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 website or 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 you use email 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 as well as inappropriate content which may be considered offensive. Illegal activities will also be prohibited.

For security reasons, it is also likely that you 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 will set out the style and tone of workrelated 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 you are representing.

Your employer may specify what content is prohibited which could include 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

It is likely you will only be able to send emails from you own password-protected account. Passwords are generally strictly controlled, changed frequently and a mix of letters, numbers and symbols.

4. Confidential information

Your Employer may have 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. They might 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 your employer may prohibit the use of email for any contractually significant communications and insist that such documents are posted.

Email and Internet Policies

5. Receiving emails

Your Employer may set out who should read incoming emails. Generally, you should read only your own emails.

Any policy should cover how incoming emails are handled when you are absent (e.g. on holiday). If your employer decides to allow someone else to check your emails, it must ensure personal emails are handled appropriately.

Emails can pose a security risk to your employers 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 is often provided to help you identify a 'suspicious' email.

6. Email surveillance

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

Your employer can inspect individual emails for 'specific business purposes', including: establishing the content of transactions and other important business communications; making sure you are complying with the law and with internal policies; preventing abuse of the telecoms system; and checking emails when you are on leave.

You are generally entitled to a degree of privacy at work but if your employer suspects you are wasting time on personal emails, they may monitor your emails but only if you have been told of their right to do so as per the policy.

Enforcement

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

For internet usage:

Your employer may structure any internet policy to ensure you use the internet 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, if you have an office based job, that you may need internet access. In other situations - such as in a factory - only certain staff members will need internet access. Your employer may need to provide training in some areas, for instance: how to use specialist internet software or cloud computing services; what their internet policy says and why it matters; spotting and avoiding security risks; and efficient use of the internet. They may wish to ensure that you follow their internet access procedures. Your employer may protect their business by using a firewall and security software and consider restricting your ability to change settings. They may also set rules about whether you may connect your own devices, such as a mobile phone, to the company network.

2. Usage

It is usual to allow you to access websites for business

Email and Internet Policies

purposes and seek to control suspected misuse of the internet by blocking some content. Your employer may decide to: limit personal use of the internet on business owned equipment, to breaks, or restrict the websites you can visit 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

Your Employer may 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 your work. It can be hard to define where business use ends, and personal use begins.

Security and legal issues apply to all internet use. You may be restricted in the sites that you can visit and your employers systems may block some content.

4. Downloads

Downloading files from the internet involves risks. Downloaded files may contain viruses, spyware or other malware. Your employer may install virus-checking software and update it regularly. They may use security software to block or disable potentially harmful applications. You may be prohibited from downloading inappropriate files and from installing software.

Enforcement

You should be given a copy of the policy and may be asked to sign a copy to confirm you have read it. There are legal restrictions on how your Employer may monitor your use of the internet (and email). If your Employer wishes to use monitoring software, they must tell you that they intend to do so in their internet policy and your employment contract.

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.