, procurement, trial, implementation, review and maintenance.

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

Health and safety

[Name of employer] recognises that the impact of new technology on the workforce needs to be assessed in terms of duties imposed by the 1974 Health and Safety at Work Act/ Order requiring protection of the health, safety and welfare of employees, as well as the 1999 Management of Health and Safety at Work Regulations requirement assessment of ill health risks, ensuring hazards are removed or proper control measures put in place to reduce risks so far as is reasonably practical.

Consequently, a risk assessment will be conducted of proposals for new technology using the HSE Management Standards, regular reviews of the risks will be agreed as appropriate and trade union safety representatives will be consulted throughout these assessments.

Particular attention will be paid to ensuring that any automated tracking of work and setting of work rates ***[if relevant to your workplace]*** will be balanced against the health and well-being of the workforce.

[Name of employer] recognises that disconnecting from work is vital to a healthy and sustainable work life balance, but that the use of new technology may create risks, expectations, or pressures to work longer hours that often encroach on home life. ***[Name of employer]*** does not expect staff, in normal circumstances, to work more than their contractual working hours.

The use of new technology will not be allowed to infringe workers' 'right to disconnect' from work demands outside contracted working hours or when officially on-call.

Other than where expressly agreed with the staff member, line managers will not contact staff outside of their agreed working hours for work-related matters. If staff

do receive any form of work-related communication outside of working hours, there is no expectation that they read it or respond until within their working hours.

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: ……..

APPENDIX ONE - Some key laws affecting the use of new technologies within the workplace

The basics of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)

The UK data protection regime is set out in the Data Protection Act 2018, along with the UK GDPR.

On 8 March 2023, the UK government introduced the **Data Protection and Digital Information (No. 2) Bill** in parliament. The Bill, if brought into force, would amend various provisions in the UK General Data Protection Regulation and the Data Protection Act 2018.

As the Information Commissioners Office describes, data protection "is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society."

More information:

ico. (Information Commissioners Office)

https://ico.org.uk/

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.

Introduction to data protection https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/

Guide to the General Data Protection Regulation (GDPR) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

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.

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 of paper-based information.

Processing includes:

- Obtaining and retrieving information.
- Holding and storing information.
- Making information available to others, within or outside an organisation.
- Printing, sorting, matching, comparing, altering and destroying information.

A data controller (the natural or legal person, public authority, agency or other body which, alone or jointly with others) determines how personal data will be used. The employer is likely to be the data controller.

A data processor is a body which processes information on behalf of a data controller. Any use of data is 'processing' so includes obtaining and retrieving information, holding and storing information, making information available to others, within or outside an organisation, printing, sorting, matching, comparing, altering and destroying information.

Data subjects are the individuals whose personal data the data controller and data processor holds. Employees and service users will be data subjects.

The employer should have someone appointed with designated responsibility for data protection matters, including UK GDPR. They will be responsible for ensuring that personal data is correctly collected, stored, used and securely destroyed once it is no longer needed.

The six lawful bases for processing personal data

Under UK GDPR there are **six lawful bases for processing personal data**. Everything an employer's data controller 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 freely given clear consent for the employer's data controller to process their personal data for one or more specific purposes.

(b) Contract: the processing is necessary for a contract the employer, as the data controller has 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, as the data controller, to comply with its legal obligations.

(d) Vital interests: this usually applies where processing cannot be based on another legal basis. For example, where the processing is necessary to protect someone's life, or in some cases someone's property, such as in monitoring emergency situations, natural or man-made disasters.

(e) Public interest task: the processing is necessary for the employer's data controller to perform a task in the public interest or for the official functions vested in the controller.

(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 the data controller is a public authority processing data to perform official tasks – the public interest task basis applies in this circumstance.)

Special category personal data

Some personal data is classed as "special category" or "sensitive" under data protection law. This data includes information relating to an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual orientation
- 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.

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 data subject involved has given explicit consent for the data to be used by the employer's data controller 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 UK GDPR, the employer's data controller has to be more transparent about what they are collecting data for and how they use it.

More information:

'Employment information' from the Information Commissioner's Office
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/

Data protection impact assessments (DPIAs)

The UK GDPR also includes an obligation to conduct a **Data Protection Impact Assessment (DPIA)** for types of processing in certain circumstances likely to result in a high risk to data subjects' rights and freedoms. For example it would include processing that might lead to discrimination, deprivation of rights, revelation of special categories of data and profiling.

It's also good practice for employer data controllers to conduct a DPIA for any other major project that involves the processing of personal data.

It is likely that the introduction of any new technology for monitoring, surveillance or assessing of workers whilst working, will require a DPIA.

The Information Commissioner's Office (ICO) has an example DPIA template
https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx

The ICO also has a clear DPIA screening checklist that, if followed will help ensure DPIAs are undertaken when legally required and best practice.

There is also a DPIA process checklist and 'have we written a good DPIA?' checklist to help ensure that the assessment is fit for purpose.

The TUC has some useful information for trade unions on what to consider before undertaking a digital project, that includes consideration of DPIAs – the same principles should be considered by employers
https://digital.tuc.org.uk/privacy-by-design/

Examples of risks that may be identified include the potential loss of data or inappropriate sharing and use of the data collected, a negative impact of the decisions made using the data including discrimination, reduced pay, lack of promotion opportunities, damage to the individual's reputation.

Once the DPIA has identified the purposes of processing, necessity and proportionality of those purposes, as well as the risks, the employer should state what safeguards and actions will be taken to mitigate them.

More information from the Information Commissioner's Office on DPIAs:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Data protection impact assessments: a guide
Produced by Prospect trade union in partnership with the Institute for the Future of Work www.ifow.org/knowledge-hub-items/data-protection-impact-assessments-a-guide-for-union-representatives

Automated decision-making and data protection

The UK GDPR also covers automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

There are specific information obligations under Articles 13 and 14 of the UK GDPR. The data subject must be informed about the fact that profiling is taking place, together with information about the logic involved, as well as the significance and envisaged consequences of the processing.

Profiling might be part of an automated decision-making process and profiling information could be gathered from such sources as internet searches, social networks and lifestyle data from mobile phones. There are a number of ways in which employers might impermissibly process such data.

Examples where it is used in the workplace are recruitment aptitude tests using pre-programmed algorithms and criteria, or where personal data is used to analyse or predict performance at work.

Under Article 22 of the UK GDPR, an individual (the data subject) has "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

This would include for example, e-recruiting practices without any human intervention.

Employers can only use automated decision-making or profiling at work if they can show that the decision is:

- necessary for the purposes of a contract between them and the data subject
- authorised by law (eg to prevent fraud or tax evasion), or
- based on the data subject's explicit consent.

Workers should always understand the reasons behind any decisions made about them – as data subjects – by automated processing used by the employer as a data controller, and the possible consequences of the decisions. There should also always be a means of objection to the decisions made and human intervention.

Further information from the ICO:

Rights related to automated decision making including profiling

For organisations
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

For individuals
https://ico.org.uk/your-data-matters/your-rights-relating-to-decisions-being-made-about-you-without-human-involvement/

The Privacy and Electronic Communications (EC Directive) Regulations 2003

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications, which apply whether or not personal data is processed, particularly in relation to online behavioural advertising. They were most recently amended in 2018.

Although the current law is 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.

Examples of “electronic communications” are email, direct messages on social media, text message, fax and automated telephone calls. “Direct marketing” is defined very broadly and includes the promotion of an organisation’s aims, values and policies, so need not involve selling a product.

The rules in the current 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 are 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 or valid consent.

Subscribers and users must be provided with “clear and comprehensive” information about the relevant purposes. With apps, this is likely to be within the sign-up stage. Consent must be freely given, specific and informed. The ICO has confirmed that the same definition of ‘consent’ applies for rights under UK GDPR and PECR.

The key requirement of the PECR is that individuals contacted electronically must have given their prior consent for this communication, other than in very limited circumstances.

More information:

Information Commission's Office Guide to Privacy and Electronic Communications Regulations https://ico.org.uk/for-organisations/guide-to-pecr/

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. It may be taken into account when considering how a worker's rights are applied under (for example) employment law and data protection law.

More information:

Equality and Human Rights Commission (ECHR)
www.equalityhumanrights.com/en/human-rights/human-rights-act

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. However, the Act is mostly used to legally challenge the intrusive behaviour of public bodies or governments.

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.

An updated and simplified Code came into effect on 12 January 2022.

The **12 point guiding principles** as laid out in the updated Code are:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

APPENDIX TWO - example policy covering use of phone, email and internet within the workplace

Telephones and ICT acceptable use

[This is a very basic example of an acceptable use policy.

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 been 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.

[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.

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 seven ***[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].***

APPENDIX THREE – example monitoring and surveillance in the workplace policy

[This is an example of a policy covering the use of technology for monitoring and surveillance.

Details will always be specific to individual workplaces as appropriate to the type of work undertaken and as negotiated with the trade union.

As Acas guidance points out, "Employers should have written policies and procedures in place regarding monitoring at work. Monitoring shouldn't be excessive and should be justified. Staff should be told what information will be recorded and how long it will be kept.]

[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.

The use of technology for monitoring or surveillance of staff ***[such as CCTV and other tracking or audio recording or biometric monitoring arrangements]*** is 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 policy
- preventing and detecting crime.

All use of technology ***[such as CCTV and 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 technology ***[such as CCTV and 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 seven ***[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 technology ***[such as CCTV and 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, audio or biometric records of themselves recorded by technology ***[such as CCTV and other tracking or audio recording or biometric monitoring arrangements]*** and to receive a copy of these images, audio 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].***

Body worn cameras

The use of body worn cameras is in line with relevant legislation and guidance provided by the Information Commissioner's Office and the Surveillance Camera Commissioner, to help ensure the health and safety of staff.

They are to be used to support staff during their duties with the aim to act as a deterrent to reduce assaults, threats, abuse and other incidents of anti-social behaviours. They can also be used to capture any identified safety hazards or safety related incident.

All use of body worn cameras will be conducted in accordance with a data protection impact assessment that ***[name of employer]*** has carried out to ensure that their use 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].***

All employees issued with body worn cameras, must receive training on their management, operation as well as data protection principles. Body worn cameras must only be used in an overt manner where it is fully visible and all use must be justifiable and proportionate to the issue at hand.

All data captured on the body worn camera will be automatically downloaded once the camera is returned to its docking station and the end of the shift ***[or adapt as appropriate to your workplace]***.

Once transfer of the data has been completed all footage stored on the body worn camera will be deleted automatically. When not in use the body worn camera must be stored in a secure place under lock and key.

All recorded footage remains the property of ***[name of employer]*** and storage and access to footage will be controlled in the same manner as conventional CCTV.

[Name of employer] will regard any attempt to use a body worn camera that is not in accordance with this policy as gross misconduct.

[As appropriate to your organisation, you may also include details of how staff members should operate the body worn camera, such as booking equipment in and out, periodic checks by line managers to ensure that no unauthorised data is stored on the device, when it is appropriate to start recordings on the device, how to verbally warn those being recorded.]

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 wrongdoing, 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.

APPENDIX FOUR - 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 evidence. 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."

More information:

Acas guidance on conducting workplace investigations
www.acas.org.uk/acas-guide-to-conducting-workplace-investigations

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.

More information:

Information Commissioner's Office guidance on 'CCTV and video surveillance'
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

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.

Employers do 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 the employer to release the information.

More information:

Information Commissioner's Office 'Data Sharing Code of Practice'
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/

Information Commissioner's Data Sharing Checklist
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist /

APPENDIX FIVE – glossary

AI – standing for 'artifical intelligence'. So-called 'smart' machines that use data and algorithms supplied to them to draw conclusions that can then be acted on by humans or can cause other machines to take action without further human involvement. The computers carry out tasks that you would normally expect to be carried out by a human such as making decisions or recognising objects, speech and sounds.

The UK's Parliamentary Office of Science and Technology has published a briefing on what AI is, how it works, how it can be used, as well as concerns and perceptions around AI.

Algorithm – mathematical rules or step-by-step instructions given to a computer on how to use the data supplied to it to solve a problem or complete a task. They can be used to enable predictive models to be developed by picking up patterns in the data.

Algorithmic management systems (AMS) – when machine learning is used on data about workers to automate or inform manager decisions. For example, they may monitor workers through surveillance such as location tracking or facial recognition, then collect data from this surveillance such as times, frequencies etc, process and analyse the data, which can then impact on a worker's behaviour or treatment of them by the manager based on the AMS' perception of their performance.

App – a small software programme often downloaded onto a mobile device such as a smartphone

Asynchronous video interviews (AVIs) – interviews that are recorded by candidates and reviewed by the interviewer at a later stage. The interviewers and candidates do not meet. AI technology may be present. The AVIs may have passive AI, they may be AI-assisted or AI-led. The technology may make recommendations in a report to the interviewer on the hiring decision by interpreting aspects of candidates' performance such as facial expression, gesture, tone of voice, and/or keywords in responses, or it may be used to assess whether candidates progress to the next phase of the recruitment process without any human decision-making.

Automation – the process by which machines replace tasks previously done by humans. It encompasses technology such as artificial intelligence, advanced robotics, 3-D printing, nanotechnology, and advanced biotechnology.

Automated individual decision making or automated decision making (ADM) - making a decision solely by automated means without any human involvement

BWV – body worn video

Big data – ‘big’ often refers to a scale so exponential that many might struggle to conceptualise it

Biometrics – used to identify 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.

CCTV – standing for closed-circuit television more commonly known as video surveillance

Chatbots – a computer programme or software that simulates human conversation through voice commands or online text chats or both. A website chatbot may be fed thousands of human text chats from the past, so it can learn how to mimic a conversation with a customer.

Cookies – information saved by a web browser when an individual visits a website so that the website can retrieve it at a later time

Data – information in a format that computers can store and use. In the workplace it may be details about your age, gender, pay, when you clocked in for a shift, tasks completed, a visual recording of your face, a voice recording of a phone call etc.

Deep learning – a type of ‘machine learning’ (see below) based on a set of algorithms that attempt to model high level abstractions in data. Deep learning describes a connectedness, which means that if one machine makes a mistake, all autonomous systems will keep this in mind and will avoid the same mistake the next time.

Digitalisation or digital transformation – the process of adoption and implementation of digital technology by an organisation in order to create new or modify existing products, services and operations by the means of digitisation

Digitisation – the process of converting information from physical formats (text, pictures, sound) into a digital format that can be processed by computers

Generative AI - artificial intelligence capable of generating text, images, or other media, by learning the patterns and structure of their input training data and then generating new data that has similar characteristics. ChatGPT is one example.

ML – standing for ‘machine learning’ is a type of AI, when a computer is programmed to learn from the use of its algorithms by analysing and making predictions about the data. Although humans tell the software what to output, they don’t tell it how. The software learns through trial, error and feedback.

Platform work - an employment form in which organisations or individuals use an online platform to access other organisations or individuals to solve specific problems or to provide specific services in exchange for payment

Predictive models - the conclusions that are generated by machine learning using historic data. These models enable AI decision-making.

Profiling – automated processing of personal data to evaluate certain personal aspects of an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability behaviour, location or movements

Radio-frequency identification (RFID) tracking – a way to send information using electromagnetic fields to automatically identify and track objects

Robotics – the design, construction, operation, and application of robots for tasks traditionally done by humans

Spyware – software that enables a user to steal information about another's computer activities by secretly transmitting data from their hard drive

Tachographs – used to record information in a vehicle about driving time, speed and distance

Workforce analytics – also called people analytics, is the process of collecting, analysing and using quantitative and qualitative data about the workforce, alongside business performance data. An example would be collecting data to link a staff pay increase with increased productivity or customer satisfaction.