A–Z OF EMPLOYING

Employees and Technology

SUPPORTING, FACILITATING & REPRESENTING BUSINESS

BusinessCentral

This is only a guide. It should not be a substitute for professional advice.

Please seek advice from our AdviceLine Team if you require specific assistance.

Contents

Introduction

Technology plays an important role in all aspects of business, from the way companies communicate internally and externally to how attendance is monitored. It has become an integral part of New Zealand business. The rules relating to different types of technology are located within both legislation and case law. Employers should comply with the relevant law to reduce the likelihood of an employee having a successful claim against the company at a later date.

This guide provides a summary of the law in relation to technology in the workplace. It also outlines some issues that employers may encounter in dealing with technology and suggests factors that a business may consider when creating a policy or procedure to deal with the use and misuse of technology.

For more in-depth information about any of the enclosed topics, please refer to the relevant A-Z Guide or contact Adviceline.

Computers

Computers have become so common in the workplace such that it is vital for employers to have clear guidelines around their use. This avoids any confusion as to what is acceptable and unacceptable use of the company's computer network. Policies should be enforced consistently across all employees as consistency is an important factor when it comes to disciplining an employee for a breach.

Property rights

Companies have a right to protect their property from harm or damage caused by employees or people outside the organisation. Property rights can exist in a range of areas in the workplace including:

- Hardware
- Software
- Copyright
- Trade Marks
- Patents
- Information
- Licenses and contracts

It is recommended that you consider what property is at risk and therefore requires protection. Protection can range from limiting access to certain computers or files, to provisions within employment agreements that make employees responsible for indemnifying the company for any physical or actual damage to property and/or financial losses. Technology policies should clearly outline what constitutes acceptable and unacceptable use of the company's hardware and software. Policies should also detail what action the company will take if the policy is breached.

The level of protection or preventative measures that you take to avoid a threat to your property rights depends on your individual needs. Electronic security can be used to prevent incoming and outgoing illicit or illegal materials. Files can be password protected to limit access to confidential material. Alternatively, restrictions can be placed on your computer network to limit which employees have the ability to download files and internet access can be password protected.

You might consider discussing your company's individual needs with an IT specialist to ensure that the computer network is secure and protected

Employment rights

An employer has the right to prescribe the levels of conduct expected of their employees. This needs to be weighed against employees' expectations that their employer will preserve their right to privacy, fair treatment and safety (see 'harassment' below).

Employees owe a duty of fidelity and confidentiality to their employer. Whilst these duties can be express terms in an employment agreement they are also implied terms in all employment agreements. In short, the duty of fidelity is that of loyalty and reflects both the employers' and employees' obligations to act towards one another in good faith. The duty of confidentiality prevents employees from using confidential information to advance their personal interests to the detriment of his or her employer.

Consideration of these duties raises issues concerning how employees use company computers. Employers could consider regulating the transfer of confidential company information via software and hardware. Policies could also address whether the use of personal USBs or other storage devices in the workplace is acceptable. Additionally, it may be useful to have a policy that deals with the monitoring and/or limiting of emails that transfer company information.

You might also consider the possible impact of allowing employees to use their personal laptop (whether it be for personal or professional use) on the company's computer network. If an employer provides a laptop for employees to use, the employer will have greater control over the information stored on it when the employee leaves.

Monitoring computer use

There are ways to limit the misuse of an employer's computer network without requiring monitoring, including: having a policy with clear expectations and limiting access to threatening or time wasting websites. However, there may be situations where an employer needs to monitor an employee's computer usage or email use. You must have a compelling reason for monitoring an employee's computer or email use.

It is important for a technology policy to state that computer use is monitored and it is advisable to have signage to reiterate this. The inclusion of signage on a computer which states that an employee's usage is monitored serves as a constant reminder of the policy and also acts as a deterrent.

The Privacy Commissioner released a case note (Case note 229558 [2012] NZ PrivCmr 1) in response to an employee's complaint about their employer using key stroke software to monitor the employee's computer usage. The Privacy Commissioner noted that accessing information directly from the employee's computer was not a breach of the Privacy Act 1993 because the employer had a clear policy in place. However, using key stroke technology to collect the employee's private information and then using the information gained to access the employee's personal email was a clear breach of the Privacy Act 1993.

Computers and reputation

It is recommended that employers consider how the misuse of technology in the workplace could affect their business's reputation. A serious breach of a company's IT security or negative comments made about the company on social networking sites can adversely affect your reputation. Additionally, if someone within your organisation were to make offensive or unauthorised comments via the company's email system, those undesirable comments could possibly be attributed to the company. This may negatively affect how other organisations or people do business with you.

You might consider how your employees, and the company as a whole, interact with people and businesses outside your company. A policy can be drafted to manage internal and external communications to ensure that the company's image and reputation remains intact. The potential negative impact of social media is discussed in more detail below.

Computers and harassment

You have an obligation to provide a safe workplace for your employees. Harassment is not limited to verbal communication; it can occur through email or text as well. A technology policy could state that harassment in any form will not be tolerated in the workplace. Employers should also consider whether the use of work email for the purpose of harassment can also be construed as misuse or unauthorised use of electronic mail and the employer's time.

Harassment via email may lead you to monitor emails for content and/or to block certain email addresses. Emails may be "quarantined" if they contain certain trigger words that the employer considers inappropriate language for work emails. The employee would then receive notification that an email, either outgoing or incoming, had been quarantined with the option of asking for it to be released if the employee believes it is work related. An email policy should stipulate that emails may be monitored for content. The policy should also differentiate between work-related emails and personal emails, and provide guidelines as to what constitutes an appropriate amount of personal use of a work email.

You can consider including guidelines within the policy as to how employees should respond to emails that are believed to be racist, sexist, bullying or harassment. The policy could outline how employees should respond if they have concerns about an email they have received. The employer's response will depend on whether the email was sent by an internal or external source. The policy can make it very clear that sending inappropriate emails from a company email address is not acceptable and may result in disciplinary action. It could also provide that forwarding an inappropriate email to other employees or external email addresses may breach the company's email policy and result in disciplinary action.

Limiting access to websites

It is advisable that the company's technology policy makes it clear that computer use may be monitored. The policy could address whether personal use of the work computer is acceptable and, if so, to what extent. If personal use is deemed acceptable, employers could consider whether access will be restricted to certain websites or unrestricted. Employers could also consider whether use will be monitored in order to determine whether it is at an acceptable level.

A computer policy can address an employees' ability to access certain "time wasting" websites. The idea being that, as an employee is at work to do work for the employer, they should not be browsing the internet for personal reasons. Employers have the option of limiting access during work time, for example from 8am to 6pm. Outside of these hours the websites may be accessible, within reason.

Employers should ensure that the policy suits the operational environment of the organisation. For example, there is no point in having a strict 'no personal use' policy if it is not going to be enforced.

Providing employees with a laptop

Employers who provide their employees with laptops can stipulate within the policy, how laptop use will be monitored. Policies should outline whether the laptop is only to be used for business purposes or if personal use is permitted, to what extent. Will data cards be provided to employees with laptops? If so, how will that be administered?

It is recommended that you clearly outline in the employment agreement or policies that a laptop provided by the company belongs to the company and not the employee. You might consider how you will deal with the liability for replacement if the laptop is damaged or stolen as a consequence of negligence, carelessness and/or sabotage.

Employment agreements can also make it clear that the laptop is to be returned to the company at the end of the employment relationship. Further, agreements should also provide for the return of a laptop where an employee is on leave, not performing the role, or at the employer's discretion.

Employers should consider what action will be taken if the laptop is not returned and whether a deductions clause could be included in your employment agreements as a safeguard. These are factors that should be considered when providing a laptop to an employee. If they are dealt with in a policy or employment agreement then if/when an issue arises, both parties know where they stand.

Cloud Computing

Cloud computing can come in many different forms. It generally refers to the sending of information outside your business for storage, management and processing. It can involve the storage of information with a different company and on servers overseas and can include having a third party process the information – including, for example, your payroll.

If any of the information that you send outside your business is considered to be your employee's personal information, it will be important to consider your obligations under the Privacy Act 1993.

Under the Privacy Act 1993, personal information is defined as "information about an identifiable individual". The Privacy Commissioner notes this includes "People's names, contact details, financial, health, purchase records: anything that you can look at and say "this is about an identifiable person".

Among other things, the Privacy Act 1993 requires that personal information remains accessible, as employees have the right to access personal information that you hold about them and the ability to correct it if the information is incorrect. Furthermore, under the Privacy Act 1993 you have an obligation to ensure that the information is kept secure and not subject to unauthorised access or disclosure. Consequently, it is important to consider how the personal information might be encrypted and what terms will be included in your commercial agreement with your cloud provider to ensure that the information is kept secure.

The Privacy Commissioner has released a Cloud Computing Guide which contains further detailed information about managing privacy in the cloud. The Guide is available at www.privacy.org.nz.

In addition to the Privacy Act obligations, there are obligations under the Employment Relations Act 2000 and the Holidays Act 2003 to retain records and ensure that they remain immediately accessible. It is important that employers comply with these obligations, even if the records are stored on the cloud.

Cellphones

The use of cellphones within a company is a great way to remain in contact with staff members who may not spend a lot of time in the office. However, cellphones can also be a source of distraction and decreased productivity. Creating a cellphone policy to manage the use of cellphones in the workplace is important for privacy, security and health and safety reasons.

You should consider whether cellphone use in the workplace is necessary and, if so, what restrictions might be in place to limit the negative impacts on the business. A policy can be created to set out clear guidelines as to what constitutes unacceptable use of a work or personal cellphone in the workplace and whether disciplinary action may result.

Use of a work-allocated cellphone

Where employers provide their staff with cellphones, it is usually on the condition that the employee is contactable wherever they are throughout the employee's working day. However, employers should have realistic expectations about whether employees are required to answer work-related calls outside of work hours, during the weekend or while on holiday.

A policy could include a clause that requires any communications with clients or colleagues via cellphone to remain professional. It can also set out that confidential communications via cellphone must be conducted in a private setting where the conversation will not be overheard.

The cellphone policy could outline the extent to which the company will pay for the phone, line rental and usage. Usage may include phone calls, texts, voicemail access, internet data and other functions that may be available. If the company decides to only pay for work-related communications, the cellphone policy might outline what constitutes "work-related communications" and also how the employee will be held accountable for usage that is of a personal nature.

The policy can also discuss an employee's financial responsibility if the phone is damaged, lost, stolen or not returned upon resignation/termination. Including a deductions clause within an employee's employment agreements would provide a mechanism through which the employer may recoup the cost of the phone and/or personal usage of it.

Personal use of a work cellphone

Employers may consider the extent to which personal use of the work cellphone will be acceptable. This includes considering whether employees will be held accountable for any personal calls, texts and personal internet data usage. The policy can outline what (if at all) is an acceptable level of personal usage and how personal usage will be monitored.

The policy can also outline how an employee might be held accountable for any cellphone usage that is deemed unacceptable. If an employee is required to contribute to the charges generated as a result of their unacceptable usage, employers should consider including a deductions clause in the employee's employment agreement dealing specifically with this situation.

Personal cellphones in the workplace

Employers can consider whether or not employees will be permitted to use their personal cellphones within the workplace and what restrictions can be implemented.

While some companies may only allow employees to use their cellphones while on a break or in case of emergency, other companies may not place any restrictions on the employee's ability to use their cellphone. You can consider what restrictions are reasonable and necessary to limit the negative impact of personal cellphone use in the workplace.

You could consider not only when personal cellphone use is permissible but also what type of use. The cellphone policy can set clear guidelines as to what is and is not an acceptable use within the workplace. Such guidelines can protect the company's private or confidential materials as well as the privacy of other employees. In a security sensitive workplace, it may be appropriate to impose more stringent rules than would be appropriate in a more public workplace.

Employers should keep in mind that as technology develops so too do the functions available on a cellphone. As current cellphone models have camera, video camera, voice recorder and USB drive capabilities, employers might need consider whether or not the use of these functions in the workplace is acceptable.

Health and Safety

Cellphones have the potential to cause distraction and within certain places of work this distraction may be hazardous.

Under the Health and Safety at Work Act 2015, employers being persons conducting a business or undertaking ("PCBU") have a primary duty of care to ensure so far as is reasonably practicable the provision and maintenance of a work environment without risk to health and safety. Employers are required to eliminate risks to health and safety so far as is reasonably practicable and if they are not able to do so, minimise those risks as is reasonably practicable. With this duty in mind, employers could for instance consider banning employees from having their cellphones on them in certain areas of the workplace; for example on the factory floor.

However, you must be mindful that employees may want their cellphones to be accessible in case of an emergency. Employers could consider having a process in place for an emergency situation where an employee's family or friends may need to contact them. This process can be clearly outlined in a policy and communicated to employees so as to remove the justification for them having a cellphone on their person.

Cellphones in cars

On 1 November 2009 drivers became liable for an $80 fine and 20 demerit points if caught texting or talking on a handheld cellphone while driving.

You are required to manage hazards in the workplace and eliminate hazards so far as in reasonably practicable. An employee's "place of work" includes a vehicle in which they perform their work. It follows that driving with a cellphone is a hazard and therefore employers are required to take all reasonable and practicable steps to ensure that employees do not use a handheld cellphone while driving a company vehicle.

You must ensure that employees are aware of the law and state within your policies that driving whilst using a handheld cellphone may result in disciplinary action. Employers can also consider providing hands-free devices for company cellphones.

Privacy

Your organisation has a right to prescribe acceptable levels or standards of conduct in respect of people, the workplace, and the tools in the workplace. However, this must be weighed against the employee's right to privacy. Sometimes this means that privacy considerations collide with employment obligations.

Employers may wish to access their employees' work cellphones to investigate an allegation of misconduct or serious misconduct. It is advisable that employers first consider whether accessing the phone is necessary to substantiate the allegation. If access is necessary, you should ensure that the right to review or monitor the employee's usage of the cellphone is provided for in the company cellphone policy.

Best practice

It is important that your company has a policy that sets out clear guidelines as to what will and will not be construed as acceptable use of cellphones in the workplace. The policy should also outline what action will be taken by the company if your employee uses their work cellphone or their personal cellphone in the workplace in an unacceptable manner.

Surveillance

Surveillance in the workplace can take many forms ranging from video cameras, drug testing, vehicle searches, to Global Positioning Systems (GPS). It provides employers with the opportunity to monitor their employees and activities in the workplace. When deciding whether to conduct surveillance the benefits need to be weighed against considerations involving privacy, the implied term of mutual trust, confidence and good faith. If you are looking at implementing any form of surveillance it is important to take into account potential privacy implications and consider whether surveillance is fair and reasonable.

Privacy considerations

The Privacy Act 1993 has established 12 Information Privacy Principles which promote and protect an individual's privacy. These Principles relate to the collection, use, and disclosure of personal information. Not all of these Privacy Principles, or all of the conditions the Principles impose, are discussed in respect of surveillance. However, the following Principles are relevant to the topic of surveillance and should be taken into consideration.

Privacy principle 4

Principle 4 prescribes the manner in which personal information must be collected.

It states that an employer shall not collect personal information by:

- Unlawful means; or
- Means that are, in the circumstances of the case, either unfair, or, intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Privacy principle 3

Principle 3 imposes a number of conditions on the collection of personal information, where it is collected from the individual concerned, that an employer must comply with. The individual concerned is entitled to know that the information is being collected, and, the purpose for which the information is being collected.

The employer does not have to comply with this principle if it believes, on reasonable grounds, that:

- The individual concerned has authorised the collection; or
- The interests of the individual concerned will not be prejudiced by the collection; or
- Non-compliance is necessary to avoid prejudice to the maintenance of the law; or
- Compliance would prejudice the purposes of the collection; or
- Compliance is not reasonably practicable in the circumstances of the particular case; or
- The individual concerned will not be identifiable.

Privacy principle 10

Principle 10 places limitations on the use of personal information. If your organisation conducts any surveillance to collect personal information in connection with one purpose, the company should not use the information for any other purpose.

However, an employer does not have to comply with this principle if it believes, on reasonable grounds, that:

- The use of the information is authorised by the individual concerned; or
- Non-compliance is necessary to avoid prejudice to the maintenance of the law; or
- Non-compliance is necessary to prevent or lessen a serious and imminent threat to either public health or safety, or, the life or health of the individual concerned or another person; or
- The purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or
- The individual concerned will not be identifiable.

Closed Circuit Television (CCTV)

CCTV is a form of video surveillance. If you wish to introduce CCTV it is important to plan ahead and consider why you want to implement this form of surveillance. CCTV has many benefits and can be used as a method of protecting the security of staff and the company premises as well as monitoring incoming visitors onto the work site.

People who enter the workplace should be made aware of where the CCTV cameras are operating and signage can be installed to inform people of the camera's location. It can also be used as a way to deter employee theft as employees are aware that cameras are operating.

Policy development

Video surveillance should not be undertaken without first implementing a good policy. If you are considering installing CCTV cameras it is advisable that employees and or their representatives are consulted with before implementation, and that you ensure that the policy complies with the Privacy Act. Employees should be given opportunity to provide feedback on the draft policy and it is recommended that you communicate the rationale for implementing CCTV. Staff should be informed of the level of monitoring and why it is necessary.

Global Positioning Systems (GPS)

With the advancement of technology and GPS systems employers now have the ability to obtain very valuable information with regards to company motor vehicles. The GPS is a particularly useful device where an employer operates a fleet of company vehicles as the technology can attest to where an employee has been and provides time and speed information.

While activated, the GPS can record the following information about:

- The speed a vehicle is driven at
- Fuel consumption
- Where the vehicle has travelled
- How many stops it makes and the time involved in those stops

GPS policy development

You can consider implementing a policy with rules around company vehicle use and what information the GPS will monitor. Best practice would be for you to consult with employees before implementing the GPS system to advise them of what information will be collected and explain why the information is being collected. It is advised that the policy also states that misuse of the company vehicle, as indicated by the GPS records, may result in disciplinary action. Employers can also include guidelines in the policy as to what constitutes work use versus personal use of a company vehicle. Additionally, it could spell out the consequences of misuse of the vehicle.

Covert Recording Devices

Covert surveillance

In certain circumstances employers can conduct covert surveillance on employees, particularly if they are suspected of dishonesty, vandalism, theft or engaging in other illegal activities. In these circumstances, alerting the employee to the fact that they are being filmed may jeopardize your ability to obtain proof to substantiate the allegation. However, employers will have to justify this type of surveillance as it is more intrusive on an individual's privacy; particularly with regards to other employees who are unaware they are being filmed.

Covert surveillance should not be undertaken unless there is no alternative means of gathering the desired information. Covert surveillance should not be used for a 'fishing expedition'. You should have a specific allegation or suspicion that you are attempting to gather evidence to substantiate in order to justify undertaking covert surveillance.

If you are monitoring employees covertly, and are conducting an investigation because you are suspicious of theft or other illegal activity, you can use the information obtained through covert surveillance as evidence in potential disciplinary meetings.

In the view of the Privacy Commissioner, employers who conduct any covert surveillance should:

- Clearly record the purpose of the surveillance; and
- Conduct the surveillance only during relevant time periods; and
- Restrict the surveillance to the least amount of time possible; and
- Ensure only information relevant to the reason for the surveillance is collected; and
- Unless there are extraordinary circumstances, do not conduct any surveillance at any times or in any areas where employees would expect complete privacy i.e. in bathrooms

Covert GPS recording

Employers may be able to monitor their employees covertly by installing a GPS device into a company vehicle if they have suspicions that an employee is misusing a company vehicle in breach of company policy. You have to be able to justify using GPS to monitor an employee without their knowledge as it is more intrusive on an individual's privacy than monitoring with their knowledge.

By using GPS covertly, employers can gather information regarding the misuse of the company vehicle and potentially use the information in a disciplinary meeting.

Recording disciplinary meetings

An employer may face a situation where an employee is summoned to a disciplinary meeting to discuss an allegation of misconduct or serious misconduct and the employee covertly records the meeting. If the employee is dismissed following the meeting they may seek to use the recording as evidence that he or she was unjustifiably dismissed. In most cases, the employer will be unaware that the employee recorded the disciplinary meeting until a personal grievance has been raised. Two distinct issues arise from this situation, concerning privacy and admissibility of the recording as evidence.

Privacy

The Privacy Act 1993 ("the Act") contains 12 information privacy principles that govern the collection, storage and disclosure of personal information. Secretly tape-recording a conversation may, depending on the facts, be a breach of the Act. The principles that are directly relevant to secret tape recordings are Privacy Principles 1-4.

The effect of the Act on covert tape recordings was examined by the Court of Appeal in *Harder v Proceedings Commissioner* [2000] 3 NZLR 80. The majority of the Court found that secretly recording a telephone conversation did not breach the Act. In this case, the argument was limited to Principles 3 and 4. The Court found that secretly taping a conversation does not automatically breach Principle 3. That principle is concerned only with the collection of personal information, not the manner in which that information was collected. In this case, the Court held that it is enough that a person knows that the information is being collected, they do not have to also know how that information is being collected. The Court gave a wide interpretation of what it means to know that the information is being collected and in this case held that answering questions was enough for a person to know that information is being collected.

Applying this to the context of a disciplinary meeting, it will be hard to find that an employer did not know that the information was being collected. Disciplinary meetings are conducted in a formal setting where both parties have the right to exchange information and take note of what each party says.

Where the situation becomes tricky is with the manner in which the information is being collected. Principle 4 states that personal information shall not be collected by unlawful means, or by means that, in the circumstances of the case, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

The issue of fairness in secretly taped conversation will be determined on a case by case basis as different individual circumstances may apply. In Harder the Court stated that the primary objective of Principle 4 is to prevent people from being induced by unfair means into supplying personal information which they would not have otherwise supplied. In this case, the tape recording of a conversation between a defence lawyer and a witness for the prosecution was deemed to not be unfair. Again, this rationale can be applied to disciplinary meetings. If the meeting is conducted in a procedurally reasonable and fair manner, it is hard to conceive of situations where an employee by secretly taping the meeting, will manage to extract information from the employer which they would otherwise have not supplied.

Admissibility

Sometimes an ex-employee will attempt to introduce the secretly taped recording as evidence that he or she were unjustifiably dismissed. The question then arises whether this evidence will be admissible before the Authority or the Court.

Under section 160 of the Employment Relations Act 2000, the Authority has discretion to call for and consider any evidence or information as, in equity and good conscience, it thinks fit. The admissibility of secret tape recordings as evidence is fundamentally a question of fairness, not only to the employer but also to the employee. Thus, in *Simms v Santos Mount Eden Limited* (Unreported) AA254/03; 21 August 2003; J Wilson; an ex-employee tried to introduce tapes and transcripts of two conversations with his former employer that he had recorded in secret. The Authority commented that while recording conversations in secret may breach trust, confidence and fair dealing, to deny the ex-employee the opportunity of supporting his version of the conversation with the tape recordings could be construed as unfair to him.

Good Faith

All employment relationships contain an implied and mutual duty of trust, confidence and good faith. In some circumstances, secretly taped conversations would undermine that trust and confidence. However, each case is decided on its own merits, and what could be a breach of good faith in one case may not be so in another. As a general rule, parties in an employment relationship must be responsive and communicative towards each other. An employee who surreptitiously records a disciplinary meeting may be found to have breached the implied obligation of good faith.

Best practice

As an employer, you could include a clause in either your employment agreements or policies that deals with secret tape recordings. This may be desirable as it could act as a deterrent against such conduct. This clause could ban any covert recordings of any conversation between the employer and the employee, or the employee or any other employee of the employer. Such a clause could be further enhanced by providing for steps that the employer will take if an employee breaches this clause.

If you suspect that the employee will secretly record the disciplinary meeting, you can make your own arrangements to record the meeting and let the employee know that you will be doing so. This will negate the need for the employee to make their own copy.

If either an employee or employer wishes to record a disciplinary meeting, they can advise the other party of their intention, which eliminates the issues associated with covert recording. The party wishing to record the meeting does not need to obtain permission from the other parties to record the meeting. If a party objects to being recorded, they would need to justify their objection.

Time Keeping

Finger scanners

Finger-scanning systems are increasingly being used to keep track of when employees arrive and leave work. This is a relatively new workplace practice in New Zealand and tends to be used for clocking in and out. This system is often introduced to replace standard timesheets, which employees often fail to fill out correctly or on time.

There is some debate about whether the information collected by the scanning equipment is personal information that falls under the Privacy Act 1993. However, if the finger scan is related to a particular person in the workplace and the system has the means to identify that person, then it is likely to be viewed as personal information.

Prior to introducing a finger-scanning system into a workplace, you must ensure that the system complies with the relevant Privacy Principles. In addition, you must ensure that the system complies with any contractual provisions and ensure that you undergo a thorough consultation process with the affected parties, including unions if applicable.

Privacy principle 1

As with any collection of personal information, you must show that the collection of fingerprints is lawful and that it is necessary for the functions or activities of the business. The finger-scanning system will record the points of reference from a fingerprint. You must show that the fingerprint is collected for a lawful purpose connected with your activity and that the collection is necessary for that purpose. For example, it may be necessary to install the finger-scanning system to assist the efficient administration of your payroll. In this case, you must be able to show that the information collected through the finger-scanning system is reasonably necessary for this purpose.

Privacy principle 3

An employer must also inform the affected employees why the collection is necessary and what it will be used for. You must ensure that employees are fully aware of the reasons why you consider the system to be necessary. Since fingerprints are usually associated with criminal investigations, you must take particular care to explain to employees how the system works and what information will be collected and stored.

When proposing a finger-scanning system, you should ensure that employees have been given all the required information about the system prior to it being installed. Issues commonly arise where employees have not been fully informed about the reasons why the system is required and how it will operate. Thoroughly consulting with employees and asking for their feedback will ensure that the implementation and operation of the finger-scanning system runs as smoothly as possible.

Privacy principle 4

The finger-scanning system must not be an unfair or unreasonably intrusive method of collecting personal information. Whether the system will be considered to be unreasonably intrusive will depend upon the reasons for installing the system, the policies surrounding its use and the type of equipment involved. Usually, if you comply with Privacy principles 1 and 3, it will also comply with Privacy principle 4.

Phoning in attendance

An alternative time keeping system that some employers use is to require their employees to call when they arrive at work and when they finish work. This is commonly used where employees are required to work at different sites. If this is a requirement, then you need to draft a clear policy that explains when and how an employee is required to phone in and out. For example, this policy can outline who the employee is required to call at the beginning and the end of the day and what will happen if the employee disregards this requirement.

In addition, it may be prudent for the policy to outline your expectations when it comes to reporting employee absences. With modern technology it is very common for employees to use text messages as a way to communicate that they will not be coming in to work on a particular day. This is problematic as sometimes text messages are not received or are sent to the wrong person; therefore it is best to have a policy that requires all employees to telephone either their manager or supervisor before they are due to start work if they are sick. Having such a policy will also ensure that all employees are aware of the process and know what is expected of them.

Best practice

Prior to installing the finger-scanning system, an employer needs to make sure that there is a lawful and necessary reason for collecting personal information this way. This reason must be connected to the functions of the business. Additionally, an employer must be able to show that there is no alternative available to fulfill this function. Information about the system, how it will operate and what information will be collected needs to be provided to all employees, and any feedback received must be considered in good faith.

Having a policy that outlines the reporting requirements employees are expected to follow when they call in sick will ensure that a consistent standard is applied across the workplace. This will be useful when it comes to managing employee absences.

Social Media

Social media websites such as Facebook, Twitter, LinkedIn and online blogs affect the employer-employee relationship. Leaving aside the positive aspects that social media can have, employers need to be aware of the risks associated with the use of social media use and how it can impact their business. The risks include productivity issues, damage to business reputation and conflict between employees. Social media activities may have implications at the pre-employment stage, during employment and post-employment.

Pre-employment

Recruiters are increasingly using social media to gather information about potential employees. Issues may arise where information that cannot be lawfully considered for the purposes of recruitment are inadvertently obtained. It is advisable to refrain from gathering information that cannot have any bearing on screening candidates and could give rise to discrimination such as age, race, or sex.

During employment

All employment agreements contain implied terms that employers and employees alike must adhere to. These implied terms include confidentiality, fidelity and trust and confidence. The misuse and abuse of social media may, in some cases, breach these implied terms therefore employers may take action against employees in breach. Employment agreements may also contain specific clauses that provide employers with protection. For example, a general clause regarding employee conduct may be used to address misconduct carried out through social media.

Having a specifically formulated policy is also an effective way to address social media issues that arise during employment. These policies can be drafted broadly to address all forms of social media activity during or outside of work time, and on work or private computers. In such policies, you can include guidelines around what is considered to be appropriate social media use and outline the possible consequences of breaching the policy. Such consequences may include disciplinary action up to and including dismissal.

When considering discipline and/or dismissal in response to a policy breach, there are several factors that need to be taken into account. Both the nature of the comment and who may be able to view the comments are relevant factors to consider. If a policy on social media exists within the organisation, it is recommended that the policy is referred to when considering disciplinary action.

An employee can use social media in a way that detrimentally effects their employment without posting negative comments about their employer. In the case of *Taiapa v Te Runanga O Turanganui A Kiwa t/a Tauranga Private Training Establishment*, Mr Taiapa's summary dismissal was upheld by the Employment Court because photos he had posted on Facebook proved that he had taken sick leave without a genuine reason.

Post-employment

Post-employment conduct of an employee can have an impact on employers as former employees can post or blog negative or confidential comments about former employers and their businesses. It is best to have an express term in an employment agreement that governs post-employment conduct. Express terms must state that they survive past the end of the employment relationship in order to afford you the most protection. If there is a breach of this term then an employer may take action for penalties and/or damages.

Best practice

The New Zealand experience with social media use and employment law is relatively new and limited. Because social media use is on the rise, employers need to be aware of the potential implications it could have on their business and the employment relationship. It is recommended that you take steps to ensure risks are minimised as much as possible. Such steps include having specific clauses and policies that set rules and expectations when it comes to social media use.

Advertising Standards Authority

Employers should be aware that the Advertising Standards Authority (ASA) has held businesses accountable for their own online content and also any other user generated content directly under their control.

The ASA has released guidelines for social media advertising which are available on the ASA website. It is recommended that employees who are responsible for a business's social media be familiar with these guidelines to avoid any potential complaints.

Illegal file sharing

Sections 122A to 122U of the Copyright Act 1994 provide a regime through which copyright owners can seek enforcement of their rights against infringing file sharers. The regime came into force on 1 September 2011 and enforcement is against the internet account holder, not necessarily the particular user on the network. Therefore, it is advisable that employers closely monitor their employee's internet usage in the workplace to avoid being held liable for infringements caused by their employees.

The process

The Act's regime sets out a three-strike notification before a copyright owner can take enforcement action against an alleged illegal file sharer.

Every internet connection has an IP address (internet protocol). Copyright owners monitor peer-to-peer protocols and software to find incidents of file sharing that infringe their copyright. Through this monitoring the copyright owner will be able to identify the IP addresses which they believe are infringing their copyright. The IP address is sent by the copyright owner to the internet service provider (termed IPAP in the Act) who then matches the IP address with the internet account holder.

The internet account holder is issued with an infringement notice by the IPAP. After the first and second notice there is a 28 day 'on notice' period during which any further incidents of infringement will be recorded but will not result in another infringement notice.

After the third infringement notice is issued, the copyright owner has 35 days to bring enforcement action against the alleged infringing file sharer. Enforcement includes pursuing an order from the Copyright Tribunal for a sum up to $15,000. There is provision in the Act to seek an order from the District Court to suspend the account holder's internet for up to 6 months. However, the option to request internet suspension is not currently available.

There are provisions in the Act for challenging any notices however the account holder is the liable party, whether or not he or she was the person who actually downloaded or uploaded the infringing file. The account holder will get infringement notices and be fined by the Copyright Tribunal.

Impact on businesses

The internet account holder will be held accountable for any infringement occurring on their internet connection, regardless of whether the account holder participated in a file sharing infringement. Therefore, a company may be held responsible for any illegal file sharing done through their internet connection, whether or not the company was aware of it.

Any business that allows its employees, contractors, guests, patrons or others to use its internet might consider what preventative measures may be appropriate to reduce the risk of their becoming accountable for others illegal file sharing.

Businesses should inform those using their internet about the new law and explain that illegal file sharing will not be tolerated. You could update your information and communication technology policy so clear guidelines are in place around the monitoring of internet usage. Policies need to state the steps will be taken, including disciplinary action, should an allegation of file sharing infringement by an employee arise.

It is also important that you develop an internal process as to how internet usage is monitored and recorded. If you receive an infringement notice or evidence that there has been illegal file sharing on the network, it is important that you are able to identify who the infringer was, on which computer and how it happened so further infringement can be avoided.

You may need to discuss which preventative measures are best suited to the company's needs with an IT specialist. Preventative measures might include:

- Restricting website access
- Limiting the ability to download software
- Remove peer-to-peer software from company computers
- Password protect your wireless internet so only authorised users can access the internet
- Make sure your virus protection is up to date

You could also discuss how any infringement notices will be received with your ISP. The default method under the Act is the same method that the ISP uses to send bills. If the account holder ordinarily receives their bills via post, the time it takes to receive the infringement notice will reduce the amount of time the business has to challenge the notice, as the challenge period is based on the date of the infringement notice, not the date it is received.

Published: August 2017