WE KNOW HUMAN RESOURCES

CANTERBURY EMPLOYERS' CHAMBER OF COMMERCE

A Guide for Employers

THE PRIVACY ACT 1993

CONTENTS

INTRODUCTION

The Privacy Act 1993 has major implications for employers as its primary purpose is to allow employees greater access to personal information kept on files compiled and held by their employers.

Personal information may be collected only for a lawful purpose connected with a function or activity of the employing organisation and only if necessary for that purpose. As a general rule, the information must be collected directly from employees and they must be told why it is needed and the use to which it will be put. All employees have the right to see information collected about them, seek a correction if they consider it wrong, and add their own version of events.

To control the information collection process the Act establishes 12 information privacy principles. It is important for employers to be familiar with these, so that unintentional breaches are minimised. Certain exceptions and exemptions apply in particular situations and are listed in this guide.

To ensure they comply with the Act, employers should make certain systems of data collection and retention allow employee requests for access to personal information to be dealt with promptly.
The Act applies, as well, to customer/client information.

OBJECTIVE

The objective of the Privacy Act is to provide better protection for individual privacy in relation to the collection, use, access to, correction and disclosure of personal information held by any public or private sector "agency". The term agency includes an employer.

The Privacy Commissioner is responsible for promoting adherence to the privacy principles and for investigating alleged breaches. In doing so, the Commissioner is required to have regard for the general desirability of a free flow of information and must recognise the right of government and business to achieve their objectives in an efficient way.

COVERAGE

The Act is concerned with protecting “personal” information, that is, information relating to identifiable individuals (persons). It does not apply to companies or organisations.

"Agency" includes all private or public sector organisations with the exception of the Sovereign, the Governor-General, the House of Representatives, Members of Parliament, the Parliamentary Service Commission, the Parliamentary Service, Ombudsmen, Royal Commissions, commissions of inquiry and inquiries to which s6 of the Inquiries Act 2013 applies.

Courts and tribunals are exempt from the Act in relation to their judicial functions while the news media are exempt in relation to news gathering and dissemination but not in their capacity as employers.

INFORMATION PRIVACY PRINCIPLES

The Act sets out 12 information privacy principles relating to the collection, access, correction and disclosure of personal information.

The principles are summarised below:

Principle 1 - Purpose

An employer may only gather personal information for a lawful purpose connected with some function or activity of the employer’s organisation or business. The information must be necessary for that purpose. If challenged, the employer must be able to establish a relationship between the collection of the information and the way the organisation or business operates or is run.

Principle 2 – Source

An employer must generally collect data directly from the individual concerned. However, it is not necessary to comply with this principle if the employer believes on reasonable grounds that:

- the information is publicly available;
- the individual concerned authorises collection of the information from someone else;
- non-compliance would not prejudice the interests of the individual concerned and is necessary to avoid prejudice to the maintenance law;
- non-compliance is necessary for the protection of public revenue;
- non-compliance is necessary for the enforcement of a law imposing a monetary penalty;
- non-compliance is necessary for the conduct of any court or tribunal proceedings;
- compliance would prejudice the purposes of the collection;
- compliance is impracticable in the circumstances of a particular case;
- the information will not be used in a form in which the person concerned is identified or will be used only for statistical purposes;
- in limited circumstances the collection of information is authorised by the Privacy Commissioner.

Principle 3 - Collection

Where personal information is collected from an employee, an employer must ensure the individual knows that it is being collected, is aware of the purpose for which it is collected and the intended recipients, and that there is a right to access the information and have it corrected.

The employee must also be told who is collecting the information, who will hold it, and, if the information is required by law, which law applies. The employer must also make clear whether providing the information is mandatory or voluntary and the consequences, if any, of a refusal to provide the information (or any part of it).

Compliance with the above is not necessary where the employer believes on reasonable grounds that one or more of the exceptions listed under Principle 2 apply. (*Not* principle 3)

Principle 4 – Manner of Collection

Personal information must not be corrected by unlawful, unfair or unreasonably intrusive means.

Principle 5 – Security

Employers must ensure that personal information is protected - by such security safeguards as it is reasonable to take - against loss, modification, unauthorised access, use, disclosure or misuse (although an employer may *authorise* access, use, modification or disclosure). If information collected has to be given to someone who provides a service to the employer, everything reasonably possible must be done to prevent unauthorised use or disclosure.

Principle 6 – Access

Where personal information can be readily retrieved the employer must allow an employee to confirm that he or she has a file, access it, check it, and, if necessary, request correction. If possible, information should be made available in the way the employee requests, although if this would impair efficient administration, be contrary to a legal duty, or prejudice New Zealand's security or the employer's trade secrets - or if there is some other reason for refusal recognised by the Act - the employer may stipulate how the right of access is to be exercised.

The employee may be allowed to inspect any document (but need not be allowed to take it away), or can be given a copy of it. Where the "document" in question is in the nature of a recording, photograph, film video, or the like, the employee must be allowed to hear it or see it. In some instances, a transcript of a document may be provided - as in the case of a recording or something written in shorthand. Or an employer may provide an excerpt, summary, or oral information about a document's contents. Where the information is not provided in the way requested, the employee must be told why not and, if asked, the employer must give supporting reasons (unless to do so would prejudice New Zealand's security, defence, or international relations, or the employer's trade secrets or commercial position, see also Question 12).

This principle does not apply if a statute imposes a restriction on the release of personal information.

Principle 7 – Correction

Where an employer holds personal information, the individual concerned can request correction. Where such correction is not made, the individual is entitled to have a statement of the correction sought attached to the information.

Principle 8 – Accuracy

Employers must take reasonable steps to ensure that before use, the information is accurate, up-to-date, complete, relevant, and not misleading.

Principle 9 – Information Retention

Employers must not keep personal information longer than is necessary for the purposes for which it can be lawfully be used.

Principle 10 – Limits on Use

Personal information collected by an employer for one purpose may not be used for any other purpose unless the employer believes on reasonable grounds that:

- the information was obtained from a publicly available publication and its use would not be unreasonable;
- the disclosure is authorised by the individual concerned;
- non-compliance is necessary to avoid prejudicing the maintenance of law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences;
- non-compliance is necessary for the enforcement of a law imposing a monetary penalty;
- non-compliance is necessary for the protection of public revenue;
- non-compliance is necessary for the enforcement of a law imposing a monetary penalty;
- non-compliance is necessary for the conduct of any proceedings before a court or tribunal - either commenced or contemplated;
- the use of the information is necessary to prevent or lessen a serious threat to public health or safety or to the life or health of the individual concerned or of someone else (a serious threat is one likely to be realised at the time it is made and likely to have serious consequences);
- the purpose for which the information is used relates directly to the purpose for which it was obtained;
- the information is used only for statistical or research purposes and will not be published in a form likely to identify the individual concerned;
- disclosure is authorised by the Privacy Commissioner.

Principle 11 – Limits on Disclosure

Employers may not disclose personal information unless they believe on reasonable grounds that:

- disclosure is one of the purposes for which the information was obtained;
- the source of the information is a publicly available publication and disclosure would not be unreasonable or unfair;
- disclosure is to the individual concerned;
- disclosure is authorised by the individual concerned;
- non-compliance is necessary to avoid prejudicing the maintenance of law including the prevention, detection, investigation, prosecution and punishment of offences;
- non-compliance is necessary for the enforcement of a law imposing a monetary penalty;
- non-compliance is necessary for the protection of public revenue;
- non-compliance is necessary for the conduct of court or tribunal proceedings;
- disclosure of information is necessary to prevent an imminent threat to public health or safety, or to the life or health of the individual concerned or of someone else;
- disclosure is necessary to facilitate the sale of a business as a going concern;

- the information disclosed is used in such a way that the individual concerned is not identified, or is used for statistical or research purposes only;
- disclosure is authorised by the Privacy Commissioner.

In personal grievance proceedings, the Privacy Commissioner has approved the release of an employee's medical certificate to an independent doctor after the employee had refused an independent medical examination but had indicated an intention to file proceedings at which the certificate would be produced. The employer could reasonably consider the prior disclosure necessary to advance its case.

This principle does not apply if a statute authorises the release of personal information.

Principle 12 – Unique Identifiers

An employer must not assign a unique identifier (code number, for example) to an individual unless assigning a unique identifier is necessary to enable the employer to carry out any one or more of its functions efficiently. The assignment of a payroll number to facilitate wages and superannuation payments would, for example, be acceptable.

Furthermore, an employer must not assign to an individual a unique identifier that the employer knows another employer has assigned to that individual, unless the two employers are associated persons as defined in income tax legislation. Where a unique identifier has been assigned, the employee concerned can be required to disclose it only for one of the purposes for which it was assigned, or for a related purpose.
A unique identifier does not include an individual's name.

CODES OF PRACTICE

The Act provides for the development of codes of practice for particular sectors, agencies or classes of information. Codes of practice are "disallowable instruments" – in effect, regulations made the Act and can impose a higher or lower standard of duty than those set out in the privacy principles. Under the Act, the Privacy Commissioner is responsible for consulting about codes, issuing them, and where necessary, revoking them.

Privacy codes of practice should help to avoid any difficulties associated with the generality of the privacy principles, for example their application to particular activities and professions.

Industry bodies can apply for a code of practice, or the Privacy Commissioner can initiate a code's development. Applications for a code can be made by a body whose purpose, or one of whose purposes, is to represent the interests of any class or classes of agency, or any industry, profession, or calling.

Draft codes are published so that submissions on them can be made.

A code of practice may not be issued until the Privacy Commissioner has done everything reasonably possible to advise all persons who will be affected by it, or their representatives, of its proposed terms and of the reasons for having a code. The Commissioner must also give those affected or their representatives a reasonable opportunity to consider the draft code and make submissions on it.

Where a code is in force, any action that would otherwise be in breach of an information privacy principle will not be a breach if done in compliance with the code. Similarly, failure to comply with the code, even though it is not otherwise a breach of any information privacy principle, is deemed a breach. In other words, a code is an alternative to the information privacy principles.

If it is necessary to issue a code urgently, the Commissioner may issue a temporary code, in force for no longer than one year.

Two Codes of Practice of interest to some employers are the Superannuation Schemes Unique Identifier Code and the Health Information Privacy Code.

The Superannuation Schemes Unique Identifier Code allows employer superannuation scheme trustees, or a scheme's administration manager, to use a unique identifier assigned by the employer for some other purpose for superannuation scheme purposes. This use by a second agency of an employer's (the first agency's) unique identifier would otherwise be prohibited by the Act.

The Health Information Privacy Code is concerned with patient privacy but deems accredited employers under accident compensation legislation to be health agencies in relation to any health/medical information they receive. Usually, such information would go to the Accident Compensation Corporation and so must be handled by exempt employers with particular care.

AGENCY RESPONSIBILITY FOR COMPLIANCE WITH THE ACT

To ensure that proper compliance procedures are in place, an agency (employer) must have at least one person whose responsibilities include encouraging compliance with the Act's privacy principles, ensuring compliance with privacy provisions, dealing with privacy requests, and working with the Privacy Commissioner if a complaint is made and an investigation carried out.

The appointment of a Privacy Officer, as the Act requires, should help to prevent privacy complaints and at the very least, reduce the number of such complaints. It is important for staff to be made aware that when a privacy complaint arises, it is in the first instance the privacy officer who should deal with it. Any privacy complaint should always be referred immediately to an organisation's Privacy Officer.

ACCESS TO INFORMATION

Information privacy requests may only be made by someone who is in New Zealand or who is a New Zealand citizen or permanent New Zealand resident.

An employer must, within 20 working days after a request has been made, decide whether it will be granted and what charge (if any) will be imposed and inform the individual accordingly.

An employer must give reasonable assistance to anyone seeking access to his or her personal information.
Where an agent acting for the individual seeks access, the employer must ensure the agent has been properly authorised before granting access to personal information.

Information must, subject to certain conditions, be made available in the way the individual asking for it prefers.

Where the information is in the form of a document, the individual who asked for it must be able to inspect the document or be provided with a copy.

When allowing access to files, employers should ensure that evaluative material is not inadvertently disclosed at the same time.

Where a large amount of information is sought, and an extension of time is needed, the employer must say so, explain why the extension is needed, and tell the individual requesting it that he or she has the right to make a complaint to the Privacy Commissioner about the extension sought.

TRANSFER OF REQUESTS

Where an information privacy request is made to an agency that does not hold the information sought but the person dealing with the request believes another agency does, the first agency must transfer the request to that other agency within 10 working days of receiving it and inform the individual who made the request accordingly.

REFUSAL OF ACCESS TO PERSONAL INFORMATION

Under *Common Questions and Answers,* questions 8 and 9 discuss situations where employers may refuse to disclose personal information. Of particular interest to employers is the ability, generally, to withhold references from employees where evaluative material been compiled solely to determine suitability, eligibility or qualifications for employment, appointment, promotion, continuance in employment, or removal from employment, and confidentiality has been promised. However, a failed job applicant can ask to see any notes made by an interviewer and this information must be provided unless there are good reasons not to.

Whether evaluative material can be withheld depends on those two related factors: that the reason for collecting the information is one of those listed above (determining appointment to employment etc.), and that the person providing the information requested confidentiality.

Evaluative material in the nature of an in-house personal appraisal may not be withheld from an employee, even if provided for promotion purposes, since in the view of the Privacy Commissioner, evaluative material generated in-house cannot be the subject of a confidentiality request. However, it may be possible to withhold the results of a personal appraisal done to assess suitability for promotion if, for example, an outside management specialist, who has asked that the material and/or his or her identity not be disclosed, has carried out the appraisal.

When giving a reference on behalf of a former employee, an employer may ask that both his or her identity and the contents of the reference be treated as confidential.

An employer refusing an individual's information privacy request must give reasons for the refusal and note the individual's right to seek an investigation and review of the refusal by way of a complaint to the Privacy Commissioner.

CHARGING FOR ACCESS TO PERSONAL INFORMATION

Private sector agencies may charge fees for access to personal information under the Act, providing the charges are reasonable.

Where a charge is imposed, the agency (employer) may require payment or part payment in advance.

If there is a dispute about the amount charged, the Privacy Commissioner can be asked to decide the matter. Guidelines for charging can also be included in codes of practice issued by the Privacy Commissioner.

Public sector agencies cannot charge for access to information unless they can satisfy the Privacy Commissioner that they would be commercially disadvantaged in comparison with competitors in the private sector. In that case the Privacy Commissioner may approve charges being made.

COMPLAINTS

A person with a complaint may first ask the agency concerned to rectify it (though need not necessarily do so).

Anyone may make a complaint - orally or in writing - to the Privacy Commissioner alleging that an action is, or appears to be, an interference with an individual's privacy.

The Commissioner may decide to take no action if:

- the complaint is trivial or frivolous;
- the time between receiving a complaint and the date at which the alleged subject-matter occurred is significant and therefore an investigation of the complaint is no longer practicable or desirable;
- the complainant does not wish any action to be taken or where the complainant does not have a sufficient personal interest in the subject-matter of the complaint.

The Commissioner must inform the complainant if no action is to be taken and give reasons why not.

Everyone about whom a complaint is made must be given details of the complaint and the opportunity to make a written response to the Commissioner.

The Privacy Commissioner has the power to call a compulsory conference of the parties to discuss a complaint and seek a satisfactory resolution. The Commissioner may require any person to give information on oath and produce any documents considered relevant to an investigation.

The Commissioner must inform the parties of the results of any investigation and what further action (if any) is proposed.

Having investigated a complaint and found it to have substance, the Commissioner must try to secure a settlement between the parties and obtain a satisfactory assurance against repetition. To help secure a settlement the Commissioner may call the parties to a compulsory conference.

If a settlement cannot be reached or assurance given, the complaint can be referred to the Director of Human Rights Proceedings who must decide whether or not there should be a hearing before the Human Rights Review Tribunal. Before taking proceedings against anyone the Director of Human Rights Proceedings must first give that person the opportunity to state his or her case.

If the Privacy Commissioner or the Director of Human Rights Proceedings is of the opinion that a complaint does not have substance or that the matter ought not to be proceeded with, or if the Proceedings Commissioner declines to take proceedings, an individual may bring proceedings before the Human Rights Review Tribunal.

POWERS OF THE HUMAN RIGHTS REVIEW

If the Human Rights Review Tribunal is satisfied that the defendant's action has interfered with the privacy of an individual it may grant one or more of the following remedies:

- Declare that the action of the defendant is an interference with privacy;
- Issue an order restraining the defendant from continuing or repeating the interference;
- Award damages;
- Issue an order requiring the defendant to remedy the interference;
- Order such other relief as it thinks fit.

ENFORCEMENT

Took out the 1st paragraph. 1996 is quite a long time ago.
The Director of Human Rights Proceedings may bring proceedings in respect of an action that interferes with someone's privacy (including a class action) and any aggrieved person has the right to proceed directly to the Human Rights Review Tribunal to obtain orders, and possible compensation and/or damages.

FURTHER POWERS OF THE PRIVACY COMMISSIONER

In addition to the powers outlined under the heading "Complaints", the Privacy Commissioner has a number of other powers.

The Commissioner may authorise an agency, subject, if necessary, to certain conditions, to collect, use or disclose personal information, in breach of principles 2, 10 or 11, if satisfied that in the special circumstances of the case the:

- public interest in collection or disclosure substantially outweighs the interference with the privacy of the individual concerned;
- collection (or disclosure) involves a clear benefit to the individual concerned that outweighs any interference with his or her privacy.

Authority will not be granted if the individual concerned has refused to authorise the collection, or the use or disclosure of the information requested for the purpose in question.

The Privacy Commissioner may publish any of the following information:

- nature of any personal information held by any agency;
- purpose for which any personal information is held by any agency;

- classes of individuals about whom personal information is held by any agency;
- period for which any type of personal information is held by any agency:
- individuals who are entitled to have access to any personal information held by any agency, and the conditions under which they are entitled to have that access;
- steps that should be taken by any individual wishing to obtain access to any personal information held by any agency.

INFORMATION MATCHING BETWEEN GOVERNMENT AGENCIES

Subject to controls, certain government departments and agencies may exchange information.

Government agencies between which information matching will be permitted include:

- The Accident Compensation Corporation;
- The Customs Department;
- The Ministry of Justice;
- The Ministry of Business, Innovation and Employment;
- The Department of Social Welfare;
- The Inland Revenue Department;
- The Ministry of Education;
- The Registrar-General under the Births, Deaths Marriages and Relationships Registration Act 1995.
- WorkSafe New Zealand

PUBLIC REGISTERS

A number of principles also apply to Public Registers.

The principles cover information supplied compulsorily for public registers, such as births and deaths.

Breaches of codes of practice or of the public register privacy principles can lead to a Privacy Commissioner's report, plus recommendations, to the relevant Minister. The Commissioner can also make general recommendations to Ministers about their registers.

LIABILITY OF EMPLOYERS AND PRINCIPALS

Employers are liable for anything done, or omitted, by an employee in the course of employment, whether or not it was done, or omitted, without the employer's knowledge or approval.

However, it is a defence for an employer to prove that he or she took reasonably practicable steps to prevent an employee doing (or not doing) the action complained of.

OFFENCES

Obstructing or hindering the Commissioner or knowingly providing the Commissioner with false statements are offences for which the maximum fine on summary conviction is $2,000.

COMMON QUESTIONS AND ANSWERS

Question 1: What is meant by an "agency"
An agency is a private or public sector organisation or person, including both private and public sector employers. For the purposes of compliance with the Act “agency" can be read as standing for "employer" (although as well as employee information, personal information from clients and customers is also covered).

Question 2: What is meant by an "individual"?
An individual is a natural, living person, not a legal person (such as a company).

Question 3: What is meant by personal information?
Personal information is information (e.g. medical history) about an identifiable individual, in other words, about a known, living individual. It can include written documents, video and oral recordings.

Question 4: What information can be kept on personnel files?
Although the type of information employers will want to keep will vary from business to business and from one organisation to another, all employers will keep certain information such as name, address, kind of work on which employed, tax file number, copies of employment agreements, performance appraisals and so on.

In some industries a prospective employee will have been required to undergo a pre-employment medical and the results of this, and any subsequent medical, examination, will be retained.

Warnings given to an employee must be recorded (for use in the event of any future personal grievance claim) and it may also be appropriate to note any special commendations received, together with comments on work attitude and/or ability.

Terminating employment on the basis of information which has not first been brought to the employee’s attention could lead to a claim of unjustified dismissal.

Information must not be collected by unfair or unlawful means and should always be accurate, up-to-date, complete, relevant and not misleading.

Question 5: Should information be kept on ex-employees?
Precisely what information is kept will depend on the particular employing organisation. No information should be kept longer than necessary for the purposes for which it may lawfully be used. For example, information used as a basis for a demotion or dismissal must be retained for at least 90 days from the time the action was taken, that is, for the period of time during which a personal grievance may be raised with the employer. However, a longer period is desirable since there are circumstances in which a grievant may granted an extension of the 90-day period. Wage and time records must be retained for six, and tax records for seven, years.

Question 6: Should information be kept on job applicants?
Information on job applicants should be kept for at least 12 months. This is because a rejected job applicant may appeal against the appointment made, particularly if he or she believes discrimination on one of the grounds prohibited by the Human Rights and Employment Relations Acts was the reason for his or her rejection. Then a complaint may be made to the Human Rights Commission up to 12 months after the alleged discrimination occurred or the grievance may be raised with the employer under the Employment Relations Act’s personal grievance provisions (with the possibility of an investigation by the Employment Relations Authority). Also, in some cases the retention of personal information will enable an unsuccessful applicant to be offered employment in the future should a subsequent vacancy occur.

Question 7: What right of access do employees have to file notes relating to disciplinary procedures?
Employees have full access to notes of disciplinary interviews, warnings given and so forth and are entitled to seek correction where such information (or, in fact, any information) is considered by them to be inaccurate. If a correction is refused, reasonable steps must be taken to ensure any employee statement about the correction sought is attached to the information, to be read together with it.

The statement of correction should be forwarded to anyone else receiving the information about the employee or who has already received it.

Question 8: May employees see their personal performance appraisals?
Access to personal performance appraisals cannot be denied unless these are done by some third party outside the employing organisation. Although it is permissible to withhold evaluative material in the nature of a reference - where it is provided to determine suitability, eligibility, or qualifications for employment, promotion, continuance in employment, or removal from employment - this can only be done if the person providing the material has asked that it, and/or his or her identity, be kept confidential. It is not likely that access could be refused to performance appraisals supplied in-house.

Question 9: When may an employer refuse to disclose information?
Employers may refuse access to personal information if disclosure would be likely to:

- damage the security or defence of New Zealand or the country's international relations (or those of the Cook Islands, Niue, Tokelau or the Ross dependency);
- be detrimental in respect to any information entrusted, on the basis of confidence and trust, to the New Zealand government by some other government or international organisation;
- undermine the maintenance of law and order, including the prevention, investigation and detection of offences and the right to a fair trial;
- endanger the safety of any individual;
- result in the disclosure of a trade secret;
- affect unreasonably the commercial position of the person who supplied or was the subject of the information (although these latter two points will not apply in any case where for them to apply is contrary to the public interest);

or if:

- disclosure would involve the unwarranted disclosure of someone else's affairs or the affairs of a deceased person;
- non-disclosure was requested when evaluative material (such as a reference) was supplied (see *"Refusal of Access to Personal Information"*);
- the employer is satisfied that disclosure would be likely to prejudice the employee's physical or mental health (after consultation, where practicable, with an employee's doctor);
- disclosure would be contrary to the employee's interests in the case of an employee under the age of sixteen;
- disclosure would breach legal professional privilege;
- disclosure of information contained in material placed in a library, a museum or an archive would breach a condition subject to which the material was placed there;
- disclosure would constitute contempt of court or of parliament;
- the request for disclosure is frivolous or vexatious;

or if the information requested:

- Is not readily retrievable (see question 11);
- does not exist or cannot be found;
- is not held by the employer concerned and the person dealing with the request has no grounds for believing that the information is either held by another agency or is more closely connected with the functions and activities of another agency.

Question 10: May employers video their employees?
Videoing employees is permissible in certain limited circumstances.

Unless there is some good reason why not, employers should notify employees when video surveillance is to be undertaken and, if possible, secure their agreement to it. However, there may be times (as in the case of suspected misuse or appropriation of company property) when there is good reason to undertake some limited covert video surveillance. Where this is done, the employer should clearly record the purpose of the surveillance which should take place only at relevant periods and be limited to the collection of personal information relevant to the investigation. For example, if thefts are occurring after work, or at lunch time, those are the times when surveillance should be carried out. Except where some extraordinary reason exists, surveillance should not include areas where complete privacy is normally to be expected (such as toilet and washroom facilities).

Where video surveillance is to be undertaken, the employer should determine in advance how long the tape is to be kept and who is to have access to it. Contents should not be disclosed other than for the purpose for which the surveillance was carried out, and the video must be protected from loss, unauthorised access, misuse and so on (as provided in privacy principle 5). Parts of the video not relevant to the investigation should be erased as soon as possible. Additional tapes should not normally be made.

Video surveillance for external security purposes should be notified, its purpose recorded, and the video kept for a predetermined time. It should also be subject to security measures and be disclosed only for the purpose for which the surveillance was undertaken. Signs should be prominently displayed so that casual visitors/customers know of the surveillance.

Videoing an employee to determine work habits is not acceptable.

The same points apply to listening-in on employee conversations as apply to covert videoing.

Question 11: Is testing for drug or alcohol abuse permissible?
Nothing prevents employers asking employees or prospective employees to undergo drug or alcohol testing but the privacy principles will apply to the process requiring that employees must be told why the information is sought, who will see it, and be allowed to have access to it. Employees must agree and cannot be forced to take a drug test.

Random drug testing is permissible in safety sensitive areas but as what constitutes a safety sensitive area will depend on the particular circumstances, it would be better for employers who might otherwise consider random testing to adopt, and ensure their employees' are aware of, a drug and alcohol testing policy.

Question 12: What is meant by "readily retrievable" information?
Provision is made for the non-disclosure of not readily retrievable information and although what this means is not spelled out, it is likely to refer to information whose retrieval would involve an excessive amount of time and/or difficulty.

Question 13: When an employee asks to see his or her personal file must that employee be allowed to take the file away to inspect or to copy?
Access must include an opportunity to inspect documents, or if requested, to be provided with copies. Within reason the information must be provided in the way preferred by the employee seeking access. There is nothing in the Act that requires unsupervised access. Employers should generally not allow files to be taken away out of their control. In certain circumstances, evaluative material need not be provided (see question 8).

Question 14: May employees have access to references from third parties?
An employee is entitled to see any reference which was provided in the knowledge or expectation that it would be given to the employee concerned.

There is no obligation to disclose either the contents of any reference, or the identity of the person who supplied it, where an employer has expressly promised or has implied, that these will be kept confidential.

This is something employers need to be aware of when they themselves provide references, and it should be taken into account both when the information is collected and when it is given out.

Question 15: May a former employer provide a prospective employer with a reference without the employee's consent?
Since the general rule is that (with certain exceptions) information must be collected directly from the individual concerned, the ex-employee's permission will be needed before a reference can be provided. While, from the prospective employer's point of view, it might be thought that the exception allowing collection from a source other than the employee would apply if the direct approach would prejudice the purposes of collection, from the point of view of the ex-employer there is no exception allowing information to be disclosed in the absence of consent.

It is good employer practice to obtain prior permission from employees so that references can subsequently be given on their behalf without the need to seek specific consent at a later date. Should permission for a prospective employer to approach a former employer or employers for a reference be refused, it will be for the prospective employer to draw his or her own conclusions.

Question 16: May an employer supply a credit reference for an employee (particularly where the information relied on has been gathered for some other purpose)?
If the employee agrees to information being used for a purpose other than the purpose for which it was collected, the employer is free to give a credit reference. But if the employee does not authorise disclosure, then giving a credit reference is not one of the exceptions that allow disclosure to be made in the absence of consent.

Question 17: May an employer charge for the cost of retrieving information?
Private sector employers may impose a reasonable charge for access to personal information, having regard to the labour and materials involved in making information available in accordance with a request. Public sector employers may only charge in limited circumstances (as where they can satisfy the Privacy Commissioner that they are commercially disadvantaged in comparison with private sector competitors by the inability to charge).

Question 18: May employers maintain personal files in alphabetical order?
Employers may list files alphabetically with employees' names attached. A unique identifier may be assigned if this is necessary to enable the employer to carry out any one or more of its functions efficiently. An employee's name is not classified as a unique identifier.

Question 19: May employers assign payroll numbers to their employees?
Yes, provided the reason for assigning payroll numbers is to enable the employer to carry out any one or more of its functions more efficiently, for example, to facilitate wages and employer superannuation scheme payments.

Question 20: May the trustees or administration manager of a company's superannuation scheme use a number assigned to an individual for company purposes for superannuation scheme purposes?
Yes, the Superannuation Schemes Unique Identifier Code permits this but without the Code, doing so would not be permissible. Principle 12 does not normally allow one agency to use a number assigned by another agency e.g. employers may know their employees' IRD numbers but may not use these for company purposes.

Question 21: What relationship exists between the Privacy Act and the Official Information Act 1982?
The Privacy Act is concerned only with *personal* information held by the state and private sectors (including information about employees), whereas the Official Information Act relates to information held by state organisations (Government Departments, Ministries, Producer Boards, Universities and so forth) that may or may not be personal in nature. Both state and private sector employees should, therefore, seek personal information under the Privacy Act, and take any subsequent complaint in terms of that Act. Both Acts, however, make provision for consultation between the Privacy Commissioner and an Ombudsman in cases where any doubt arises as to which office should deal with a particular complaint. Some complaints relate to information which is a mix of personal and "public" and are more appropriately dealt with by an Ombudsman. It is also possible that consultation might establish that rather than dealing with a complaint under the Official Information Act, it would be better dealt with, wholly or partly, under the Ombudsmen Act 1975, or under the Local Government Official Information and Meetings Act 1987.

Question 22: Is provision made for the Privacy Commissioner to refer some complaints on to an official other than the Ombudsman?
Yes, depending on circumstances the Privacy Commissioner may consult with the Health and Disability Commissioner, determine a complaint should be dealt with under the Health and Disability Act and refer the complaint accordingly. Provision is also made for the referral of complaints, if appropriate, to the Inspector General of Intelligence and Security and to an overseas privacy enforcement authority. In the latter case, the Commissioner must consult with the authority and determine that the complaint should be referred and the authority and the complainant must agree.

It is important to note that in any given situation, the particular facts will determine whether or not the Act's privacy principles have been contravened. Where there is any doubt, employers should consult their regional employers' organisation.

End.