MATT GINGELL
020 3797 1264 | mattgingell@mattgingell.com

Privacy: HR guide

Description

Introduction

Employers must respect **privacy**, and can only access private emails and messages of their staff in limited circumstances.

Employee right to privacy

The European Convention on Human Rights, which is incorporated into UK law, states that everyone has the right to respect for their private and family life, their home and their correspondence. The right to **privacy** is qualified and there are some instances when interference with the right can be justified. There should be a balance between the general interest of the community and the individual's fundamental freedoms. In the employment context a balance has to be struck between the employee's right to **privacy** and the employer's interests.

Although only public bodies must expressly comply with this right, it is relevant to all employers (including the private sector) as courts and tribunals must interpret, as far as possible, all legislation consistently with the right.

In most instances, therefore, emails and messages received and sent through private accounts outside work would be considered private, and employers would have no justification in scrutinising them. But there could be exceptions.

Misconduct/damage to reputation

Employers can dismiss fairly for misconduct and the misconduct may be inside or outside work. Damage to reputation could also provide a valid reason.

For conduct outside work, a key question would be whether the actions affect or could affect the employee's work in some way or whether there is or could be reputational damage to the employer. Sending emails or posting messages outside work could fall within scope.

There have been a number of cases where employees have posted inappropriate messages on Facebook that could have damaged the reputation of the employer, and have led to fair dismissals.

Monitoring

Another question is whether employers have the legal right to snoop on employees.

In September 2017 the Grand Chamber of the European Court of Human Rights (ECHR) considered whether an employer acted lawfully by accessing an employee's private messages on a business Yahoo Messenger account, where the employer's rules banned use of the company's IT systems for private purposes.

Overturning an earlier decision, the ECHR held that the right to **privacy** was breached on the basis that, among other things, the Romanian domestic courts had failed to determine whether the employee

had received prior notice from his employer of the possibility of monitoring, which was a relevant factor to be taken into account.The ECHR set out useful guidance in its judgment.

These are factors which should be taken into account in monitoring cases:

- Whether the employee had been notified about possible monitoring and been provided with adequate safeguards.
- The extent of the monitoring and the degree of intrusion into the employee's **privacy**.
- Whether the employer has provided legitimate reasons to justify the monitoring.
- Whether it would be possible to carry out monitoring by using a less intrusive form of monitoring than accessing actual content.
- The consequences of the monitoring for the employee.

Under the General Data Protection Regulations (GDPR) employers are obliged to provide detailed information to their employees about processing of personal data, which would cover monitoring personal data. This could be through CCTV monitoring or, for example, monitoring telephone usage, internet usage or emails.

The GDPR set out broadly the same data protection principles as under the old data protection law, although there are some distinctions.

The first GDPR data protection principle states that personal data must be processed lawfully, fairly and in a transparent manner. This would include employers having to provide detailed information such as the purpose of the monitoring, how long any monitoring data will be kept for, who the monitoring data will be shared with and the legal rights of the data subject.

In order for the data processing to be lawful the data controller must satisfy at least one of a list of conditions. One of the conditions is consent, which must be freely given, specific and informed. However, the Information Commissioner's Office (ICO) has published guidance stating that employers are unlikely to be able to rely on consent given the unequal power between employers and employees. Employers will need to rely on another condition, such as the processing being necessary for the purposes of the legitimate interests of the data controller or the legitimate interests of a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of

the data subject.

The third GDPR data protection principle states that personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

This is highly relevant to monitoring and requires employers to act proportionally, justifying their monitoring activities. The monitoring of email content from private accounts, for example, is likely to continue to be seen as one of the most intrusive forms of monitoring – and could be very difficult to justify.

Employers also need to be aware of the other GDPR data protection principles too, including demonstrating compliance. Undertaking a data protection impact assessment is compulsory where the type of processing involves a high risk to the rights and freedoms of individuals. Employee monitoring is likely to be high risk processing. In the context of monitoring, carrying out an impact assessment will involve identifying the purpose of the monitoring and the benefits, looking at the adverse effects of the monitoring, considering whether less intrusive monitoring is possible and assessing whether the monitoring is justified.

When it comes to monitoring, employers should consider the interception of communications framework as well. Before an interception, normally consent from the sender and recipient is required. Employers may, however, intercept communications which are “relevant to the business” without obtaining consent. The difficulty though is it will not be easy for an employer know for certain if an email is relevant to the business without opening it.

This guide is intended for guidance only and should not be relied upon for specific advice.

If you need any advice on **privacy** issues or have queries relating to other employment law matters please contact me on 020 3797 1264.

Do check mattgingell.com regularly for updated information.