The Risks Of Downloading Data In The Workplace

If an employee is transferring data outside the workplace or is downloading questionable material from the internet, there are a number of concerns that arise. Even if the intent is innocent, the risk for employers is real. Employers should monitor these activities and implement appropriate company policies to address this issue.

Typically, downloading occurs when data is transferred to a disk, USB key or information is sent to the employee's personal email address. Sometimes the downloading is innocent – the employee is simply taking work home. The downloading may also be for an improper purpose, such as a precursor to the employee departing. Often downloading of information is the employer's confidential business information. The information may have proprietary value and may include items such as marketing plans, client lists, financial data, pricing information, etc.

A secondary consideration is the privacy implications if the information being downloaded relates to identifiable individuals and the data becomes lost. For instance, the USB key or laptop which contains human resource data gets stolen from a car. The provincial and federal privacy laws mandate that an employer with confidential information about identifiable individuals safeguard and protect the confidential information from improper or inadvertent disclosure. The Privacy Commissioners encourage the encryption of confidential information.

Downloading may also occur when the employee is inappropriately accessing internet sites. These can include online shopping sites, excessive use of Facebook or other social media sites, or visiting inappropriate sites. These forms of downloading can reduce employee productivity and expose the employer's network to viruses and malware. It is important that employers continually update their policies and address issues associated with downloading. What we see and suggest will depend upon particular circumstances of the employer, but we frequently suggest some or all of the following practices:

- When hiring a new employee, the offer letter should contain specific requirements relating to computer use;
- Create an up-to-date confidentiality policy;
- Ensure there is a computer and internet use policy including policies regarding social media and downloading;

- Review your privacy policy;
- Develop education and training programmes in respect to the policies and the identification of potential risks;
- Identify high-risk situations (which may be employee access to information situations and taking appropriate and proactive steps to manage the high-risk situation);
- Conduct random audits of employee compliance with employer policies; and
- Discipline employees for breach of the policies.

Article by Michael D.A. Ford, QC

Davis LLP