



Commercial Briefing

Use of technology in the workplace – employee monitoring

With the advent of new technologies, an employer's capability to monitor its staff is increasing. Data about employees can be collected in a whole manner of ways using CCTV, swipe card systems and phone, e-mail and computer records. On occasion, employers may try and use data collected from this kind of monitoring to improve the performance of staff or even for disciplinary purposes.

There are strict rules relevant to this kind of activity which must be followed. Whilst employers may be widening the scope of technology to which their staff have access, it does not follow that their right to use any data collected from use of that technology increases.

In this bulletin we look at the framework which should be in place to ensure that this kind of activity is lawful.

Monitoring must be justified

There can be legitimate reasons for monitoring but it must be undertaken within the right framework. The first thing therefore, is to ensure that any monitoring which does take place can be justified. The legislation which covers these issues envisages a number of reasons for which monitoring may be legitimate. For example, monitoring may be justified in order to make sure that policies are being complied with or to detect unauthorised use of computer or other communications systems.

An employer looking to undertake any kind of monitoring should carry out a review or impact assessment of the need to monitor before the monitoring takes place. This should establish whether or not there is a justification for the monitoring and if so, whether it is of an appropriate nature, taking account of both the benefits as well as any disadvantages which may arise. An assessment should also take account of whether business aims can be achieved without intrusive monitoring. For example, would an assessment of traffic data on a statistical basis satisfy the organisation's aim rather than specific monitoring of individuals' e-mail usage?

It is also worth noting that covert monitoring may only be justified in the most rare of circumstances, usually where there is a well-founded basis for suspicion of criminal activity. Therefore any entity engaging in covert monitoring of any kind should consider immediately whether the activity can be justified.

Prior notification that monitoring may take place

The second key thing which is commonly missed in practice, is the requirement to give staff prior warning of the fact that monitoring may take place from time to time and to explain

what any data collected will be used for. Monitoring will only be justified where such prior notice has been given.

This translates itself into a practical need to have in place a comprehensive IT policy which sets out clear provisions on what kind of activity is permitted when making use of facilities and to explain the circumstances in which monitoring may take place. Not only does this give the prior notice which is necessary but it also makes clear what the scope of permitted use is so that there can be clarity on whether or not policy has been breached.

IT policies will obviously vary between organisations but typically will address issues such as the use of e-mail, internet access and phone systems as well as IT security, use of portable devices and personal use restrictions. They are also an opportunity to remind staff of the importance of treating electronic communications in the same way as other written communications.

Best Practice and Guidance

A full code of practice published by the Information Commissioner's office provides guidance on the relevant legislation and offers advice about best practice on communications monitoring and interception. Significantly, earlier in the year the Commissioner issued a summary guide on the issue and specifically made a point of highlighting that the guide is aimed at small businesses in particular.

CCTV in the workplace

Another relevant issue is the use of closed circuit television. This kind of technology is now so commonplace that it has become part and parcel of many working environments. Wherever CCTV is used, notices should appear to warn anyone including employees who may be caught by CCTV that such a system is operating in the area. In addition, the notice should state who is responsible for the system and should appear in a prominent location.

Further guidance on this issue has been issued by the Information Commissioner together with a CCTV Small User Checklist which is again specifically aimed at small businesses. This covers issues such as the siting of cameras, image retention and usage and maintenance of the system. Care should be taken to follow the guidance which reflects legal requirements under several pieces of legislation relevant to this area.

To discuss how Berg Legal can assist you with these issues, please contact either Stephen Foster, Head of our Corporate and Commercial Department at stephenf@berg.co.uk or Luisa D'Alessandro who is an Associate in the team at luisad@berg.co.uk. Alternatively you can call Stephen or Luisa on 0161 833 9211.

berg legal 35 peter street manchester m2 5bg
t. 0161 833 9211 f. 0161 834 5566 e. help@berg.co.uk
dx 14379 manchester 1 www.berg.co.uk Regulated by the Law Society

The information and opinions contained in this document are not intended to be comprehensive, nor to provide legal advice. No responsibility for its accuracy or correctness is assumed by Berg Legal, or any of its partners or employees. Professional legal advice should be obtained before taking, or refraining from taking, any action as a result of the contents of this document.

