COLEMAN GREIG
LAWYERS

Employment Law Update

November 2018

How Your Business can Protect Confidential Information From Departing Employees

Employment relationships are just like any other relationship: the only certainty is that they will eventually come to an end.

One unfortunate reality is that departing employees often pose the greatest risk to the future goodwill of a business, as they have had the opportunity to form relationships with the client base and supplier network. Similarly, employees will often have had widespread access to commercially sensitive documents and information, and have received training on how best to exploit it, at least for the benefit of the company.

One common way for businesses to try to protect their goodwill and prevent former employees from either poaching clients or setting up businesses in competition, is to include broad confidentiality terms and restraint of trade clauses in their contracts of employment.

Another unfortunate reality is that the most common obstacles faced by employers when seeking to enforce post-employment obligations are self-inflicted, usually coming as a result of a lack of evidence caused by poor planning and administrative oversights.

Reasonably drafted confidentiality and restraint of trade terms can be extremely effective, however courts will be reluctant to make orders to enforce contractual restraints if the company cannot demonstrate that the contract was properly entered into, and that the employee, through their conduct in breach of the contract, poses a genuine risk to a legitimate interest of the company. For more information on this, please see our Plain English Guide to Post-Employment Restraints of Trade & Protection of Confidential Information.

With that in mind, businesses need to plan for the inevitable employee break-up from day one of their time with the company, and there are a few simple steps that businesses can take to give their contracts the best chance of being enforceable if their staff do run off and try to take the business with them.

Risk Management: From Day One

Obtain professional legal advice with regard to the employment contract. Restraint of trade terms can be particularly tricky to navigate, and will be closely scrutinised by a court. Be careful of using templates, as restraint terms should be tailored to each employee.

Ensure that a signed copy of the employee's contract is scanned and saved to a dedicated location on the company's computer system. A signed contract is the best evidence that an employer can have in proving to a court that an employee did agree to be bound to their post-employment obligations. Without a signed contract, it is possible that an application to enforce a restraint of trade term might be dismissed.

A couple of recent examples from my own experience illustrate just how easily this problem can occur, and similarly, how easily these issues could be avoided:

1. The company issues the contract to the employee via email and the employee turns up to work without returning a signed copy. The company do not have a follow-up procedure in place.
2. The company is attempting to enforce post-employment obligations against an employee who commenced with the company 10 years earlier. When employee started with the company, the responsibility for storing employment contracts had been given to an individual administrative officer who is no longer employed by the company. Now, nobody knows where the contracts were previously kept.

How Your Business can Protect Confidential Information From Departing Employees cont.

It is critical that employers have and maintain a comprehensive workplace surveillance policy.

Workplace surveillance by a company is largely prohibited throughout NSW and ACT unless the company has a policy in place which explains:

1. the nature of any surveillance being carried out; and
2. the purpose for which the surveillance may be used.

In the context of enforcing post-employment obligations, evidence obtained by an employer through unlawful surveillance, i.e. without a proper policy in place (such as evidence of emailing documents to themselves or secretly contacting customers) is likely to be inadmissible in court proceedings. Carrying out unlawful workplace surveillance may also attract civil, or potentially criminal penalties.

Businesses should recognise that even if they are told not to, employees will use their personal devices for work, unless they are given an alternative. Allowing staff to use their own devices can save a company money, but does also create risk. Providing staff with a company phone or laptop comes at a cost, but can have a number of potential benefits with regard to the protection of confidential information.

As an example, many people can and do access their company email account from their phone. Senior employees, and technical or sales staff will regularly send and receive commercially sensitive information via email. If staff are allowed to use their personal devices to access their company email accounts, company documents sent as attachments will find their way into personal cloud storage services such as Dropbox, Google Drive or iCloud. Another problem is that staff will use their personal phones to communicate with clients. Once an employee leaves the company, their contacts and text messages will go with them.

A company issued device on the other hand:

1. can be configured to control access to the company network and mail server;
2. can be monitored remotely to identify suspicious activity; and
3. belongs to the company and therefore the device, and the data stored on it belongs to the company and must be returned when the employee leaves.

It is important to maintain strict IT security with proper controls, particularly over sensitive business information. Similarly, your company should make sure to regularly back-up emails, document management and accounting systems, and use continual monitoring of email and data usage.

It is wise for businesses that utilise cloud storage services not to authorise staff to use their personal accounts, and instead, to consider setting up a corporate account and providing individual user access credentials for each staff member. This way, when a staff member does leave, their access to the storage account can be removed by the company.

Some cloud storage accounts do contain logs which can be useful in identifying download activity, as well as any devices and IP addresses that have connected to the account. These logs often provide useful evidence of misappropriation of confidential information.

How Your Business can Protect Confidential Information From Departing Employees cont.

The Notice Period

Whether an employee resigns, or is terminated, the notice period can be a risky time for businesses.

Departing employees tend to be looking forward to their next positions, thus their focus and priorities often shift from looking after their employer's interests, to taking care of their own. The notice period is also the most likely time that an employee will attempt to steal company property and documents. For that reason, businesses need to manage the transition process carefully in order to get the most out of departing employees, while also protecting themselves from risk.

What are some simple steps that companies can take during the notice period?

Take some time to consider whether there is any actual benefit to the company in having the employee serve out their notice period in the office. It may be safer for the business if the employee is directed to serve out their notice period from home, or even to simply offer them an early release.

Prepare a termination checklist for the employee that includes, amongst other things, the following steps. Keep in mind that it is just as important to allocate a person to complete the checklist, in order to ensure that everything is ticked off sufficiently:

- A review by the employee's manager looking at the status of their current work, including any critical dates for the completion of tasks;
- Updating customer and supplier records to ensure that all relevant contact details are up to date;
- A calculation of monies that may be owed (for example study expenses or equipment purchased under a salary sacrifice arrangement), as well as calculating any accrued entitlements (including superannuation) up to and including the date of termination;
- Identifying all services and systems used by the employee, in order to manage the removal of any access to those services and systems; and
- The return of all company property in the employee's possession, including any documents.

Prepare a letter that clearly communicates to the employee:

- The last date they are required to attend work;
- Any specific tasks they are expected to complete;
- A list of company property that is to be returned, including a reminder that property includes documents and information; and
- When and where they are required to return all company property.

You may also include in the letter a short statement reminding the employee of their confidentiality obligations, as well as any contractual post-employment restraints (if applicable).

Above all, Coleman Greig strongly suggests seeking legal advice, especially in the case of employees who are leaving to go to a competitor.

How Your Business can Protect Confidential Information From Departing Employees cont.

Termination Day

Making a clean break and preserving data

Firstly, it is important to always conduct an exit interview with the departing employee, and in turn, to have the employee sign a declaration stating that they have returned all company property that was in their possession. Be sure to make an official internal note of the interview in case there is ever a discrepancy in the future. Either during, or immediately prior to this exit interview taking place, make sure to cut off the employee's access to any company IT services and/or accounts, and be equally careful to change all passwords used by the employee to access company services.

Save and preserve a complete copy of the employee's mailbox, making sure to include their calendar and any calendar notes.

If the employee has used a company issued computer and/or phone for work, consider sending the device to a forensic IT specialist to conduct a basic review of the device to check for abnormal activity.

Whilst this is not necessarily a crucial step in every case, no harm can come from taking a cautious approach to an employee's departure.

What should you do if you suspect that an employee has stolen company data, or is working in breach of a contractual restraint of trade term?

Try to secure any electronic devices that were previously used by the employee prior to them leaving by locking them in a secure place. It is important not to attempt any sort of examination of the employee's devices without professional assistance.

Collate relevant documents:

- Employment contract(s);
- Termination or resignation letters;
- Exit interview documents;
- Related company policies, such as workplace surveillance, use of electronic devices, and confidentiality; and
- Any documented evidence of a breach, such as evidence of copying data and suspicious emails, or other communications with customers and suppliers.

It is also important for companies to review all current and future business opportunities which the employee in question may seek to exploit, and to prepare a detailed rundown of any relevant information.

Seek urgent legal advice! Any delay by a company may be viewed by a court as evidence that there is no genuine business risk to protect, and the court may in turn dismiss a case on that basis alone.

Common pitfalls for employers

From experience, the most common obstacles faced by employers when seeking to enforce post-employment obligations are self-inflicted. These are:

- Having poorly worded contracts, usually as a result of employers preparing their own employment contracts without seeking legal advice;

How Your Business can Protect Confidential Information From Departing Employees cont.

- Failing to keep signed copies of employment contracts;
- Providing staff with access to sensitive information without monitoring that access or maintaining controls over how that information can be copied or sent;
- Not maintaining a workplace surveillance policy;
- Failing to act quickly once they become aware of a potential breach; and
- Compromising the integrity of key evidence by attempting to examine electronic devices themselves.

To quote Nigel Carson from KordaMentha Forensic, "every computer contact leaves a digital trace". It truly is important to take heed of the fact that in an environment where the best evidence usually wins, conducting inexpert investigations can be a self-defeating exercise.

Of course, all of these pitfalls are easily avoidable with a little bit of advance planning, disciplined business management and legal advice.

Finally, we all recognise that in 2018 filing cabinets and ledgers are pretty much a thing of the past. Similarly, I suggest that it is also time to acknowledge the fact that the "IT guy" and the "mate of the boss who's a bit of a tech-head" have likewise become redundant. Virtually all business activity is conducted electronically through computer systems, so regardless of how small a company may be, the IT system is often the most important piece of commercial infrastructure that they have.

A professionally managed IT system using up to date hardware is not just good for business, it will also save you certain grief in the future if you need to rely on it to recover data or gather evidence for use in legal proceedings.

How can Coleman Greig help your business to protect its confidential information?

Coleman Greig's employment team can assist businesses at every stage of the employment life-cycle. Our lawyers are able to provide expert advice on the preparation and implementation of internal policies and procedures, drafting contracts and agreements, risk identification and management, and enforcement of post-employment obligations including litigation to prevent misuse of confidential information, and to enforce contractual restraints of trade.

Please bear in mind that whilst Coleman Greig's Employment Law team can provide legal advice on risk management and the protection of confidential information, we don't manage IT systems. I would urge any business with an IT system currently serviced by the "IT guy" to seek professional advice from a reputable company!

If you have a query regarding any of the information found in this article on protecting confidential information, please don't hesitate to get in touch with:

Dominic Russell, Senior Associate
Phone: +61 2 9895 9295
Email: drussell@colemangreig.com.au

Unfair Dismissal and Technology: Terminated via Text, Email or Facebook Messenger

Calling a meeting to inform an employee that their employment is being terminated is rarely a comfortable experience, so it is unsurprising that some employers look to skip the meeting altogether, and instead opt for one of the many digital communicative tools that have worked their way into modern life. This is a risky approach, with unfair dismissal being cited in a number of cases involving technology, as a number of recent examples have shown.

In the recent case of Cachia v Scobel Pty Ltd, the employer (a small business with fewer than 15 employees), applied the Small Business Fair Dismissal Code, in what the commission found was a robust and thorough manner, giving the employee procedural fairness before termination. Deputy President Sams had one criticism of the process, which was that the termination was communicated by a late night email.

Deputy President Sams found that the termination was fully justified, as the employee did legitimately pose a threat to other employees. With this said, he was not impressed by the email dismissal, saying:

"I do not consider that informing an employee of their dismissal by phone, text or email to be an appropriate means of conveying a decision which has such serious ramifications for an employee. As there had already been one meeting with [the employee] I can see no reason why a further meeting could not have been organised for the purpose of explaining [the company's] decision and discussing the termination arrangements."

While the code did not include any requirement that the dismissal decision must be made in person, Deputy President Sams commented that:

"It would only be in rare circumstances that a decision to dismiss an employee should not be conveyed in person. For example, it may be necessary where the employer believes a dismissed employee might be a threat to the safety of his/her employees or because the employee expressly did not want a "face to face" meeting to hear the outcome of any disciplinary process. To do otherwise is unnecessarily callous.

Even in circumstances where email or electronic communications are ordinarily used, the advice of termination of employment is a matter of such significance that basic human dignity requires that dismissal be conveyed personally with arrangements for the presence of a support person and documentary confirmation."

I suggest that employers bear these words in mind, especially under circumstances where utilising a potentially less confronting method of communication is tempting.

It is also relevant to note that the use of these remote methods of communication can sometimes lead to conversations getting quite out of hand. In the recent case of Morris v Alphaeus Hair Salon, where an employee was terminated during a late night Facebook Messenger conversation between a hairdresser and the owner of the salon where she worked, which started as a normal conversation but quickly spiralled out of control.

Unfair Dismissal and Technology: Terminated via Text, Email or Facebook Messenger cont.

In this case, the owner and the employee had frequently communicated via Facebook Messenger, although in this particular instance the conversation went as follows:

a) The owner messaged to enquire whether the hairdresser had a morning appointment. When the employee did not reply immediately (she said her phone battery had died while she was fixing Christmas lights), the employer sent further messages saying "I will not take silence anymore", and that she had to decide whether she was with or against him.

The employer continued by threatening to 'sever' her as he had done to others;

b) The owner said: 'Just fixed your detrimental situation with the client you destroyed her hair!' and 'You are not in control I am girl.'

c) The owner ordered the hairdresser to cut ties with former colleagues and said 'I've been shown a vision of you leaving me!'

d) The hairdresser claimed that she was stressed out, and that she would not come to work the following day;

e) The owner said 'Good luck in your new job if you can find one, you won't given my presence. I will cut you from my fold'.

f) The hairdresser then messaged the owner to say that she'd quit and did not need his luck.

g) The owner then issued a further diatribe in messages, including threatening to destroy the hairdresser and break her bones.

It was not apparent to the commissioner whether either party was lacking in sobriety at the time.

As the hairdresser's message stating that she had quit had followed on from the salon owner's statement relating to her getting another job, the commissioner decided that it was a case of unfair dismissal, as the termination had been instigated by the employer, and that the salon owner had failed to provide the hairdresser with a reason. Similarly, by using Facebook Messenger for the conversation, it was decided that the owner had failed to provide a proper opportunity for the employee to respond.

The owner's 'reasons' for the employee's termination seemed to consist of nothing more than a conspiracy theory, which were grounds for unfair dismissal, and the employee was subsequently awarded compensation amounting to four weeks' salary, to cover the period up until she found new employment.

These two cases help to illustrate the danger of using remote methods of communication for termination and pre-termination conversations (as opposed to direct personal meetings). Communication of a final decision via remote communication may be in order if the previous process has been conducted in person and with a proper amount of detail, but not if a there are matters of substance to be discussed, and definitely not if the remote conversation turns to anger, and degenerates to termination without proper process.

Unfair Dismissal and Technology: Terminated via Text, Email or Facebook Messenger cont.

As an experienced employment lawyer, I suggest that the old wisdom of not terminating in anger is still good advice, even when using new technology!

If your organisation is currently facing issues relating to employee performance, conduct management, employee terminations and/or risk management when it comes to unfair dismissal, please don't hesitate to get in contact with:

Stephen Booth, Principal
Phone: +61 2 9895 9222
Email: sbooth@colemangreig.com.au

Romance in the Workplace - Yay or nay?

Unsurprisingly, there is a wide range of useful information available to assist organisations in preventing and (should the need arise) addressing unwanted sexual advances, or indeed any type of inappropriate conduct in the workplace. It therefore follows that many workplaces will already be equipped with relevant policies covering sexual harassment, and subsequent procedures to deal with such issues - at least to some extent.

If your workplace is without such a policy, I would suggest that you make implementing one an immediate priority!

This is particularly important at the moment ,given the current spotlight on sexual harassment following the recent announcement by Sex Discrimination Commissioner Kate Jenkins of the national inquiry into sexual harassment in Australian workplaces, which will focus on identifying examples of good practice and making recommendations for change.

But what about consensual, or reciprocated romantic relationships? Do you have a Relationships in the Workplace Policy covering those? Have you considered whether this is even something that your workplace should have a policy on - or are you appalled by the suggestion?

Why you need a Relationships in the Workplace Policy

Whilst the idea of having such a policy in your workplace may initially conjure thoughts of intruding on the private lives of your employees (thus inherently defining it as a matter of no relevance to the workplace), the reality is that some romantic relationships do have the potential to impact on the workplace.

Below are a few relevant examples that I suggest taking into account when deciding if your organisation needs to implement a Relationships in the Workplace Policy:

- If a co-worker were to witness inappropriate behaviour by a couple, it may lead to them feeling uncomfortable, and result in a sexual harassment claim;
- Romance between a manager and their subordinate could be viewed as a conflict of interest, and could potentially give rise to favouritism. Even where the manager does not exercise their power to the benefit of the subordinate, there may be a perceived bias given the relationship. In turn, the relationship is likely to undermine the impartiality of all of the manager's decisions; and
- Whether the relationship is between a manager and their subordinate, or simply between two co-workers, questions relating to the productivity of those in the relationship (are likely to come in to question - whether justified or no). This is particularly relevant if they participate in closed door meetings or discussions out of the ear shot of others, which may not be uncommon for other employees in the workplace, and had it not been for the romantic relationship would not be questioned.

What should your Relationships in the Workplace Policy look like?

It is important to remember that your overall objective should never be to intrude on the private lives of your employees - rather, the purpose of any 'Workplace Relationship Policy' should be to educate your employees on:

a) why you as the employer may need to know about the relationship; and

b) how the relationship can be managed in the best interests of all workplace stakeholders.

Romance in the Workplace - Yay or nay? cont.

The above points should be made very clear in the opening of the policy.

Ideally, your Relationships in the Workplace Policy will also clearly state:

- at what point your employees are required to disclose a relationship, with specific directions on who they are to disclose the relationship to;
- that where applicable, and if considered appropriate, the confidential nature of the relationship will be maintained;
- the possible consequences of failing to disclose the relationship when required (for example, any relevant disciplinary action);
- examples of when the relationship may become a concern for the employer;
- examples of when a conflict of interest may arise;
- examples of what measures may be put in place in order to address any employer concerns, or perceived conflicts of interest (e.g. changing reporting lines); and
- examples of unacceptable behaviour/interactions between the couple (e.g. displays of public affection).

Given that some relationships may be more of a concern than others due to their likely impact on the workplace (typically, the more senior the employees are, the higher the chance of conflict, and in turn, the potential that it will impact the workplace), the best thing for your organisation to do is implement a policy that allows you to manage each relationship that is brought to your attention on a case by case basis and not adopt a one size fits all approach for dealing with relationships.

Coleman Greig Lawyers are experts in Employment Law & WHS. We can assist your business in navigating the complex area of romantic relationships in the workplace and help you put policies in place to mitigate any potential risks to your business.

We are also currently undertaking the White Ribbon Australia Workplace Accreditation Program, and takes a zero-tolerance stance with regard to any and all forms of violence against women. If you are concerned that you may be a victim of domestic violence, we urge you to seek help via the White Ribbon Australia website.

For more information contact:

Anna Ford, Senior Associate
Phone: +61 2 9895 9233
Email: aford@colemangreig.com.au