MEMBER BULLETIN

Form No. MBN102

Employees who download confidential work documents to personal devices can be subject to dismissal

Employees working from home (WFH) can pose confidentiality issues for employers and reduce the capacity to keep sensitive company files secure.

Most employees, particularly when working from home or remotely, use both their employer and personal devices to send and receive emails, access and edit documents or join virtual meetings. In the absence of clear policies, the risks of sensitive information being copied or saved to an employee's personal device without permission can be high.

A case in point

Recently a Queensland employee argued that their dismissal for downloading confidential files to a personal device was unfair. The employee claimed that there was an absence of protocols and processes regarding accessing and storing documents remotely and the challenges of working from home, such as network outages, justified the reliance on desktops and USBs to save and access work.

The state government senior employee allegedly downloaded confidential documents onto a personal device and saved copies of the documents onto the desktop of their company provided computer and a privately owned USB without authorisation. After an audit and investigation, the employer dismissed the employee.

The employee claimed unfair dismissal. The matter was heard and dismissed by the Queensland Industrial Relations Commission (QIRC). The QIRC found that downloading work documents on a personal device was a valid reason for dismissal. It noted that as an experienced policy officer who had previously been in roles in which he dealt with confidential documents regularly, the worker should be "aware of the very strict requirements that related to the handling of [documents] to protect the confidentiality and security of the information."

Emailing work documents to a personal account

To protect commercially sensitive information, some companies claim copyright over documents in addition to any confidentiality policies. Therefore, sending those documents to a personal email address may constitute reproduction in a material form under the *Copyright Act 1968* (Cth), which is of course unlawful.

This can become especially relevant when information sent to a personal account or device is to set up a competing business or move to a competitor.

However, not all breaches of a code of conduct provide grounds for dismissal. In a case before the Fair Work Commission, a worker received compensation and reinstatement after their dismissal for breaching the employer's code of conduct was found to be harsh.

According to records, the employee emailed documents to their personal email address and stored photos of the documents on a personal device. The employee argued that none of the information was sensitive or classified and the captured information was for work purposes, with the FWC concluding that breaches were not "serious errors of judgment" and "did not warrant dismissal." Further, the FWC said the employee's failure to follow "lawful and reasonable directions" was not "substantial, wilful or intentional."

Authority to access and download

Employers should ensure that employees are fully aware of the policies and procedures regarding accessing or downloading confidential documents while working from home, through regular training and communication.

For further information contact ir@asial.com.au