Remote Working Considerations: Use of personal email & personal devices for work

During Covid-19, the vast majority of those working in the non-profit sector did so from home. A knock-on impact of this sudden pivot to remote working saw many using personal devices and emails for work purposes. While employers have an obligation to provide the necessary equipment to carry out work tasks, it may not have always been possible. This is particularly true in situations of restricted finances, which many in the non-profit sector felt due to limited fundraising.

There are some considerations for employers who find that employees are using personal emails and devices for work purposes in particular as remote and hybrid working practices are a continued feature. This comes on the back of a recent Workplace Relations Commission (WRC) case that found in favour of an employee who was found to be unfairly dismissed for using his personal email account.

Background to the WRC Case

An employee was awarded €4,500 after the WRC found he had been unfairly dismissed. The WRC adjudicator found that the actions of the employer in processing his personal data was a *"serious departure from the trust and confidence enshrined in a contract of employment".*

The employee had become aware of an external agency giving false information to customers about the services. He set up an experimental contract using his personal details and email. The external agency contacted the organisation who confirmed that the claimant was in fact an employee.

The employer began an investigation, and the employee became concerned about his data privacy rights and the fact his personal email was shared in the minutes of a meeting. He said he was told that the consequences of the disciplinary procedure if proven could lead to his dismissal. Before the findings of any hearing were issued, the employee resigned as he feared dismissal and the consequences for his career.

The employer stated that the employee resigned on a voluntary basis and the disciplinary procedure was lawful and reasonable. It argued that the case should be dismissed and there was no evidence he had been driven out of the organisation.

However, the WRC adjudicator said it was *"of note"* that one of the allegations raised occurred from the worker's personal email while logged off from the employer's IT system. She found the actions of the employer *"constituted a repudiatory breach of contract"* and said the organisation's *"processing of the complainant's personal data without apparent preclearance or complainant consent demonstrated a serious departure from the trust and confidence enshrined in a contract of employment".* And *"it was unreasonable and did not comply with the contractual provision on data protection".*

Use of personal email in the workplace

While this particular case highlights some warnings for employers, it should be stated that the use of personal emails for the purposes of work should not be allowed. There should be clear guidance for employees laid out in the Employee Handbook as well as Social Media Policy.

October 8, 2021

Apart from the obvious security risks associated with employees using personal email, what they may not realise is that any communications sent from a work laptop or PC is not only accessible by IT, it is also legally owned by the employer if it has been sent on work time.

Use of personal devices for work purposes

Since the commencement of the pandemic and with remote working practices being commonplace, employees should already have been advised not to use personal devices for work purposes. However, many employers have accommodated certain instances where employees use personal devices to carry out work tasks, such as tablets, phones and laptops. This has become even more common whilst employees have been working remotely. And while some obvious financial benefits exist there are considerable risks for the organisation.

The biggest risk is security; will the devices have appropriate levels of security software? Is the employer confident that employees won't share confidential information with other people outside the organisation and is the equipment being stored in the remote setting safe and secure? Many employees working in the non-profit sector will often have sensitive information on people they are supporting in the community and any loss of sensitive or confidential information could lead to fines from the Data Protection Commission.

An employee's right to privacy is also a consideration for employers so measures should be in place to be able to differentiate and protect personal information on devices from work-related information.

As with email and social media use, if an employee is using personal devices for work, there should be a specific policy in place. In that policy, it should be clear what information can be accessed by the employer, if the device is to be monitored, how the monitoring happens so that the employee can give informed consent.

Data protection of the remote office has both employer and employee obligations and duties. The continued operation of remote and hybrid work practices means that employers within the non-profit sector should take the lead in ensuring appropriate policies are in place, expectations relating to IT security and usage are communicated and most importantly that the principles of the General Data Protection Regulations are adhered to.

If your Organisation needs help in developing policies for the above scenarios, please get in touch with our expert-led team at Adare Human Resource Management.