ISSUE 33 | SUMMER 2013

Commercial eSpeaking

BREADEN McCARDLE CHUBB 44C Ihakara Street, Paraparaumu, PO Box 140, Paraparaumu 5254
Ph: 04-296 1105 | Fax: 04-297 3231 | info@bmc-law.co.nz | www.bmc-law.co.nz

Welcome to the first issue of *Commercial eSpeaking* for 2013. We hope that the start of this year has been good for your business and that it prospers during the 12 months ahead.

Enjoy reading this newsletter; we trust these articles are both interesting and useful to your business. If you would like to talk further about any of the topics covered in *Commercial eSpeaking* or any business law matter, please be in touch with us.

Inside:

Managing email, internet and social media

IT policies for your business

Does your company have an information technology policy? If so, when did you last update it and do your employees know it exists? This article looks at the pros and cons of your employees' internet access and what you can do to develop a policy around this… CONTINUE READING

Anti-Money Laundering Deadline Looms

Five months remain to get organised

One of the key items on this year's 'to do' list for all affected businesses will be getting ready for the main provisions of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 that come into effect from 30 June 2013. Given the extent of what's required in order to comply, there's not a lot of time left. Those who've yet to make much progress in getting ready would be well advised to plan for the incoming regime as soon as possible… CONTINUE READING

Business Briefs

Further changes ahead for the Employment Relations Act 2000… CONTINUE READING

Employee's Facebook fallacy… CONTINUE READING

The next issue of Commercial eSpeaking *will be published in May.*

Managing email, internet and social media

IT policies for your business

Does your company have an information technology (IT) policy? If so, when did you last update it and do your employees know it exists? This article looks at the pros and cons of your employees' internet access and what you can do to develop a policy around this.

Benefits and pitfalls

Do you provide your employees with portable devices such as iPhones, iPads, Blackberries or laptops? Do you allow your employees to access your business' network using their own portable devices? Does your IT policy adequately address the security risks arising from your employees using portable devices?

We have all heard or read of horror stories about emails written in anger and sent in haste (occasionally these end up plastered across the front page of the *New Zealand Herald*). Does your IT policy set out what is and what isn't acceptable when sending internal and external communications (including emails, texts and communications on letterhead)?

Social media sites such as Facebook, Twitter, YouTube, Pinterest and LinkedIn, amongst others, provide a myriad of marketing and networking opportunities for some businesses. Various issues can arise, however, from employees' misuse of company email, internet and social media; these could include:

» Loss of productivity
» Increased internet connection costs
» Reduction of internet speed due to high use/downloading which can affect business efficiency
» Inadvertent or intentional disclosure of confidential and/or commercially sensitive information
» Damage to your business' reputation as a result of negative comments made by employees in emails or on social media sites, and
» Allegations of bullying or harassment as a result of derogatory comments posted on social media sites by one employee about another employee.

What does a good IT policy contain?

A good policy will:

» State your business' position on your employees' personal use of work email, work devices such as computers and smart phones, internet and social media sites stipulating what level of personal use (if any) is acceptable
» Set out the types of behaviour which are deemed unacceptable, for instance, making intimidating or derogatory comments about other employees or clients, or disclosing confidential information
» Address security risks, for example, the use and disclosure of passwords, and protection of confidential information
» Confirm that your business owns any equipment/portable devices provided to employees and all information contained on them
» Advise whether your employees can access your business network via their own portable devices/home computers and, if so, the limitations you wish to place around that
» Set out the steps you take to monitor your employees' business and personal use of work email, work devices such as computers and smart phones, and their internet use. If you allow employees to access your network via personal devices then you should stipulate the steps you can take to monitor their use of personal devices to do that
» Specify the extent to which (if at all) it's acceptable for employees to refer to your business or other employees in blogs or on social media sites. Point out to employees that information posted on social media sites may not be private
» If you require employees to maintain company blogs, or social media sites, set guidelines for the type of content that's appropriate, and
» State what steps may be taken if an employee breaches your IT policy.

The key to any good policy is that it should reflect the culture of your business, should be easy to understand and accessible to all your employees.

The start of the year provides a good opportunity for all businesses to review, update or implement an enduring and robust IT policy. A good policy can be proactively used to manage risk while maximising the benefits that email, portable devices, the internet and social media can deliver to your business. ■

« BACK

Anti-Money Laundering Deadline Looms

Five months remain to get organised

One of the key items on this year's 'to do' list for all affected businesses will be getting ready for the main provisions of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 that come into effect from 30 June 2013. Given the extent of what's required in order to comply, there's not a lot of time left. Those who've yet to make much progress in getting ready would be well advised to plan for the incoming regime as soon as possible.

AML/CFT is an issue that New Zealand has paid some attention to over the years, but just not enough. It's big business internationally. The International Monetary Fund and World Bank estimate that US$2 trillion to US$3 trillion is laundered around the world each year. Regulators aren't afraid to take action and impose substantial penalties for failing to comply with AML/CFT laws. For example, global bank HSBC has been under investigation over allegedly allowing clients to transfer potentially illicit funds from countries such as Mexico, Iran and Syria. Late last year the bank agreed to pay US$1.92 billion in fines to US authorities as a result of those investigations and, as part of its settlement, will be subject to independent monitoring and assessment against various measures directed at improving the bank's structure, controls and procedures.

New Zealand's regime

International audits have revealed significant deficiencies in New Zealand's AML/CFT regime. The Act is intended to address a number of these deficiencies. If we don't get it right, credit ratings and trade relationships with other countries could be negatively affected, which will ultimately hurt us all directly or indirectly.

So, who does the Act apply to? The Act applies to 'reporting entities', a term which includes banks, life insurers, finance companies, building societies, credit unions, issuers of securities, trustee companies, futures dealers, brokers, certain financial advisers, casinos, money service businesses, those involved in financial leasing, safe deposit businesses – the list goes on. There are a range of exclusions and exemptions for businesses that might otherwise be caught, such as accommodation providers that provide guests with safety deposit boxes, accountants, real estate agents, pawn brokers and lawyers.

Reporting entities will need:

- A written risk assessment of the money laundering and financing of terrorism that could be expected in their business
- An AML/CFT programme that includes procedures to detect, deter, manage and mitigate money laundering and the financing of terrorism
- A compliance officer appointed to administer and maintain the AML/CFT programme
- Customer due diligence processes based on their risk assessment including customer identification and verification of identity, and
- Suspicious transaction reporting, record-keeping, auditing and annual reporting systems and processes.

Guidelines have been issued

The regulatory bodies that are responsible for supervising the new regime (the Reserve Bank of New Zealand, the Financial Markets Authority and the Department of Internal Affairs) have issued guidelines on various topics to assist businesses to comply with the new regime. The topics covered so far include points of interpretation in determining whether a business is a 'reporting entity' and therefore caught by the Act, the required risk assessment and AML/CFT programme, as well as the territorial scope of the Act (including the extent to which it applies to overseas entities).

For customers of reporting entities the impact of the Act will largely be felt through the customer due diligence that will need to be done on them. This will generally involve customers having to provide more information which, in some cases, will include needing to provide information on the source of funds and wealth. Trusts in particular will come under close scrutiny, as they can be an easy way to hide the beneficial ownership of funds.

For reporting entities that don't comply with the Act, the consequences can be significant. The Act provides for a range of sanctions for non-compliance, ranging from formal warnings to injunctions, substantial fines and imprisonment. ■

« BACK

Business Briefs

Further changes ahead for the Employment Relations Act 2000

Looking at the year ahead, we're likely to see further reforms to the Employment Relations Act 2000, with the proposed changes anticipated to come into effect in the second half of the year.

One area of the proposed reforms aims to further clarify Part 6A of the Act, which deals with 'vulnerable workers' whose work is affected by restructuring. The proposed changes include:

» Exempting incoming employers with fewer than 20 employees from complying with Part 6A
» Requiring outgoing employers to forward individual employee information to the incoming employer
» Detailing a process to help outgoing and incoming employers to agree how to apportion accrued service-related entitlements of employees, and
» Adding additional penalties and compliance orders for non-compliance with Part 6A.

Amendments to the collective bargaining regime are also expected, including changes to:

» Empower the Employment Relations Authority to declare the end of collective bargaining in certain circumstances
» Allow employers to opt-out of multi-employer bargaining
» Allow partial pay reductions in cases of partial strike action, and
» Remove the requirement for non-union members to be employed under the terms and conditions of a collective agreement (where one is in force which covers their work) for the first 30 days of employment.

Other changes include amending the duty of good faith in section 4 to align it more closely with the privacy principles in the Privacy Act 1983, and extending the right to request flexible working arrangements to all employees, from their first day of employment.

More details on the proposed changes can be found at www.dol.govt.nz ■

Employee's Facebook fallacy

Social networking forums have become the modus operandi of connecting, meeting and communicating for billions of people worldwide. Employees, however, need to realise that what is said in a supposedly private setting online often isn't as private as intended, as has been highlighted in the recent case of *Taiapa v Te Runanga o Turanganui A Kiwa*[1].

After requesting one week's leave without pay to attend a sporting championship and being granted only three days by his employer, Mr Taiapa reported in sick claiming he had damaged his calf muscle and was unfit for work. Regrettably for Mr Taiapa, a colleague saw him leaving town with his family and his employer became aware of a photograph on Facebook showing Mr Taiapa smiling and giving the thumbs up with 'a large female sitting on his knee'.

After an investigation and based on a number of factors, Mr Taiapa was dismissed for serious misconduct by dishonestly taking sick leave. The Employment Relations Authority concluded it was open to a fair and reasonable employer to view Mr Taiapa's actions as dishonest and that they undermined the necessary trust and confidence required in the employment relationship. ■

1 [2012] NZERA Auckland 252