LAWEXPRESS
Greater legal clarity

EMAIL AND INTERNET POLICIES

In a world which contains the "internet of things" it is perhaps inevitable that a lot of business is conducted via the internet, either on websites or through email. As such employers generally have in place email and internet policies to provide a framework for conduct and usage.

Here we look at what such a policy may typically contain.

For Emails:

1. Authorised usage
Generally, a workplace email facility is for work related emails. It is sensible to permit some personal use of email, especially if email is used for business purposes outside of normal working hours. However, it is generally the case that there will also be a restriction on excessive personal use by an employee as well as sending emails with inappropriate content which may be considered offensive. Illegal activities will also be prohibited.

For security reasons, it is also likely that employees will only be able to access work emails from specified devices all of which will usually be password protected.

2. Permitted content
The issue of content concerns not only what is said and circulated, but also how it is said. Many guidelines set out the style and tone of work- related emails as well as the font and format. Known as the 'house' style it is designed to reflect the professionalism and nature of the business they are representing.

Employers may specify what content is prohibited which could include: sexist, racist or other offensive material; defamatory material; bullying, and links to inappropriate material such as, jokes, chain letters, online gambling, and pornography. Spam filters are often set to ensure such content is blocked.

3. Sending emails
Employees are generally only able to send emails from their own password-protected account. Passwords are often strictly controlled, changed frequently and a mix of letters, numbers and symbols.

4. Confidential Information
Sometimes an employer may impose rules for handling confidential information; and may prohibit certain types of information from being sent by email for example, lists of customers and information about new products. It is also possible specify that some information can only be sent using encrypted email.

An email can be as contractually binding as any other form of communication and employers may prohibit the use of email for any contractually significant communications and insist that such documents are posted.

5. Receiving emails
An employer may set out who should read incoming emails. Generally, employees should read only emails addressed to them.

Any policy may also include how to handle incoming emails in the event of an employee being absent. If the employer decides to allow someone else to check employee emails, it must ensure personal emails are handled appropriately.

Emails can pose a security risk to an employer's business, they are often used to distribute viruses and spyware, or for phishing attempts. However, even the strongest filters will allow the occasional malicious email to slip through. Guidance should be provided to help employees identify a 'suspicious' email.

6. Email surveillance
An employer can monitor the use of a workplace email system, and there may be a relevant clause on email monitoring in the employment contract. If an employer uses monitoring software, staff should be made aware of this, and that the employer reserves the right to read individual emails.

Employees are generally entitled to a degree of privacy at work but if they are suspected of wasting time on personal emails, it may be possible to monitor usage provided there is a right to do so it the policy or contract.

Enforcement
Any email policy should be available for all to read. This may be in a staff handbook or form part of the employment contract. Any breach of the policy may result in disciplinary action being taken.

For Internet Usage:

An employer may structure any internet policy to ensure the internet is used effectively, by stating what is and is not allowed, and set up procedures to minimise risks to their business.

Such a policy may contain information about:

1. Access rights;
It is likely, for office based jobs, that internet access will be required. In other situations - such as in a factory - only certain staff members will need internet access. Training may be needed to provide training in some areas, for instance: how to use specialist internet software or cloud computing services; what the internet policy says and why it matters; spotting and avoiding security risks; and efficient use of the internet.

Protections may be in place such as firewall and security software and as well as restricting an employee's ability to change settings. There may also be set rules about whether personally owned devices can connect to the company network.

2. Usage;
It is usual to allow staff to access websites for business purposes and seek to control suspected misuse of the internet by blocking some content. An employer may decide to: limit personal use of the internet on business owned equipment, to breaks, or restrict the websites which can be visited when browsing.

There will usually be a policy to restrict downloads, to prevent causing damage to data and systems. Access to social media sites will generally be restricted or even prohibited.

3. Surfing;
Many employers make it clear that the web should be used for business purposes only. Some companies ban personal use altogether. Some companies allow limited personal use, if it doesn't affect an employee's work. It can be hard to define where business use ends, and personal use begins

Security and legal issues apply to all internet use. Employees may be restricted in the sites that they can visit, and employer's systems may block some content.

4. Downloads;
Downloading files from the internet always involves risk. Downloaded files may contain viruses, spyware or other malware. An employer may install virus-checking software and update it regularly. They may use security software to block or disable potentially harmful applications.

Enforcement
Employees should be given a copy of any policy and be asked to sign a copy to confirm they have read it. Very often breach of email and internet policies can be a disciplinary matter and breach can be treated as a form of misconduct.

Use of AI

The power and endless possibilities of AI are increasingly attractive to employees. AI may be integrated in some workplace operations and others may feel the need to engage such platforms as Chat GPT. It is important employers have a clear policy on this; not all results from such search engines are accurate or trustworthy and can result in false information being published.