UNIT-12 Use of Social Media in the Workplace

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Understand the potential benefits and disadvantages of workplace social media use ✓ Know where to draw the line between productive and potentially problematic behaviour ✓ Monitor staff in a proactive manner that complies with the Data Protection Act of 1998

Unit 12

Use of Social Media in the Workplace

Introduction

Employees' increased use of social media, email, and the internet at work has created new challenges and risks in the workplace, particularly in terms of discipline and an employer's legal liability for its employees' actions.

Potential Risks to Employers

The following are some of the issues that can arise as a result of using social media and misusing email and the internet at work:

- Employees who are distracted or spend a lot of time online or sending personal emails have a negative impact on their performance.
- Breach of confidentiality if employees share commercial information, private customer information, or other sensitive data;
- Negative publicity for the company if an employee makes disparaging remarks about it online;
- Possibility of a bullying or harassment claim if one employee makes disparaging remarks about another or sends an offensive message to another.

It's important to remember that an employer faces a variety of legal risks as a result of its employees' actions.

Computer viruses are another threat that employers are vulnerable to. The download of certain types of files from the internet or attachments to emails is the most common source of computer viruses. Employees may unintentionally open emails that contain viruses. Employers must take steps to ensure that employees use caution when using email in order to protect their interests.

Have a Clear Policy

To manage the potential risks, it's critical to have a clear and well-communicated acceptable use policy in place, and to make sure that all employees are aware of it. This policy should be clear and concise, remove any expectation of privacy that employees may have, provide for an employer's right to monitor employees' use of social media, the internet, and email, and state that any information obtained through monitoring may be used in disciplinary proceedings.

By making it clear to employees what is and is not acceptable in terms of social media and electronic communications, an acceptable use policy can help to avoid problems. This could include the amount of time spent, when using such media is acceptable, and what types of

websites are acceptable. The existence of a policy will also make dealing with any issues that arise easier, such as disciplinary action when an employee uses social media to make defamatory remarks about the company.

The policy should not be so prescriptive (for example, regarding specific websites) that it quickly becomes obsolete. It should state who is authorised to communicate on behalf of the company via social media, as well as whether or not the use of social media will be monitored. It's worth noting that any monitoring should adhere to the Information Commissioner's Employment Practices Code.

Other organisational policies, such as disciplinary policies, bullying and harassment policies, and so on, will need to be linked to the policy. It's also a good idea to include a clause in employee contracts that spells out the employee's responsibilities when it comes to confidential information, and make sure that this clause covers social media.

When creating a policy, it's critical to consult a diverse group of employees from various departments to determine the current level of social media usage and to ensure that the policy is in line with the company's culture.

Ensure that the policy is properly communicated to both existing and new employees once it has been finalised. It should be included in the contractual documentation provided to all new employees and distributed to existing employees with the instruction that it is a part of their terms and conditions and should be carefully read.

Technology is rapidly evolving, and this trend is likely to continue. There have also been a number of significant legal cases that can help employers. Employers must keep up with technological and legal developments, and policies must be reviewed and updated on a regular basis to ensure that they remain current.

Monitoring Staff

The Data Protection Act of 1998 allows employers to monitor their employees' use of social media, the internet, and email. The Information Commissioner is in charge of ensuring compliance, and has published a document called "The Employment Practices Code," which includes information on an employer's right to monitor employees. Except in exceptional circumstances, such as when there are grounds to suspect criminal or equivalent malpractice, the Code protects employees from covert monitoring.

It can be found at www.ico.org.uk, the Information Commissioner's website.

If employees have been informed that their email accounts will be checked while they are away, the Code allows companies to do so. Unless their employer has a valid and defined reason to

examine the content, employees' privacy must be respected if they clearly mark an email as personal.

Using the Internet

Any restrictions on using the internet must be stated in the company policy, as well as whether access is allowed for business use only or for personal use as well. Even for business purposes, browsing has the potential to become unfocused and time-consuming. This wastes employees' time and resources, even if they do it on their own time. The policy should also include a warning about the dangers of obtaining and using unverified information for business purposes.

The policy should spell out what is and is not acceptable in terms of downloading time.

Downloading offensive, obscene, or indecent material is prohibited and will result in disciplinary action, according to the policy. Policies should also make it clear that downloading or transmitting certain images is a criminal offence, and that if there is any evidence of such activity, the police will be notified.

Much of what you see on the internet is protected by copyright, or at least claims to be. Any unauthorised reuse of downloaded information is prohibited. Many businesses have strict photocopying policies, and the same should be applied to copying from the internet. The law of copyright covers both documents and software.

Social Media

As a source of information, online diaries, or blogs, have grown in popularity. People are increasingly using social media sites like Instagram, Facebook, and Twitter to stay in touch and make new connections.

It is not just time lost which is of potential concern to employers, it is also the content which is posted.

Involving at least some employees in the proper use of social media for work-related activities, on the other hand, can provide significant benefits to the employer. Employees may conduct research, promote the company's products, and establish important contacts and relationships.

Employers can use corporate social networking to communicate with and engage their employees. Some businesses use social networking forums to raise awareness of their activities, bring employees from various locations together, or inject energy and "buzz" into internal communications. If employers create corporate social networks, a clear distinction must be made between corporate social networking for business purposes and personal social networking.

Employers should decide how they want to manage the use of blogs and social media and make sure it's spelled out in their policy. They should specify whether there are any restrictions on use, such as whether access to social networking sites is permitted only during lunchtimes or if there is a complete ban.

Defamatory statements about the company should be treated as a disciplinary offence, and confidential information should not be discussed in such forums, according to the policy. Employees who are unaware of the accessibility of content posted on social media and the potential audience can cause problems. It's easy to overlook the fact that even information shared in a closed group or protected by privacy settings can be shared. Employees must be educated about the potential risks in order to be reminded to behave responsibly online.

If employees feel they have no other option, they are more likely to use social media to air their grievances against the company. Clear and fair mechanisms for employees to file grievances, as well as an open culture in which managers listen to and respond to problems raised by employees, can help to prevent this.

Using Email

Although email communication has the same speed and apparent informality as using the telephone, it also has the permanence of written communications and, as such, must be controlled to ensure that it meets the same standards as well as other previously published documents.

The policy should specify whether the email service is only to be used for business purposes or if personal communication is permitted. If the telephone can be used for personal communications, it may be difficult to prohibit the use of email for the same purpose, even though email has clearly greater security implications.

Some email protocol and usage guidelines could be beneficial. Employees should be encouraged, for example, to limit group emails to ensure that all those copied on the email have a genuine need to receive it, and that emails are checked on a regular basis and filed once they have been dealt with.

The policy should state that email is subject to the same laws as any other written document, that employees should refrain from making false or defamatory statements, and that sending offensive emails will not be tolerated.

The sender of an offending message must face normal disciplinary procedures, but email is no different than any other interpersonal conflict in this regard (and has the advantage that, unlike purely verbal communications, it is possible to supply evidence to support a complaint).

It is possible to include a disclaimer in external email, but the policy should still emphasise the importance of acting responsibly when writing email and seeking advice before sending if there is any doubt about the message's contents.
Despite the advantages of email, excessive use can lead to a decrease in productivity. The policy should emphasise the importance of only sending relevant emails and not automatically forwarding all messages to long distribution lists.

A procedure for dealing with incorrect deliveries should also be included in the policy. It should, for example, state that a message that has been delivered incorrectly should be redirected to the correct recipient.

Dealing with Policy Violations

The Disciplinary Procedure should be followed when responding to a disciplinary matter involving inappropriate use of social media. Before any decision is made, a thorough investigation should be conducted, and any sanction should be fair and reasonable in light of all the circumstances.

Further Reading:

- ✓ ***Social Media in the Workplace: A Handbook by Chris Bryden (Author), Michael Salter, 2015***
- ✓ ***Handbook of Human Performance Technology, 3rd Edition, Jossey-Bass; 1st edition (October 2, 2009)***