



Privacy Commissioner
Te Mana Matapono Matatapu



PRIVACY

at work

A guide to the Privacy Act
for employers and employees



Foreword



Privacy Commissioner
Te Mana Matapono Matatapu

Published by the Office of the Privacy Commissioner
PO Box 10094
Level 4
gen-i Tower
109–111 Featherston Street
Wellington 6143

© 2008 The Privacy Commissioner

ISBN 04 478 11725 6

Designed by Beetroot Communications
Wellington www.beetroot.co.nz

Printed by Lithoprint Ltd
Wellington

Price: \$20

Even if you hardly ever think about privacy issues, you will encounter them at work. Every time information about a person is collected, held, used or disclosed, questions arise about how to handle that information. These are questions that the Privacy Act helps you to answer.

For instance, if you are an employer, you may have to hire new staff, or monitor your existing staff. Your employees may want access to information you hold about them. You may have to investigate misconduct at work.

If you are an employee, you need to know what your rights are – and what the limits of those rights are. You also need to know how to treat others' personal information appropriately. For example you may have to deal with client information, or information about colleagues, as part of your job.

Staying within the Privacy Act is generally easy, and accords with good modern business practice, common sense, and mutual respect between employers and employees.

This book gives an overview of some common privacy situations at work. Of course, it cannot cater for all the different circumstances that arise in the workplace – small changes in facts can make a major difference to what is appropriate. Also, other laws may be relevant too, particularly employment law. Our advice in this book is limited to the Privacy Act and how it works. It does not cover employment law issues.

However, the book uses examples and discussion to illustrate what privacy questions may be relevant. It also suggests some ways in which employers and employees can go about answering them in a way that is appropriate for their particular workplace.

We hope that you find it useful.

PRIVACY

Contents

Privacy at work – an introduction	4
How this book is set out	4
The book is not an employment law guide	4
What does the Privacy Act cover?	5
The privacy principles	5
Knowing what to do – have a privacy officer	5
Job applications	7
Application forms	7
Checking the applicant	10
The interview	15
Access and correction	17
Employees can usually access their information	17
Charges	18
Other statutes	19
Withholding information	19
Correcting information	21
Keeping information safe	22
Disclosures	22
Security: taking personal information out of the workplace	26
Preventing employee ‘browsing’	27

Tracking, testing and surveillance	29
The need for policies	29
Searches	30
Mail	31
Video surveillance	32
Tape recording	34
Telephone monitoring	35
Internet and email monitoring	35
Drug testing	37
Using a GPS tracking system	39
Finger-scanning	40
How long to keep employee information	42
Is there a reason to keep it?	42
Specific legislative requirements	42
Relevance beyond the time of employment	43
Aggregated information	43
What to do if things go wrong	44
Sorting it out with the person concerned	44
Complaints to the Privacy Commissioner	44
Our contact details	45



Privacy at work – an introduction

HOW THIS BOOK IS SET OUT

This book uses examples to illustrate common workplace situations, discusses the privacy issues that those situations raise, and suggests ways to resolve them.

The book focuses mainly on obligations under the Act, but of course there are entitlements too. Also, employers and their employees need to be equally aware of the privacy obligations involved in handling personal information. Employees may deal with personal information about others as part of their job, or may come into contact with personal information about others at work. They, too, have obligations to handle that information appropriately. They may be able to work with employers to ensure the workplace has excellent privacy policies. Good privacy is good business – it is in everyone’s interests.

References to relevant principles or sections of the Privacy Act are included in the margins of the pages, for ease of use. This book is a basic guide, and these references indicate where else to go if you have further questions, or need to do more research on a particular privacy issue.

THE BOOK IS NOT AN EMPLOYMENT LAW GUIDE

This book discusses some of the major privacy issues in the workplace. It is not an employment law guide. Many other statutes (for example the Employment Relations Act or the Health and Safety in Employment Act) and their associated case law regulate workplace relationships more closely than the Privacy Act. Users of this book may need to seek further advice to find out what those laws say about their individual circumstances.

WHAT DOES THE PRIVACY ACT COVER?

The Privacy Act does not deal with all aspects of privacy. In general, it only deals with how “agencies” handle “personal information”.

Almost every individual and organisation that collects or holds personal information is an “agency”. Only some people and organisations are excluded, for example:

- MPs, acting in their official capacity;
- courts or tribunals, in relation to their judicial functions;
- the news media, in relation to their news activities.

Generally speaking, personal information is any information about an identifiable, living, human being. However, the Health Information Privacy Code applies in part to information about deceased people.

It does not have to be ‘sensitive’. Even if information about someone is widely known, it is still personal information. However, the principles in the Privacy Act contain exceptions that may apply to that information. For example, if information is publicly available, an agency can collect it.

Information about companies is not “personal information” under the Privacy Act. Privacy is about people.

THE PRIVACY PRINCIPLES

At the heart of the Privacy Act are 12 principles that govern how agencies should handle personal information. The principles cover collection, storage and security, access and correction, accuracy, retention, use and disclosure, and unique identifiers.

If another statute directly contradicts the privacy principles, that other statute ‘trumps’ the Privacy Act.

KNOWING WHAT TO DO – HAVE A PRIVACY OFFICER

All agencies must have a privacy officer. A privacy officer is the person responsible for privacy issues in the workplace.

Someone within the agency is well placed to understand that agency’s business, and ensure that it complies with the Act. Knowing what the Act says can prevent problems from arising. This can save expense, lost business and time further down the line. It is also useful for employees to know exactly who to go to if they have concerns about privacy matters.



s 2:
“agency”

s 2:
personal
information

s 6

s 7

s 23



External agencies such as employers' associations can also help employers with generic issues such as policy development.

A privacy officer:

- is familiar with the privacy principles in the Privacy Act;
- is familiar with any other legislation governing what the agency can and cannot do with personal information;
- deals with any complaints from the agency's employees or clients about possible breaches of privacy;
- trains other staff at the agency to deal with privacy properly;
- advises managers on how to ensure the agency's business practices comply with privacy requirements;
- advises managers on the privacy impacts (if any) of changes to the agency's business practices;
- advises managers if improving privacy practices might improve the business;
- deals with requests for access to personal information, or correction of personal information;
- acts as a liaison person for the agency with the Privacy Commissioner. (This is particularly important if the Privacy Commissioner is investigating whether the agency has breached someone's privacy).

The Office of the Privacy Commissioner offers training and helps privacy officers to train others, and can put the privacy officer in touch with other privacy officers.

We also have an enquiries line (0800 803 909, or 09 302 8655 for Auckland callers), an enquiries email (enquiries@privacy.org.nz) and a website (www.privacy.org.nz). Our enquiries staff cannot provide legal advice on specific circumstances, but they can give general information about how the Act works and what types of issues are relevant. Employers and employees are equally welcome to contact us.

Job applications



APPLICATION FORMS

Stephen was interested in a job as a customer services officer for an international airline. He found the application form on the airline's website.

The application form was several pages long. In the first section, it asked for a detailed medical history, including any mental health issues during the past ten years, whether the applicant had ever contracted any communicable diseases, and how many units of alcohol they drank in an average week. The applicant had to give the name of their GP, and authorise the airline to approach that GP to seek further medical information.

The second section asked whether the applicant had ever received diversion, or had been convicted of any offences including traffic infringements. It also asked for a detailed breakdown of the applicant's financial position, and sought authorisation to carry out a credit check.

The last section asked the applicant to provide a complete work history, and give two referees from the last two positions held.

Stephen felt overwhelmed by the volume and detail of the information requested. He also did not see why the airline needed some of the information to see if he was suitable for the position. He decided that he did not want to apply for the job as he felt uncomfortable about the extent of the information the airline wanted.

What information does the employer need?

Employers should only ask for the information they need to determine an applicant's suitability for the particular job. This requires thought and planning before the application process begins. What skills does the job require? What risks does the employer have to manage? What kind of person does the employer want for this job?

For example, a flight attendant might not be able to work safely if he or she has certain medical conditions. An airline would need



to obtain relevant medical information about applicants for flight attendant positions. However, the airline would not need the same medical information about a financial manager. Instead, information about experience and skills will be particularly relevant.

In the example above, some of the questions on the application form clearly go beyond what the airline would need to know for this position (eg how many units of alcohol the applicant consumed).

Financial information

It is unusual for employers to need financial information about applicants, and in most cases they should not request it. Employers therefore need to think carefully about seeking financial information about applicants. Even requiring consent for a credit check needs justification.

A credit reporter can perform a credit check if it reasonably believes the job involves a “significant financial risk” for the employer (for example a position that handles accounts or payments). However, the employer has to separately justify that it is necessary to collect it.

“Lawful purpose”

An employer must have a “lawful purpose” in requesting personal information from applicants. Usually this will not be a problem. However, for example, it can be a breach of the Human Rights Act to ask for information about various matters, including an applicant’s religion, age or ethnicity – this can be seen as discriminatory.

The Human Rights Commission deals with queries about possible discrimination. Employers or employees who have concerns should contact that Commission directly.

Be open when collecting information

The employer must make sure that the job applicant knows:

- why the employer is asking for particular information and what they will use it for;
- who will see the information;
- whether it is compulsory or optional to provide the information, and any consequences of not providing the information; and
- that the applicant may access information about themselves and correct it if it is wrong.

A well drafted application form makes this process easy.

Criminal record

Job applicants do not have to give employers information about certain types of criminal offending. The Criminal Records (Clean Slate) Act 2004 (“the Clean Slate Act”) sets out what criminal offending a person does not have to disclose, and under what conditions. Job applicants should check what they do and do not have to disclose.

For instance, a person may not have to disclose a conviction for a minor offence that is more than seven years old if the person has not offended again. Provided that the conditions in the Clean Slate Act apply, the person can state that they have no criminal record.

Certain types of jobs require greater disclosure. For example applicants for jobs as police officers, prison or probation officers, judicial officers, or roles involving the care and protection of children, such as a foster parent, have to disclose convictions that are otherwise eligible to be clean slated. The Clean Slate Act has a complete list of the situations in which disclosure is required.

It can be illegal for an employer, outside these categories, to ask a job applicant to disregard the clean slate scheme and to disclose, or give consent to the disclosure of clean slated convictions.

For further information about the Clean Slate Act please refer to: www.justice.govt.nz/privacy/clean-slate.html

Diversion information

Employers should generally not ask for information about whether an applicant has received police diversion. The nature of a diversion means that that information is not relevant for most positions. The purpose of diversion is to allow the person to avoid the stigma of a criminal conviction for minor first-time offending, and to move on from that offending. Asking an applicant to disclose diversion information undermines that purpose. Seeking that information will usually breach principle 1.

Again, though, certain types of jobs may require disclosure. It is useful to refer to the list of jobs that require clean slate information to be disclosed. For jobs on this list, it will probably also be acceptable to ask for diversion information.



s 19,
Clean
Slate Act

s 18,
Clean
Slate Act

s 19,
Clean
Slate Act

rule 11(2)
(b)(iii),
Credit
Reporting
Privacy
Code 2004



Generic and 'tiered' application forms

While it may seem more convenient to have a generic 'one size fits all' application form, asking for irrelevant information is not only legally risky but also inefficient. It is much better to be clear about what the job actually requires.

One practical option is to have a 'tiered' application form. For example, the first page can be a generic form, which requests information that all applicants for all jobs need to provide, such as contact details and details of referees. The next set of questions can request information needed for the general type of role. A final set of questions can then ask for information specific to the position.

This reduces the number of changes the employer has to make to application forms for each different job.

Remember, the application form does not need to collect all possibly relevant information. It is simply one element in the appointment process. Further information can be collected at interview, as necessary, from shortlisted candidates.

CHECKING THE APPLICANT

Mary applied to work as a caregiver with a childcare agency. As part of the application process, Mary was required to give two referees, including her current manager. She also had to sign a consent form allowing the Police to disclose information about her to the childcare agency for the purpose of assessing her suitability as a caregiver.

A couple of days after she sent in the application, Mary received a telephone call from the manager of the childcare agency, asking her to come in for a chat. The manager explained that the Police had disclosed some information that had made the childcare agency concerned about Mary's suitability for the job.

The information related to her being investigated for violent behaviour, a number of years ago. After discussing this further, Mary explained that she had been in an abusive relationship and had acted to defend herself. She had since left her partner and been through counselling.



The manager asked Mary's referees whether she was trustworthy and whether her behaviour had given any cause for concern. The referees confirmed that Mary was a good employee, and that she did not react inappropriately in stressful situations.

The manager then offered Mary the job.

Reference checking

It's easy to make sure that reference checking complies with the Privacy Act – but it's surprising how often employers don't do so.

Approaching referees

Reference checking is based on the consent of the applicant. If the applicant has not agreed to the employer approaching a person, the employer should not approach that person for information.

An employer is entitled to ask the applicant to provide the names and contact details of people whom the employer can approach for a reference. The employer can then approach those named referees to ask for information about the applicant.

Of course, applicants will usually provide the names of people who they think will give good references. The employer needs to ask questions carefully, to draw out any information that indicates the applicant may or may not be suitable for the job.

It is up to the employer to judge if the named referees are the people who can give the best information about the applicant. For example if the applicant has not given the name of his or her current or previous employer, this may be a cause for concern. It is understandable that the employer may want to check the applicant's performance with the current or previous employer. Equally, though, the applicant may have good reasons for not giving that person as a referee (for example, the applicant may not want a current employer to know that he or she is looking for another job).

Either way, it is still necessary to get the applicant's consent to approach other people for information. The employer and the applicant need to discuss it. So, the employer can ask the applicant whether they can approach the current or previous employer. It is even possible for the employer to make it a condition of a job offer that the current or previous

Principle
2(2)(b)



employer gives a satisfactory reference. This process is fair to the applicant, since it gives him or her the chance to explain – for example if there has been a personality clash or a dispute. But it also ensures that the employer is not barred from getting the information needed to make a decision whether to employ the person.

If an applicant only provides a written reference, the employer can say that they may need to contact the referee to verify the information. Again, if necessary, this can be a condition of a job offer or proceeding with an application.

The same privacy rules about reference checking apply whether the person is an internal candidate or an external candidate. If the applicant is an internal candidate, the employer can apply their own knowledge about the applicant to the process, but cannot simply ask around the organisation to see what people think about the applicant.

Confidential or not confidential?

When an employer talks to an applicant's referee, it is useful to establish at the start whether the referee is speaking in confidence or whether they are happy for the information to be given to the applicant (with or without attribution to them personally).

This is because, if information in an employment reference is given in confidence, that information will not have to be given to the applicant on request (see below under "access to information"). If there is no clear understanding of confidentiality, supported by a note on the file, it can be difficult and unnecessarily time-consuming to prove that the referee gave the information on the basis that it was to remain confidential.

It is best practice to give as much information as possible to the applicant. For example, it is often possible to provide a summary of comments received from referees without attributing them to particular referees or breaching confidentiality.

Checking qualifications

It can be very important to check the qualifications that an applicant claims to have.

Again, the key is for the employer to be open with the applicant. If the employer needs to check the applicant's qualifications, for example

with a university or training institution, the employer should say that it needs to do so. Some of that information may be available under the Official Information Act, or may be publicly available. If it is not publicly available, the employer should obtain the applicant's consent (even with an official information application, this makes life simpler). If the applicant does not consent, the employer would be entitled to refuse to appoint the person to the job.

Criminal record vetting

Ministry of Justice vetting process

Most employers do not have access to the Police vetting service. Instead, those employers apply to the Ministry of Justice and, if relevant, to Land Transport New Zealand, to receive information about an applicant's criminal history.

The applicant has to complete specific forms issued by these agencies, which include giving consent for the criminal history check. The employer then submits the forms to the agencies. The agencies filter out any clean slate information before releasing the criminal history to the employer.

For further information on these services, contact the Ministry of Justice or Land Transport New Zealand directly.

Police vetting process

The New Zealand Police operate a limited vetting service. This is for approved agencies that are responsible for providing care to children, older people and more vulnerable members of society. The purpose of the vetting process is to let these agencies know any information that might indicate that an individual is not suitable for employment. It is intended to minimise the likelihood of vulnerable members of society being put at risk by individuals who may have displayed behaviour that could be detrimental to others' safety and wellbeing.

The Police carry out a search of convictions and a search of other information that may indicate violent or inappropriate sexual behaviour. They then "red stamp" the applicant (that is, they indicate there is information making the person possibly unsuitable for the job) or they disclose this information directly to the approved agency.

The applicant has to be told that vetting will occur and why it is

s 29(3);
s 29(1)(b)



PRINCIPLE 3



necessary, and needs to consent to that process.

Security

Criminal history information is sensitive. Employers must keep the information safe from loss or misuse. This includes restricting access to the information to those who need it for their job. Once the information is no longer needed, the agency must ensure that it is properly destroyed.

Use and disclosure of the information

An employer can only use the information to assess an individual's suitability for a particular role. Once it has been used for that purpose, the employer should destroy it properly and not disclose it to others.

Unsolicited information

Shona is applying for a job to work in a bar. She used to work in a shop part-time, but left a year ago to have a baby. Before Shona left that job, she had been undergoing counselling to help treat a gambling addiction. Her manager at the time was aware of this and supported Shona in her rehabilitation. Shona is still continuing counselling but her addiction is under control and she no longer gambles.

The manager of the retail outlet heard that Shona was applying to work in a bar, so she rang the bar manager to tell him about Shona's gambling addiction.

The bar manager was concerned, especially as there are pokie machines in the bar. At the interview, he asked Shona about her addiction. Shona was very upset that he had been told about it. She explained that she no longer gambled, but she was still having some counselling. The bar manager was not sure that Shona would be suited to working in the bar, and offered the job to someone else.

Under the Privacy Act, "collection" does not include receiving unsolicited information. So, if someone gives an employer information that the employer has not asked for, then the employer has not "collected" it. The employer does not have to comply with the principles governing collection (principles 1-4). However, once the employer is in possession of the information, it needs to comply with the remaining

privacy principles.

For example, the employer needs to take reasonable steps to ensure that the information is accurate before using it. An obvious way to do so, as with this example, is to ask the applicant about it.

In this example, the bar manager has not breached the Privacy Act. However, the former employer may have breached the Act by disclosing the information. It would be difficult to show that the disclosure was permitted in these circumstances.

THE INTERVIEW

Asking questions

Interviews give an employer a further opportunity to collect information about an applicant. The same principles apply as for collecting information through an application form, referee process, or vetting process. The employer must only collect information for a lawful purpose that is relevant to the job, and the collection must be necessary to fulfil that purpose.

The unsuccessful applicant

Hana applied for a job as the assistant manager of a department store. She was asked to come in for an interview, with a panel of three senior managers. The panel asked Hana a series of questions, taking notes throughout the interview.

Hana thought she had interviewed well, so was surprised when she was told that she did not get the job. She wanted to know why she did not get the job. She asked the department store's HR manager for a copy of the notes taken by the interview panel in the hope that they would provide some explanation.

Seeing the interview notes

A job applicant can ask for a copy of any notes made by an interviewer about their interview or application. The interviewer has to provide this information unless there are reasons to withhold it. (This will be rare in the context of interview notes). Interviewers should therefore write their notes with release to the applicant in mind.

The interviewer has a maximum of 20 working days to respond to a request.

Principle 8

Principle 11

Principles 1-4

Principle 6; ss 27-29

Principle 5

Principles 10 and 11

Principles 1-4



Access and correction

Retaining applicants' information

An employer can retain the information of unsuccessful applicants for as long they require it for a lawful purpose. Generally, the information may not need to be retained much beyond the appointment process, unless, for example, the employer wants to keep the applicant's CV on file for any future positions. If the employer does want to keep it, it is a good idea to let the applicant know.

When an employer no longer wants to keep the information, they need to securely destroy it, or return it to the applicant. It is a good idea for an employer to have a policy about retaining and disposing of job application information.

If the applicant requests the interview notes, but the interviewer has already disposed of them, the interviewer may be required to recall the information to the best of his or her ability. This can be time-consuming, so it is wise to retain the notes for a short period after the appointment process has concluded to allow for any information request.

Information about a successful applicant is likely to stay on the person's file.

Keeping job application information safe

Job applications can contain very sensitive information. It is therefore important that they should be securely stored, and should only be seen by people who need to know that information.

Using and disclosing application information

Generally speaking, an employer can only use or disclose job application information for the purpose of the job application.

If the employer has to disclose job application information, the applicant should already have been made aware that this would occur and why, and should know to whom the information will be disclosed to.

EMPLOYEES CAN USUALLY ACCESS THEIR INFORMATION

Carl works for a publishing company as an editor. He has also written several children's books.

The company asked Carl to write a short story for a client. Carl agreed and signed a contract stating that he would do the writing out of work time.

Another employee told the company that Carl had done the writing while he was at work. The company investigated the allegation, but decided not to take disciplinary action against Carl.

Carl wanted to know more about the details of the investigation. He asked the company if he could see his personal file. The company agreed to let him see most of the information, but it took some documents off the file:

- a letter to the company's lawyer seeking legal advice, and the lawyer's response; and
- any material that would identify the employee who alleged Carl had written the story at work.

Employees, or former employees, can ask their employers for access to their personal files and other information about them that the employer holds.

Employers must generally provide access to that information.

"Access" can take a variety of forms. For example the employee might get a copy of the information, just have a look at it, or it might be more appropriate for the employer to summarise the information. The employer has to give access in the way that the employee prefers, unless there is good reason not to do so (see below).

Employees:

- can request access to their personal information verbally or in writing. Written requests are preferable, as they are less easily overlooked;

PRINCIPLES

Principle 6

s 42

Principle 9

Principle 5

Principles 10, 11

Principle 3



s 37

- do not have to explain why they want to see the information, though it is often helpful to do so;
- if the request is urgent, the employee must specify why it is urgent.

In most cases, an employer must let their employee access that information, but there are times when the employer can withhold information.

Employers:

- must decide whether to agree to the request as soon as possible (20 working days is the maximum time unless they say they need an extension);
- must provide access to the information in the way preferred by the employee unless this would impair efficient administration, breach a legal duty, or breach an interest protected by one of the withholding grounds under the Act. The employer must give reasons for this decision;
- must provide access without undue delay to the information they are prepared to give;
- must give reasons for a decision to withhold information;
- must tell the employee that he or she can ask the Privacy Commissioner to review a decision to withhold information.

CHARGES

Public sector employers cannot charge employees for providing access to personal information.

Private sector employers can charge a reasonable amount to recover the cost of making the information available. However, employers should not charge for the first hour of work or for the first 20 pages of copying.

If an employee wants to view an original file, this can usually be provided for free.

ss 40, 41

ss 42 (2) and (3)

ss 66 (4)

s 44

s 35



OTHER STATUTES

When a person leaves a job, they may also ask to see their wage or time records. For example they may want to check that they have been paid their correct wages or holiday pay. Employers have to provide this information under the Employment Relations Act 2000, without charge.

WITHHOLDING INFORMATION

Sometimes, an employer may be able to withhold information. For example:

- giving access to the information would unjustifiably reveal private information about another person (this may possibly be relevant in our example, depending on the circumstances);
- the information is protected under legal professional privilege (as the correspondence with the lawyer in our example will be);
- giving access to the information could hinder an investigation into a criminal offence;
- the employer compiled the information purely to see whether to appoint, promote, discipline or sack the employee and the information came from someone who only gave it to the employer on a promise of confidentiality. It is possible that the material in our example may fall into this category.

If an employer withholds information, it is best practice for the employer to let the employee know as much as possible. For example it is often possible to provide a summary of the information in a way that will not prejudice the interests the employer is protecting.

Evaluative material

Jack works as a recruitment agent. As part of his annual performance review, his employer asked Jack's manager and a number of his clients and colleagues for feedback about his performance.

At the end of the performance review process, Jack was told that he wouldn't get a bonus this year. Jack became worried about what people may have said about him and asked to see the feedback. However, his employer said that all the feedback was given in confidence and that Jack was not allowed to see it.

ss 27-29

s 29(1)(a)

s 29(1)(f)

s 27(1)(c)

s 29(3) and s 29(1)(b)



The most common reason for withholding information that an employee has requested is because it is “evaluative material supplied in confidence”. However, this exception is not as wide as employers sometimes think.

s 29(3)

First, the information has to be evaluative material, as defined in the Act. In the employment context, this is information compiled solely to determine whether the person is suitable or qualified for employment or appointment; for promotion or continuance in employment or office; for removal from employment or office; or to enable the employer to award contracts, awards, or other benefits (such as a bonus, in our example).

s 29(1)(b)

Secondly, it has to have been supplied to the employer on an understanding of confidence. This is strictly interpreted – if the person would not have given the information except for an understanding of confidentiality, then the exception can apply. For example here, part of a manager’s job is to provide feedback about staff. So an employer cannot claim that the manager only provided the information because of a promise of confidentiality. The withholding ground will not apply. If a manager says something about one of their staff members, like Jack, that staff member is entitled to know what was said, and that the manager said it.

Feedback from clients and from colleagues is different. It is best practice to reach an agreement with the employee about who will be asked to comment on their performance.

Sometimes, information is volunteered. It is possible for volunteered information to still be considered to have been “compiled” by the employer. However, it can be difficult to determine whether the information was supplied on the basis of an understanding of confidence, when nothing has been said.

If a client, colleague or peer reviewer has only provided feedback about performance on the basis that they will not be identified, the withholding ground may apply, but employers need to ask themselves exactly what is expected to be confidential. Is the information itself confidential? Or is it only necessary to disguise the identity of the person who provided that information?



The employee is usually entitled to get a summary of the information (to the extent that this will not breach the confidence).

CORRECTING INFORMATION

If the employee believes that any of the information is wrong, they can request that the information be corrected. This can include deleting information – if it is wrong, it is important that that information does not get used in future.

Often an employer and employee will have different views about what is correct. For instance they may have different perspectives on an incident at work. In this situation, the employee should give the employer a note of what they believe the correct information is. The employer should then attach that note to the file, so that it will be read in conjunction with the original information. Any future reader of the file will then be able to see a more complete picture.

Principle 7



Keeping information safe

DISCLOSURES

Paora currently works in a supermarket, but has been interviewed by Kelly, the regional manager of a retail chain, for a retail assistant position. Kelly is a friend of Tania, Paora's current manager. Over a drink one night, Kelly told Tania that she had interviewed Paora. Tania then told Kelly all about Paora's work performance.

Paora had not told anyone at his current work that he was seeking a new position. He was upset both that his current employer now knew he was looking for other work and also that Tania had discussed his performance with her friend.

It is important for an employer to have clear ideas – and preferably written policies – about the uses and disclosures of personal information about employees that are acceptable, and what disciplinary action might occur if those policies are breached.

All relevant staff should be familiar with these policies. If staff need training so they can understand their obligations, then they should receive it.

This also helps the employer to manage their risks. If an employee makes an inappropriate disclosure about a fellow employee, the employer (as well as the employee) will be liable unless the employer has taken all “reasonably practicable steps” to prevent such a disclosure from occurring. Reasonably practicable steps include having a good policy that relevant staff are familiar with.

So, for example, Kelly and Tania should both have been aware that it was not appropriate to mention Paora's application, or to discuss his performance. Sometimes this is so obvious that an employer would not be expected to have a formal policy. However, the employer might need to take other steps to ensure that recruiters and managers are aware of their Privacy Act obligations.

Employees who are leaving

Amy, who worked in the office of an auto repair shop, was dismissed because she was caught taking money from the till on more than one occasion. Her employer told the other staff why Amy had to leave. Amy was not happy that her employer had told the other staff what she had done.

There are many examples in the workplace where personal information about an employee needs to be disclosed. For instance when an employee gives notice to leave their job, they are normally bound to work out a notice period. Once the employer has accepted a person's resignation, it is reasonable to let other staff know they are leaving.

It is also reasonable that clients are told that an employee is leaving. They may need to know whom they can contact once the employee has left, and how it will affect their relationship with the agency or workplace.

It would be good practice, however, for an employer to first confirm with their employee that it is all right to let other staff, colleagues and/or clients know they are leaving.

Employees can assist by being clear about what they are happy for the employer to say. For example, an employee may not want others to know where they are going or what they will be doing. This could place the employer in a difficult situation when other staff members or clients ask. An employer should not give too many details, unless it is clear that the employee is happy with this. Instead, a general statement such as “Rawiri has gone overseas” or “Steve has left for family reasons” will be sufficient.

Where an employee is leaving because of disciplinary action, it is more difficult to know how much to say. Unless it is necessary for business reasons to let people know why the employee is going, it is usually better simply to say that they are leaving. This is less likely to breach the law.



Principle 11

PRIVACY

Principle 5

s 126



Noticeboards

Lily's name was displayed on a whiteboard at work as being a staff member who was to be made redundant. Her name remained on the whiteboard for several days and was seen by a number of employees.

Lily had previously been told by her manager that she was to be made redundant, but it was not something that others in the organisation should have known about until Lily's redundancy package had been finalised.

Acceptable disclosures, for example on noticeboards, are largely a matter of common sense, fair treatment and business need. Who needs to know the information and why? How much information do they need to know? What might the employee's reaction be (for example what would you, the discloser, think about it if you were in the employee's situation and how would you like to be treated)?

Make sure the disclosure complies with the Privacy Act

Disclosures at work may be acceptable. Check principle 11 of the Act. For example:

- disclosure may be the reason why the information was collected in the first place;
- the employee may have authorised the disclosure;
- limited disclosure may be needed for the employer to be able to investigate a complaint or incident involving the employee;
- information may need to be provided in the course of dealing with a formal employment dispute (for instance to the employee's representative, or to the Employment Relations Authority);
- in cases of possible criminal offending, information may need to be disclosed to the Police, so they can decide whether to prosecute the employee.

Principle
11(a)

Principle
11(e)(iv)

Principle
11(e)(i)



OIA,
s 9(2)(a)

The Official Information Act

Public sector employers are covered by the Official Information Act 1982 ("the OIA"). If someone else asks for information about the employee, a public sector employer may need to release information. This is because there is a presumption that official information will be made available.

However, privacy of employees is obviously important. An employer needs to consider how strong the employee's privacy interests in this particular information are. The employer then needs to consider the public interest in releasing that information. If the public interest is weaker than the privacy interests, the employer can withhold the information.

Not all information about employees is sensitive, or particularly "private". However, this will depend on the circumstances. For example the employee's work title, their qualifications or their length of service with the employer will not usually be sensitive. Also, there may be a strong public interest in releasing that information (for example to demonstrate that someone has a specialist qualification for a job). However, sometimes the context may indicate that the privacy interests are stronger than usual.

By contrast, some information about employees is inherently highly sensitive, such as financial information, or information about disciplinary action taken against them. However, the public interest may nonetheless be strong enough to require the employer to release that information – at least in some form. For example, chief executives' salary information should be released, and other salary information should often be released in bands (the bands are wider as seniority decreases).

Where information is refused, the requester has the right to complain to the Office of the Ombudsmen.

It is wise for an employer to have good policies about release of certain common types of information about employees. It is often also useful to get the employee's view before releasing information so that the employer can properly judge the strength of any privacy interests. However, the employee cannot veto a decision to release.



SECURITY: TAKING PERSONAL INFORMATION OUT OF THE WORKPLACE

Tama worked for a company operating in a rural area. He had to travel a great deal for his work. He used a laptop computer on which he kept client details, including bank account details and other financial information.

Tama had set a password on the laptop, and changed it regularly. The hard drive was also encrypted.

One night, outside a motel, Tama's car was broken into. The laptop was stolen.

Many organisations allow, or need, their employees to work outside the office. Remote working will often require use of information on portable media such as laptop computers, CDs, USB memory sticks or, of course, paper files.

If the employee is dealing with personal information about individuals, both the employer and employee need to ensure that the information is kept secure. For example reasonable steps must be taken to ensure that family members cannot access personal information about clients. Also, reasonable steps are needed to ensure that if, for instance, a laptop or memory stick is lost or stolen, the personal information will not be accessible to an unauthorised person.

What is "reasonable" depends on factors such as:

- the nature of the personal information (the more sensitive it is, or the more harmful it would be if it falls into the wrong hands, the stronger the protection needed);
- the ease with which it can be protected (it is not difficult to set a strong password);
- the cost of protecting it (encryption is now fairly accessible and affordable).

So, for example, the clients' information on Tama's laptop was highly sensitive, and the level of harm that could occur to the clients if their information fell into the wrong hands was considerable. It was therefore reasonable to expect that Tama would have a strong password, and that he would have taken further steps – here, encryption was feasible

– to prevent unauthorised access if the laptop were stolen or lost. To be safer, however, he should probably have taken the laptop into the motel with him, rather than leaving it in the car.

It can be difficult for an employer to know how to deal with a security breach, such as a theft of client information. The Privacy Commissioner has issued guidelines on security breach notification, which are available at www.privacy.org.nz.

PREVENTING EMPLOYEE 'BROWSING'

Jono is a nurse at a private clinic. One day, he and his colleagues thought they saw a local TV personality arrive at the clinic. Later that day, Jono looked on the patient database and found the celebrity's details. He discovered that she had been admitted for some minor plastic surgery. Jono considered telling his friends but decided against it, because of patient confidentiality.

Jono's employer, though, had placed an alert on the celebrity's file on the database. This alert told the employer that the file had been accessed. The employer traced the access back to Jono. Jono was subsequently disciplined for breach of the workplace policy on unauthorised accessing of patient information.

When an employee who is authorised to have access to personal information at work looks at that information without a legitimate reason to do so (for example to check up on someone, or out of curiosity), this is known as 'browsing'.

The employer holds the personal information for a particular purpose or purposes. It should only be accessed or used for those purposes. Employee browsing is therefore a breach of privacy.

Employers need to take reasonable steps to prevent browsing of personal information. As with the earlier example of Tama and the laptop, what is "reasonable" will depend on a number of factors.

Not all employers can have (or would need to have) an alert facility on a computer system. However, it might be reasonable to expect them to do so if their information holdings are large and/or highly sensitive. Wherever possible, it is important to be able to see whether files have been accessed, and to trace back the electronic footprint to the person



PRIVACY

Principle 5



(or at least the computer) who has accessed them. The employer can then enquire whether that access was for legitimate purposes.

Employers need to have a policy about what access is legitimate and ensure that employees are aware of the policy and of the implications if it is breached.

Tracking, testing and surveillance



THE NEED FOR POLICIES

New technologies provide employers with greater opportunity than ever to track, test, check, search and monitor employees. The appropriate level and type of monitoring and checking varies widely between workplaces. Excessive monitoring and checking can breach the law. Even if it does not, it can damage trust, and disrupt workplace relations and performance. Deciding what is necessary can therefore be a complex calculation.

All forms of monitoring and checking require the employer to have a good policy, which ensures compliance with relevant legislation (including the Employment Relations Act and the Privacy Act).

These policies need to be communicated clearly to staff before they are introduced, so that staff are aware of the employer's intentions, and their own obligations. Some policies may require staff agreement or consultation.

Occasionally, an employer may be able to monitor a particular employee without letting that employee know. This depends on what the purpose of the employer's action is. For instance if an employee is suspected of taking company property, an employer may want to monitor the person to gain evidence. If the employer lets the employee know, it could defeat the employer's ability to find out what has occurred. If the purpose is to deter theft, however, the employer should ensure staff are aware, for example, that there is a camera overlooking a cash register.

That footage can then usually be used as evidence if dishonesty is discovered, since that is the purpose for the surveillance.

A policy should deal with such matters as:

- the particular type of monitoring that will or may take place;
- why this is necessary;
- the frequency of the monitoring (for example, daily, weekly, or randomly), and any start and finish dates for the monitoring programme;
- the level of the monitoring – that is, how detailed it might be;

Principles
3 and 4

Principles
10 and 11



- any potential disciplinary consequences, for example if the monitoring demonstrates that the employee is in breach of their contract;
- the consequences for refusing to allow the employer to collect the information this way; and
- what will happen with any information the employer collects – who will see it, how it may be used, if it may be disclosed outside the business, where it will be stored and for how long, and if it will be eventually destroyed.

Contracts of employment may also need to set out some of these matters.

If a policy affects visitors to the premises as well, the employer must also inform visitors of the policy and the reasons for it. For example if there is video surveillance in place, there should be signs informing visitors that that is the case.

Employees (or visitors) can generally access any information that is collected about them through the use of monitoring, unless there is good reason for withholding that information.

SEARCHES

Janet discovers that her employer has searched her personal locker without her permission. She is incensed that her employer has looked through her personal belongings, and complains to the Privacy Commissioner.

Reasons for searching

An employer must have a clear and legitimate purpose for undertaking any sort of search of an employee's belongings, such as their bag, car or locker. For example:

- a business may have had a spate of violent incidents, and needs to check that weapons are not being brought into the workplace;
- there may have been a series of thefts at work, and the employer may need to check bags, cars or lockers to ensure that employees are not stealing work property or goods;
- a business may have discovered drug and alcohol use in areas where heavy machinery is being operated. It may need to search to ensure that drugs and alcohol are not being brought to work.

Type of search

The type of search must fit with the purpose of the search. For example if the search policy was put in place because laptops were being stolen from work, then it would be reasonable for sports and carry bags and cars to be inspected because they are large enough to conceal a laptop, but smaller bags, such as handbags, would not need to be inspected.

If the search was for drugs then it would be reasonable that smaller bags were inspected as well.

Level of search

The level of inspection also needs to fit with the purpose of the search. For example an employer may decide to view the contents of an employee's bag only but not rifle through their belongings.

If an employer is going to employ a security guard to undertake inspections, the security guard must be appropriately trained and must know the policy to follow.

MAIL

Louise works in the office of a small business. The manager opens all incoming mail including letters that are addressed to individual staff members.

One letter, addressed to Louise, was personal and contained sensitive information. The manager opened the letter and left it on the top of a pile of mail on his desk. A staff member came into the office when the manager was absent, and read the first page of Louise's letter. The staff member then disclosed the contents of that page to other employees at the morning tea break. Louise was embarrassed and very upset at what had happened.

At work, most mail relates to the business of the employer. So it is reasonable to have one person who opens the mail, including mail addressed to individual employees.





Employees can protect themselves to some extent. If possible, they should avoid giving their work address as the place to which personal mail can be sent. If they do need to receive personal mail at work, they should ask their correspondents to mark the mail “Private and Confidential”. If it is not marked, it is reasonable for it to be opened as normal.

The employer should have a policy about how mail marked “Private and Confidential” should be treated. Generally, it should not be opened but should be given directly to the employee.

If an employer does open mail that is personal, the employer then has to treat that mail with appropriate care. An easy way to manage this is to place the mail back in the envelope (securely, if necessary, to prevent other staff members from seeing it) and to give it directly to the employee.

The same is true, for example, of a fax that is sent to an employee personally. Care needs to be taken that any information the fax contains is kept as secure as possible.

In Louise’s case, therefore, the manager was at fault for leaving the letter within view of other staff members. Louise’s colleague was also at fault for disclosing the information to other staff members.

VIDEO SURVEILLANCE

Martin runs a small business importing European foods. As Martin spent a lot of time visiting potential clients, he was often out of the warehouse for long periods of time. After several months, he realised that money was being stolen from the safe in his office. A number of employees had access to the safe, and Martin had no idea who was stealing the money.

One Friday evening, Martin decided to erect a hidden camera in his office to catch the perpetrator. On the following Monday evening, Martin viewed the footage and discovered who had been stealing the money. He then removed the camera from the office as he no longer required it. The next day, Martin confronted the individual with the evidence and terminated his employment. Martin also provided a copy of the recording to the Police.

Video surveillance is increasingly common in many workplaces, for example in the retail industry. It can be useful as a way of protecting people, or property, and of capturing evidence of crime. However, it can be intrusive, and is open to misuse. Also, employees are unlikely to perform well if they are constantly overlooked. It is therefore important to think carefully about whether video surveillance is an appropriate way to deal with a workplace situation.

Ordinarily, there should be signs to let workers and visitors know that there is video surveillance in place (for example, “security cameras operating” or “for safety and security, please be aware that continuous video recording operates on these premises”).

If audio recording is operating – with employee consent – visitors or clients should also be alerted to that fact.

Covert surveillance

Occasionally, it will not be necessary to alert people that there is video surveillance operating. For example it might defeat the purpose of having the camera if there was a sign alerting people to its presence (as with Martin’s example above).

However, covert surveillance is intrinsically more privacy intrusive than overt surveillance, and is potentially unfair to those filmed. It is therefore particularly important to be able to justify its use, and to ensure that it is carefully controlled.

Factors which affect whether covert surveillance is acceptable include:

- the purpose for having surveillance at all, and for making it covert;
- whether it is targeted at a particular person (eg on suspicion of theft) or an area (eg from which goods are being stolen, where property is being vandalised, or where people are particularly vulnerable);
- whether the camera is stationary or whether it rotates, and why;
- ensuring that any audio recording capability is not used when the cameras are operating (audio can be more intrusive than pictures, and may well also be ‘interception’ in breach of the Crimes Act if operated covertly);
- whether the area under surveillance is one in which people undress, or otherwise expect a very high level of privacy (for example in toilets).

Principle 3

Principle 4



As discussed earlier, the employer should also have standard policies on storage and retention of the footage, potential uses and disclosures and who will have access to it. For example, there should be a set length of time for which the tapes are kept and then they should be taped over unless the video has captured information that the employer then needs to use (for example in disciplinary action against a person).

TAPE RECORDING

Jeetan worked at a service station. He was called into the manager's office and told that he was suspected of taking stock without paying for it. The manager recorded the conversation with Jeetan on a tape recorder hidden in his drawer.

Jeetan was subsequently dismissed but learned of the tape recording seven months later in proceedings before the Employment Tribunal. Jeetan believed that the employer should not have recorded their conversation without him knowing.

If an employer is intending to tape record a conversation with an employee – or vice versa – they should have clear reasons for doing so. A tape recorded conversation will contain far more detail than simply taking notes of a conversation. It may well be good to tape record a meeting with consent, so that both sides have an accurate record of what occurred.

Although covert recording is not illegal as long as one of the parties to the conversation is doing the recording, it is more difficult to justify covert tape recording under the Privacy Act since there is a strong presumption that it is unfair.

Employers should seek legal advice before using covert taping.

TELEPHONE MONITORING

Danny works for a company that conducts much of its business with customers by telephone. From time to time, the employer records conversations between the staff and customers, and uses this information to assess staff on their work performance.

The employees know about the recording, but the customers do not. Danny is uncomfortable about this.

An employer must have a clear purpose for recording the telephone conversations between employees and customers. For example, where phone calls with customers are integral to a business then an employer may well need to know that customers are getting good service, and that business objectives are achieved. Sometimes, it is also important to record calls to have an accurate record that a call occurred, and what was said (for example in certain government call centres).

An employer will need to let the employee know that calls will be recorded, and what they can be used for. Failure to do so may amount to an interception of telephone calls by someone who is not a party to the telephone call. This is illegal, unless there is lawful authority for it.

It is best practice to play a brief message letting customers know the call may be recorded and why.

INTERNET AND EMAIL MONITORING

Cameron works in the customer services team at a telecommunications company. When he started working for the company, his manager went over the corporate internet policy with him.

The company's internet and email policy allows for a degree of personal use, as long as it does not disrupt an employee's normal duties. Viewing or sending offensive or objectionable material is forbidden and constitutes serious misconduct. The manager advised Cameron that employees' internet and email usage would be monitored routinely.



PRIVACY



Cameron uses the email for work purposes, as well as some personal use. He does his banking over the internet at lunchtime, and occasionally logs on to his social networking site.

Recently, Cameron's manager became concerned over staff productivity. He arranged for an audit of employees' internet and email usage. He also looked at the content of individual emails and looked at the sites visited. Cameron found out that the manager audited his usage. He accepted this. However, he was concerned that the manager had accessed his personal email folders, and was horrified to think that the manager may have been able to gain access to his password and could access his banking details.

Principle 1

Internet and email are provided by an employer as a business resource. It is therefore reasonable for employers to exercise some form of control over how that resource is used. For example they need to ensure that employees' activities online will not compromise the business' reputation. They will also need to ensure, for example, that employees are not spending so much time on personal emails that their work is adversely affected.

However, detailed monitoring of internet or email use can be unnecessary. An employer needs to be able to justify collecting the information.

Principle 4

Employers need to have a policy about monitoring employee email and internet use. If the employer does not have a policy, or staff have not been informed of it, it will be much harder to show that checking email and internet use is fair and reasonable.

Viewing the *content* of emails needs particular care. Employees may think that their email correspondence is private, particularly where the employer has a policy permitting reasonable personal use. If the employer needs to investigate allegations of serious misconduct such as viewing pornography, breaches of confidentiality or harassing or bullying other staff members or clients, the employer may need to look at the content of emails. The policy should cater for this type of situation, so that employees are clear that an employer can and will look under certain conditions.



Employers should aim to intrude only to the extent necessary. For instance they may be able to use a computer's search function to check only for certain words, web addresses or subject lines. They may be able to set up alerts for particular types of activities, and then check only if those alerts are triggered. This will minimise any unnecessary intrusion into an employee's computer activity.

DRUG TESTING

For the past three years, Jane has been working in the office of a commercial carrier firm that specialises in long-haul cartage. The head of the company has recently announced that it will soon start conducting random drug testing on all staff.

Jane is aware that some of the drivers have been suspected of taking drugs. She supports testing for safety reasons. However, she does not think that she should be tested for drug taking because she does not take drugs and her job is in the office.

Testing for drugs in the workplace is often undertaken because of health and safety issues – of the employee, of other employees or of members of the public.

There are three main types of drug testing an employer might consider:

1. compulsory testing (eg at the pre-employment stage);
2. random testing; and
3. testing for cause (for example, where there has been an accident or a near accident in the workplace).

Workplace drug testing can be a difficult process to undertake. It includes a range of legal hurdles that an employer must consider. Drug-testing involves the collection, storage and use of information about employees, so the employer needs to consider the Privacy Act. There have been cases on drug testing in employment law, of which employers need to be aware (the leading case is *NZ Amalgamated Engineering Printing and Manufacturing Union et al v Air New Zealand*). Public sector employers need to know about the provisions of the New Zealand Bill of Rights Act. The Human Rights Act may also be relevant.



It is important that employers obtain legal advice before introducing a drug testing programme. Discussion with employees or their representatives is also advisable.

Drug testing is intrusive

A common form of drug testing is urine sampling. This is often very invasive, particularly since supervision is usually required to prevent contamination or substitution of the sample.

The more invasive the type of drug testing, the stronger the justifications need to be for its use.

The reason for the testing, and the frequency of the testing, are also highly relevant to a calculation of when it will be reasonable. For example it is easier to justify drug testing for staff working in areas where safety is a real issue (for example public transport, or operation of heavy machinery). It is more difficult to justify testing of office workers like Jane. Testing for a specific reason, for example, on suspicion is easier to support than random testing.

Testing must be linked to a sound business purpose

Before embarking on a drug testing programme, an employer should:

- consider carefully whether there is, in fact, a drugs problem in the workplace;
- assess the nature and extent of the problem;
- be certain that the drug taking could impair an employee's ability to work and that they are a safety risk to themselves and/or others; and
- consider whether drug testing is the most effective way of dealing with a suspected drug problem. There could be less intrusive alternatives that may be just as or more effective, such as supervision, a drug education programme, or confidential counselling services.

A positive drugs test result does not demonstrate a person was impaired in the workplace. Nor does it show that the person will be impaired in the workplace in future. It does not show that a person is bringing drugs to work. It can only establish that a person has had one of a number of drugs within a certain period. Some drug tests can reveal use of drugs from many weeks before, quite possibly taken outside the workplace.

The employer therefore needs to be very clear that testing of a particular type and frequency, of particular staff, under particular circumstances is necessary for their business.

How reliable are the results?

Drug testing can sometimes give inaccurate results. An employer should consider confirming the results with an independent accredited laboratory test, particularly before taking any disciplinary action.

Letting employees know

Before undertaking drug testing in the workplace, an employer must ensure that employees are aware of:

- the purpose/s of the drug testing;
- how often it will happen;
- the consequences of refusing to undergo the testing;
- who will see the test results and other information associated with the test;
- what will happen with that information – where the information will be stored and for how long, and if it will be eventually destroyed; and
- what happens if the drug test result is positive.

Access to the results

Employees are entitled to request a copy of the drug test results. They can also ask whether the test results have been confirmed by an independent laboratory test by an accredited laboratory. If so, they can also request to see those reports.

USING A GPS TRACKING SYSTEM

Businesses that run a fleet of vehicles may find GPS a useful tool to manage their fleets more efficiently. For example, a GPS system can ensure that a dispatch centre sends the closest taxi to pick up a passenger. It can deliver information on the best routes to take. It can monitor the time a driver works, and even assist with issues such as speed compliance.

However, since GPS involves monitoring where a driver is, it is important that the employer should have good policies to govern it. For example, what happens out of work hours? If the employee has access to the



vehicle for personal use, it may not be necessary to gather or use any GPS information. Any information relating to that non-work time will need to be handled very differently from the information gathered while the person is on the job.

FINGER-SCANNING

Iosefo owns a clothing factory, and employs 30 staff. He is experiencing some productivity difficulties. Some of his staff are routinely late to work and early to leave, and he suspects that staff cover for each others' absences, but he finds it hard to get proof of what is going on.

Iosefo decides to introduce a finger-scanning system. On Monday morning, when his staff arrive, he shows them the machine and explains that they will now have to clock in and clock out using this system. Some of his staff are alarmed and offended at the prospect of having their finger scanned to identify them.

Finger-scanning is a relatively new workplace practice in New Zealand. It tends to be used for clocking in and out.

There is some debate over whether the information collected by finger-scanning equipment is personal information at all. This may depend on the nature of the equipment. However, if the finger scan can be related back to a particular person in the workplace, it is likely to be viewed as personal information.

As with any collection of personal information, an employer must show that the collection of information – here the record of points of reference from a fingerprint – is lawful, and that it is necessary for the functions or activities of the business.

The employer must also inform the employees why the collection is necessary, what it will be used for, and so on. Since “fingerprints” are usually associated with criminal investigations, particular care is needed to explain to employees what the system actually does, and what information is stored.

An employer should make sure that employees have been given this information before the system is installed. It is not advisable to require employees to use a system such as finger-scanning before they have been given more detail about what it involves. So, in this example, Iosefo should have told his staff what was going to happen before introducing the system.

Whether this method of collecting personal information is unfair or unreasonably intrusive in the circumstances will depend upon the reasons for it, the policies about its use, and the type of equipment involved.

As with all personal information, employers need to store the information securely, and control uses and disclosures of that information.



Principle 4

PRIVACY



How long to keep employee information



IS THERE A REASON TO KEEP IT?

Jenny works as the HR manager at a large transport company. She has begun auditing the company's personnel files. The company has retained the personnel files relating to all of their employees, both past and present, for the last fifteen years. Jenny has run out of storage space and wants to destroy the files relating to ex-employees. She is not sure if she is allowed to do this.

The basic rule is that once an employer no longer needs the information, it should not be retained. Instead, it should be securely destroyed or, alternatively, returned to the employee.

The Privacy Act does not specify how long employee information must be kept for. It permits the employer to keep it for as long as that information can lawfully be used.

This gives employers a considerable amount of flexibility, but it does mean that employers should have policies on how long they keep information for.

SPECIFIC LEGISLATIVE REQUIREMENTS

In assessing how long to keep the files of ex-employees, first check whether there is any legislation that dictates how long certain information should be kept for. For example, employment legislation requires employers to keep wage and time records for at least six years after an employee has left their employment (Employment Relations Act), and tax law requires employers to keep PAYE information for "not less than seven years after the making of the payments to which they relate" (Tax Administration Act). The Public Records Act may also apply.

RELEVANCE BEYOND THE TIME OF EMPLOYMENT

It may be necessary to keep some other information beyond the term of the person's employment. For example, some information about the employee's performance may be relevant if the employer has to give a reference. This does not mean, however, that detailed records need to be kept. The employer should only keep the information that is relevant to such a reference.

If the employer is engaged in a dispute with the employee, they will need to retain all relevant information for as long as it takes to resolve or finalise that dispute. That may mean retaining detailed information.

AGGREGATED INFORMATION

Employers may well wish to retain statistical information about their workforce. The Privacy Act only applies to information about identifiable individuals. So if the information no longer identifies individual employees, there is nothing to prevent the employer from retaining it.



What to do if things go wrong

SORTING IT OUT WITH THE PERSON CONCERNED

The earlier a privacy problem is resolved, the better. So try to deal with it directly if possible.

If you need information about what the Privacy Act says, we may be able to help. Have a look at the Privacy Commissioner's website (www.privacy.org.nz), email us on enquiries@privacy.org.nz, or ring our free enquiries line on 0800 803 909 (09 302 8655 for Auckland callers). We cannot give you legal advice, but we can often point you in the right direction.

COMPLAINTS TO THE PRIVACY COMMISSIONER

The Privacy Commissioner can investigate complaints about breaches of privacy.

You can look at our information on complaints, or download our complaint form from our website (www.privacy.org.nz, under the heading "Your Privacy").

This information will also be useful for employers who are responding to complaints.

Our enquiries staff can also provide information about the complaint process.

OUR CONTACT DETAILS

Office of the Privacy Commissioner
PO Box 10094
Level 4, gen-i Tower
109-111 Featherston Street
Wellington
04 474 7590

Enquiries line

09 302 8655

or call free on

0800 803 909

Website

www.privacy.org.nz



Privacy Commissioner
Te Mana Matapono Matatapu

