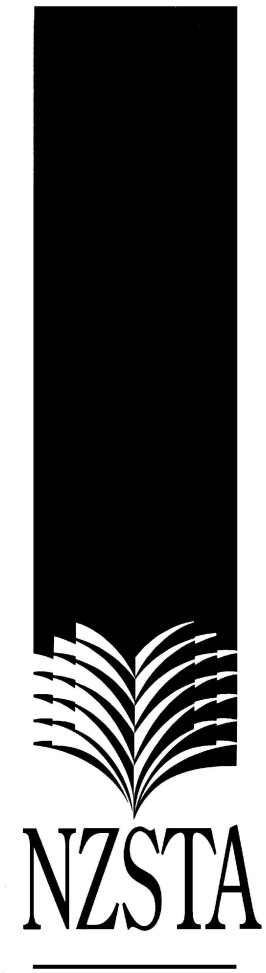


Guidelines for Boards of Trustees

Privacy Act 1993

A Publication for Members of the New Zealand School Trustees Association

PRIVACY ACT 1993

SECTION ONE - INTRODUCTION

1. THE PRIVACY ACT AND THESE GUIDELINES

The Privacy Act 1993 provides controls in the handling of personal information and gives rights and protections to individuals. It covers boards of trustees just as it covers most other agencies in the public or private sectors.

Complementing this is the Official Information Act 1982 (OIA) which also deals with the release of information. These guidelines focus on the Privacy Act and personal information. Boards do need to be aware that requests made by individuals for information about themselves must be dealt with under the Privacy Act (even though it is also, technically, official information). All other official information must be considered under the OIA. This includes personal information about identifiable individuals other than the requester, or which otherwise affects the privacy of individuals "*Privacy gets considered – but it gets considered under the privacy withholding grounds of the OIA*."[1].

The aims of the Privacy Act are achieved through 12 information privacy principles which govern the way that agencies, such as school boards of trustees, may collect, share, use, allow access to, and disclose personal information. The Act, however, does not seek to hinder schools from achieving their education objectives in the way that they choose, provided this can be achieved in a way which is consistent with the information privacy principles.

These guidelines are therefore not designed to provide specific answers to all potential situations that a board or school may be faced with. Rather the guidelines endeavour to assist in complying with the information privacy principles in a way which respects privacy but which also suits the board of the school concerned.

The guidelines therefore place a particular emphasis on explaining the relevance of the information and privacy principles in a school situation and, where appropriate, suggest possible solutions on how school objectives can be achieved consistent with these principles.

There are often several different ways to comply with particular privacy principles. The Privacy Act is designed to enable agencies to choose solutions which respect privacy but which suit the particular agency concerned. On some issues two schools might handle information in quite different ways and yet both comply with the Privacy Act. Neither the Privacy Act nor these guidelines seek to hinder schools in achieving their educational objectives in the way they choose as long as those can be done consistently with the principles. Accordingly, the guidelines seek to explain the relevance of the principles to schools and also, where appropriate, suggest possible solutions.

In some places these guidelines paraphrase the privacy principles, parts of the Privacy Act, and provisions in other laws. It is suggested that when making important decisions in reliance on a particular provision in a statute, or an exception to one of the principles, reference is made to the exact wording of that provision or exception. However, it is not necessary for every member of a school board, or every school principal or staff member, to be an "expert" on the Privacy Act. Each school must appoint a privacy officer and it is that person who should be familiar not only with these guidelines but with the Privacy Act itself.[2]

A full copy of the information privacy principles is set out as an appendix to these guidelines. This enables boards to refer to the exact wording of principles referred to in the guidelines.

---

[1] Privacy Commissioner June 2005 presentation to FOI Live Conference

[2] Throughout these guidelines relevant provisions of the Privacy Act 1993 are footnoted. It is not expected that most readers will need to refer to these provisions to get a general understanding. However, privacy officers should familiarise themselves with these provisions.

2. KEY ASPECTS OF THE PRIVACY ACT

Below is an overview of the key aspects of the Privacy Act, as it impacts on boards and schools. These areas are discussed in more detail throughout this publication.

PART II - Information Privacy Principles

- Section 6 sets out the 12 principles which give effect to the aims of the Act.
- Section 7 provides that if the action is authorised or required by law, then it is not in breach of the principles of the Act.

PART IV - Good Reasons for Refusing Access to Personal Information

- Part IV of the Act sets out the situations where a board [or staff] may refuse to disclose information sought under principle 6.
- Section 29 sets out those reasons for refusal of requests which are most likely to be relevant to schools.

PART V - Procedural Provisions in Relation to Access to and Correction of Personal Information

Of particular importance are:

section 38	which outlines the duty on agencies to give reasonable assistance to individuals making requests for privacy information;
section 39	which deals with the transfer of requests;
section 40	which determines the time-frame within which a request must be dealt with;
section 41	which allows some extension of time limits;
section 42	which sets out the ways information may be made available;
section 43	which provides for deletion of information from documents, where good reason exists; and
section 44	which requires reasons for refusal to be given.

3. SOME KEY CONCEPTS AND TERMS USED IN THE PRIVACY ACT

The information privacy principles are concerned with the handling of "personal information". "Personal information" means information about an identifiable living individual.[3] Accordingly, the Act is not concerned with information about deceased people. (Care still needs to be taken though, particularly with recently deceased individuals, such as a student who dies while at school, since there are family sensibilities to respect. Sometimes information about the pupil may also refer to someone else, and therefore be "personal information" about that other living person).

Neither is the Act concerned with information about artificial entities such as the Ministry of Education or the New Zealand School Trustees Association (NZSTA) (although, if information about the Ministry or NZSTA also refers to an individual it may still be "personal information"). Nor does "personal information" encompass statistical data from which an individual cannot be identified.

The Privacy Act contains some provisions concerning liability for actions which breach the Privacy Act.[4] Generally the privacy principles focus upon the actions and policies of the "agency", that is the board of trustees of the school, rather than the individual staff member who might be handling the personal information. The Act does, however, impose a liability on an agency for the actions of the agency's employees in respect of acts done in the performance of that person's employment.

[3] Privacy officers should refer to section 2 of the Privacy Act 1993 to see the definitions of "personal information" and “individual”.
[4] Privacy officers and boards when they are considering matters of liability should have regard to sections 3(4), 4 and 126 of the Privacy Act 1993.

However, an employee who, say, discloses information, may nonetheless carry some liability under the Act as well, or instead of, the board of that school, if that person acted in circumstances outside their employment, for example knowingly in contravention of a policy of the school that specified information not be disclosed to a particular person.

Accordingly it is important that boards not only observe the privacy principles in relation to their own decisions and in establishing school policies,[5] but also that staff who may handle personal information are made aware of their responsibilities. The privacy officer has a key role here.[6]

4. INFORMATION PRIVACY PRINCIPLES

The Privacy Act contains 12 information privacy principles. The principles are set out in full in the appendix but a summary follows:

Principle 1

Purpose of collection of personal information: Personal information must not be collected by a board (or staff) unless:

- the information is collected for a lawful purpose connected with a function or activity of the school; and
- the collection of the information is necessary for that purpose.

This principle (and principles 2-4) applies to information collected after 1 July 1993.

"Collect" does not include unsolicited receipt of information.[7] For example if parents write to a school of their own accord, information has not been "collected" and the first 4 principles will not be relevant. (Storage and use of that letter must, however, be considered - see principles 5 onwards).

This also extends to situations where videos or photographs are taken or used, particularly on websites or security cameras.

The Ministry of Education has published Guidelines for schools on the online publication of student images and schoolwork (see Section Six).

Principle 2

Source of personal information: Where a board (or staff) collects the personal information, it must collect the information directly from the "individual concerned" unless one of the exceptions to the principle applies. The phrase "individual concerned" is used throughout the Act and means the person who the information is about. It is not necessary for a board (or staff) to collect information directly from the individual concerned if it is believed on reasonable grounds that:

- the information is publicly available information;[8]
- the individual concerned authorises collection from someone else;
- the non-compliance would not prejudice the interests of the individual concerned;
- collection from another source is necessary to avoid prejudice to the maintenance of the law;[9]
- collection directly from the individual would prejudice the purposes of the collection or is not reasonably practicable in a particular case; or

[5] See, for example, principle 5(a)(ii).
[6] See section 5 of this publication for the role of the privacy officer.
[7] Refer to definition of “collect” in section 2 of the Privacy Act 1993.
[8] “Publicly available information” is defined in section 2 of the Privacy Act 1993.
[9] The full exception is more complicated than this: see principle 2(2)(d).

- the information will not be used in a form in which the individual is identified or will be used for statistical or research purposes and will not be published in a form that could identify the individual concerned.

In some limited circumstances a departure from principle 2, 10, or 11[10] can be authorised by the Privacy Commissioner.

A board (or staff) intending to rely on an exception in this or the other principles must be able to prove it applies, should they be challenged on the matter.[11]

Principle 3

Collection of information from subject: Where a board (or staff) collects personal information directly from the individual concerned, it must take such steps (if any) as are, in the circumstances, reasonable to make sure that the individual concerned is aware of:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;
- the name and address of the agency collecting the information and the agency that will hold the information; and
- if the collection is authorised or required under law, the details of that law and whether supply is mandatory or voluntary;
- the consequences (if any) if the individual does not provide all or part of that information;
- the rights of access to, and correction of, personal information provided by the principles.[12]

There are exceptions to this principle which are detailed in the Act.[13]

Individuals are to be made aware of the above matters before the information is collected (e.g. by an explanation on the form that is to be filled in). If that is not practicable they should be made aware as soon as possible after collection.[14]

Principle 4

Manner of collection of personal information: Personal information must not be collected by:

- unlawful means;
- unfair means; or
- unreasonably intrusive means.

Principle 5

Storage and security of personal information: A board (or staff) must make sure that reasonable safeguards are taken to protect personal information they hold against loss, or unauthorised access, use, modification or disclosure, or misuse.

This principle applies to all personal information whenever it was obtained.

Software and electronic security

With the increased use of computer-based human resources information systems, it is appropriate to make specific recommendations regarding software security. The factors to be considered include ensuring the reliability and integrity of the software to ensure that it performs according to specification; incorporating checks to validate the input of data to the system; providing back-up and restore facilities to ensure that the system can recover data; duplicating data on a regular

[10] The Privacy Act 1993, section 54.
[11] The Privacy Act 1993, section 87.
[12] The rights of access and correction are found in principles 6 and 7.
[13] See principle 3(4).
[14] See principle 3(2). There is an exception in principle 3(3) which allows explanations to be dispensed with if the same explanation in relation to a similar collection has been given by the agency to the individual on a recent occasion.

basis and removing it to a safe and secure site; and training of staff in the use of the system and their responsibility to maintain information privacy. The use also of information systems and websites can further extend the need for broad based policies to ensure safeguards for staff and students personal information.

Principle 6

Access to personal information: This provides that individuals concerned are entitled to know whether the agency holds such personal information, and if so, can have access to that information and may request correction of the information.

Principle 7

Correction of personal information: This provides that individuals may request correction of information held. If a correction is not made, the individual may require that there be attached to the information a statement of the correction sought.

Principle 8

Accuracy etc, of personal information to be checked before use: This requires agencies to take reasonable steps to make sure personal information is correct, up to date, relevant, and not misleading before they use it. What is reasonable is not specified and will depend on various factors.

Principle 9

Agency not to keep personal information for longer than necessary: A board (or staff) must not keep personal information that it holds for longer than is required for the purposes for which that information may lawfully be used.

Principle 10

Limits on use of personal information: This provides that information may not be used for a purpose other than that for which it was collected, except under conditions contained in the Act. This principle applies to information obtained after 1 July 1993.

Principle 11

Limits on disclosure of personal information: This prevents agencies from passing on or disclosing personal information to other people or agencies except under conditions contained in the Act.

Principle 12

Unique identifiers: This principle specifies how agencies may use unique identifiers. These include things such as IRD numbers, customer numbers, etc, but do not include a person's name.

Unique identifiers may not be used unless it is necessary for the agency to be able to carry out its functions. The same unique identifier may not be used by more than one agency. Where a unique identifier is used, agencies must take reasonable steps to make sure that they are only given to people whose identity is clearly established.

Agencies cannot ask people to disclose any unique identifier given to them by another agency unless that was one of the reasons the unique identifier was given or is directly related to the purpose for which the unique identifier was given (e.g. IRD numbers).

In education there is a National Student Number (NSN) that can be used by authorised users for the following approved purposes (all other uses are prohibited):

- monitoring and ensuring a student's enrolment and attendance;
- ensuring education providers and students receive appropriate resourcing;
- statistical purposes;
- research purposes; and
- ensuring that students' educational records are accurately maintained.

5. THE IMPACT OF OTHER LAWS ON THE ACT

Where another Act or regulation authorises or requires personal information to be made available, a board (or staff) will not breach the Privacy Act principles if it provides that information. An example of another Act which may require a board (or staff) to provide personal information is section 11 of the Social Security Act 1964 which allows the Ministry of Social Development to obtain information to determine whether a person is entitled to the benefit they receive.

When a request for personal information is made to a school, the board (or staff) need to consider the request carefully. If it is a request from an agency such as the Ministry of Education and the disclosure of the information to it would be consistent with the purpose for which it was obtained, it is likely that the school will be able to comply with the request without breaching the Privacy Act, e.g. collection of information for statistical purposes (section 144A, Education Act 1989).

If an agency requests personal information from a board (or staff), using specific statutory powers of collection, the school may wish to take steps to ensure it is able to disclose that information without breaching the Privacy Act. To do this the board [or staff] may wish to ask the agency requesting the information to put their request in writing and to provide a copy of the statutory provision it relies on. A decision can then be made on whether the information can be disclosed.

If the board (or staff) provides personal information to an agency that does not have the statutory authority to require it or provides more information than the legislation authorises, then the board (or staff) might be in breach of the Privacy Act.

The use of the OIA can impact on the process as well. Boards do need to be aware that requests made by individuals for information about themselves must be dealt with under the Privacy Act (even though it is also, technically, official information). All other official information must be considered under the OIA. This includes personal information about identifiable individuals other than the requester, or which otherwise affects the privacy of individuals.

6. DOES AUTHORISATION NEED TO BE IN WRITING?

Many of the principles permit actions which are done with the authority of the individual concerned. The Act does not specify what constitutes authorisation or that it must be in writing. Written authorisation provides clearer proof that an exception may apply if someone later makes a complaint. Where a board (or staff) knows in advance that it will need authorisation to act in a certain way, the most practical way of recording that a person has provided their authorisation will be to include it in an existing form, for example an enrolment form or an application for a vacancy.

Where oral authorisation is given, it is advisable to record it in writing including the time, date, and nature of the authorisation.

7. THE PRIVACY ACT AND SCHOOL OBJECTIVES

The Privacy Act does not seek to hinder school boards from achieving their objectives. Indeed, under section 14(a), the Privacy Commissioner is obliged to take into account the general desirability of a free flow of information and the recognition of the right of Government and business to achieve their objectives in an efficient way when he exercises his powers under the Act.

The objectives of school boards are found in their Charter, the National Education Guidelines, and legislation - particularly the Education Act. Boards of trustees have broad objectives. These include: educating students; employing staff; and controlling the management of schools.

SECTION TWO - DISCLOSING INFORMATION

8. GENERAL

This section contains general information about disclosing information to parents, students, and other agencies/schools.

9. WHAT INFORMATION MAY PARENTS RECEIVE ABOUT THEIR CHILD?

9.1 DO PARENTS HAVE A RIGHT TO ACCESS PERSONAL INFORMATION ABOUT THEIR CHILDREN ?

The Privacy Act provides amongst other things for access by individuals to information about themselves. Thus, under the Privacy Act, it is the child who has the right to access its own information. Exceptions exist where there are statutory rights of access given to parents. A clear example of such a right is section 77(b) of the Education Act 1989 which requires the principal to tell a student's parents:

> "of matters that, in the principal's opinion
> (i) are preventing or slowing the student's progress through the school; or
> (ii) are harming the student's relationships with teachers or other students."

Parents must be given such information.

In cases where there is no statutory right to information about their child, parents may make a request under the Official Information Act 1982 for access to such information. Boards of trustees are subject to that Act and must provide the information requested unless there is good reason not to. Grounds establishing "good reason" are set out in sections 6, 9, and 18 of the Act (the most generally relevant being section 9). A school may consider that it should not provide the information requested, for example, to protect the child's privacy (section 9(2)(a) Official Information Act). The school must then consider whether there is a public interest which would override that consideration i.e. is there an overriding public interest in the parent being given access to that information? The public interest which could encompass the interests of both children and parents is parents' responsibilities for the upbringing of their children. If on balance the school considered that the public interest overrode the child's interest in privacy, it would be within its rights to provide access to the parents. **Each case must be considered on its own facts**.

In difficult situations, particularly where the child is too young to have a view, the school should consider whether it is in the child's best interests to provide the information requested. In making such a decision care will need to be taken.

(a) There may be occasions when the child's right to privacy would clearly outweigh any public interest in providing access to the information.

Such an occasion would include where the child is alleging abuse by the parents. Another occasion might be where the child is of an age where it is able to make mature judgements on its own behalf and decides that the information should not be given to parents. An example is a case where the Ombudsman held that information could be withheld from a parent on the basis that the child was mature enough to consider that it should not be provided. In addition the child had had no contact with the requesting parent for some years. In that case the Ombudsman found that as

section 77 information was not involved there was no public interest which overrode the student's right to privacy.[15]

(b) Even where the facts might lead the school to decide against giving access to all information requested by the parents, it should consider whether it is possible to give access to part of the information, deleting the information raising the particular concern.

On occasions the school could make that decision itself but on other occasions it may be necessary to consult the child.

Right of Correction - Principle 7

There is one particular area relating to access to personal information which is not covered by the Official Information Act and which raises questions about the importance of the need for parental access to personal information about a child. That is the area covered by principle 7: the right to request correction of personal information. Under the Privacy Act 1993 the right to request correction rests only with the individual concerned. In the case of a child who is too young to be able to assess whether information is correct, this could have unfortunate if not serious consequences (obviously, where the question of correction arises, the school would have already considered whether the parent should have access and have given it). If the parent said that some of the information was incorrect and asked for it to be changed, the next question to be asked would be, what is the school's responsibility in this case? There is clearly no absolute duty on the school to make any correction because the Privacy Act 1993 does not apply in this situation. Common sense and the child's best interests should prevail. At the very least the school could grant the parent the opportunity to request the correction and attach it to the information if the school does not believe that it would be right to change it.

9.2 What information may the board (or staff) provide to parents and caregivers about their children?

Boards (or staff) may be able to provide information to parents because they are required to under the Education Act or because they are able to rely on an exception to principle 11.

- Section 77 of the Education Act[16] obliges principals to inform a student's parents or caregivers of any matter that they believe is preventing or slowing the student's progress or harming their relationship with teachers or other students. Information about a student which falls into this category may, therefore, be provided to parents or caregivers.

- Principle 11 provides that personal information may not be disclosed to any person, body, or agency unless one of the stated exceptions applies. There are a number of exceptions. It will not, for example, be a breach of principle 11 to provide personal information to the individual concerned or with the authorisation of that individual concerned.

- Personal information may also be disclosed where that disclosure is one of the purposes for which the information was obtained. There is a good argument that one of the reasons that schools record information about a student's progress is to be able to report on their progress to their parents or caregivers. This is because National Administration Guideline 1(v)[17] requires boards to assess student achievement, maintain individual records, and **report on student progress**.

Principle 11 gives the school a **discretion** to provide information. The Privacy Commissioner considers that it does not give a parent or caregiver the right to require that it be provided. This

[15] See Case No.s W32982 & W34275 Sir Brian Elwood, and Case No, A5861 Anand Satyanand.
[16] See section 1.5 of this publication, *The Impact of Other Laws on the Act.*
[17] Under section 61 of the Education Act 1989 every charter is deemed to contain the aim of achieving, meeting, and following the national education guidelines.

allows the board (or staff) to refuse to provide personal information if it considers it inappropriate in the circumstances to do so.

9.3 Parents' right to access personal information about themselves

Parents have the right under principle 6 to access any personal information about themselves held by the school. Parents must be given access to that information unless a good reason exists to refuse e.g. where the child alleges abuse (see 10.3(d): *Guidance Counsellor*).

10. SHARING INFORMATION WITH OTHER SCHOOLS/ AGENCIES

10.1 Sharing information with other schools

The National Administration Guideline 1(v) requires boards of trustees, through principal and staff, to:

"assess student achievement, maintain individual records and report on student progress"

If a student transfers to another school can records of progress and achievement be transferred?

Yes, on the basis that the transfer of information is "directly related to purposes in connection with which the information was obtained" (principle 11 (a)). The information was collected for educational purposes and may be passed on for the same reason, to ensure that the student has appropriate education provided.

10.2 Information should be provided on a "need to know" basis only.

It is important to ensure that only relevant information from the school record is released. It is a good idea to have a consistent policy covering information that will routinely be passed on. A policy might refer to the need to pass on information relating to subjects studied, attendance record, and immunisation/routine medical checks for example. Whether matters such as family history and sensitive personal details should be passed on should be considered on a case-by-case basis.

The relevance of such information to the pupil's education is an important factor.

"Is it in the child's best interest?" will be a useful yardstick in making such a decision.

10.3 Sharing information with other agencies

As stated above, information should be passed on, on the basis of who needs to know this information about the student, and why they need to know it. The following is information regarding the Privacy Act and other agencies that sometimes operate in schools.

(a) *Dental Nurses*
Dental nurses are employed by the local DHB so that providing information to them is disclosing information to another agency.

Why would a board (or staff) provide information to the dental nurse?

- to assist him/her to ensure that every child enrolled at school is enrolled at the dental clinic or has been given the opportunity to refuse treatment.
- to enable him/her to check with the school the whereabouts of a pupil who has not arrived for treatment.
- to know of any pupil transferring into the school so that he/she can contact the parents for authority to obtain dental records from the previous school.

- to provide health information about a pupil relevant to dental care e.g. a recently discovered medical condition. (**NB**: Principle 11 (f) would enable the school to convey information where that was necessary to "prevent or lessen a serious and imminent threat to- (ii) the life or health of the individual concerned").

There are a number of ways for a school to pass information on to the dental nurse. It can be done by:

- requesting that the person enrolling the child complete the dental clinic enrolment form.

- informing the person enrolling the child that information such as their telephone number will be passed to the clinic so that the clinic can approach them directly about enrolling their child.

(b) *Medical Officers / Medical Officers of Health and Public Health Nurses*

The sole responsibility of the board for public health examinations is in providing a venue. It is the health service provider's responsibility to seek such consents as may be necessary.

Section 125 of the Health Act 1956 permits a person authorised by the Minister of Health to enter schools at all reasonable times to examine children.[18]The powers of section 125 override any requirements under the Privacy Act to obtain consent from the child, the child's parents or guardians, or the school staff/board. In practice, however, Ministry guidelines require prior parental consent to medical examinations.[19]

The use of the powers under section 125 would therefore usually be restricted to situations where the consent of a parent or guardian has not been obtained or it is not clear whether it has been obtained and either:

- the requirement for parental consent would prevent the carrying out of routine screening

OR

- there could be significant risks to the health of a child [or other children] if the examination was not carried out.

This would occur either:

- when a health problem which requires treatment is suspected and reasonable attempts to contact the parent or guardian have failed

OR

- when abuse or neglect is suspected and it is considered that a parent or guardian might refuse permission for an examination to be carried out.

Provision of information about students to the health service provider

As with passing on information to dental nurses, disclosing information to medical officers of health will often be one of the purposes for which the information has been collected (most commonly at the time of enrolment). This collection is likely to include specific information about students which might be affecting their ability to learn e.g. eye or ear problems.

[18] Health Act section 125 authorises a medical officer or nurse employed by or contracted to the Ministry of Health to attend a school and examine any child, and to report to parents. Guidelines issued by the Ministry of Health provide that the consent of parents/caregivers for medical examinations should be sought before the powers under section 125 are exercised.
19 Consent in Child and Youth Health: Information for Practitioners (www.moh.govt.nz)

In most cases relevant health information about pupils can be passed on to medical officers/public health nurses without the need for the specific consent of the parent or pupil.

An example of this process was the release of student roll information during the HPV immunisation programme. School boards hold student roll information. A request for this information from the Ministry of Health (and or their immunisation providers) is an Official Information Act (OIA) request. In making such a request the Ministry of Health will specify exactly what information they require from the roll data held by schools.

School boards need to decide whether or not to provide the information requested. When considering the release of the information, boards will need to look first at the OIA principle: release the information unless there is a good reason to withhold it. Boards will then need to consider section 9(2)(a) of the OIA. Under this section a board has good reason to withhold student roll information on privacy grounds. Boards will then need to decide whether there is an overriding public interest in releasing the information (i.e. immunisation programme benefits).

An alternative in this situation is that if boards decide to withhold the student roll information, then the Ministry of Health (and/or their immunisation providers) could request that the boards themselves disseminate information about the HPV Immunisation Programme to parents and students on behalf of the Ministry of Health. Boards may choose whether or not to agree to that request. If a board declines the request, MOH will need to find alternative ways of reaching that community.

Abuse, neglect, emergencies

For non-routine visits by health service providers, that is, where the disclosure of the information could not be said to be one of the anticipated purposes for collecting the personal information, disclosure of personal information about the student may be prohibited. An important exception is where the school has reasonable grounds to believe that non-compliance with the principle is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned, or another individual.[20]

Where a health professional is called into a school to examine a child for suspected child abuse or neglect, this is the exception that will be most likely to justify disclosing the information.

When child abuse or neglect is suspected, no civil or criminal action can be taken against a board or any individual for that person notifying a member of the Police, Child Youth and Family (CYF), or a social worker.[21]

Confidentiality of the notifier can not be guaranteed though. When a request is made under the Privacy Act the information will be released, unless there is a reason to withhold it (for example the client has a history of violence and has threatened or abused staff on previous occasions, or the client is closely related to the notifier).

For more information refer to the protocol between MoE, Child Youth and Family (CYF) and NZSTA on the reporting of (suspected) child abuse. This protocol was signed in September 2009 and will be available on www.nzsta.org.nz.

Immunisation

While not a Privacy Act requirement, the Ministry guidelines[22] require that consent for immunisation must be obtained in all cases. There may be difficulties where consent forms are not returned. It is, therefore, useful for boards and staff to work closely with health providers to ensure that consent is obtained. See above regarding the provision of information in these circumstances.

[20] See Privacy Act 1993, principle 10(d)(i).
[21] Children, Young Person and Their Families Act 1989 section 16.
[22] Consent in Child and Youth Health: Information for Practitioners (www.moh.govt.nz)

Medical treatment

Section 125 relates to medical examinations only. Except for emergency first aid, no treatment is to be given without the specific consent of a parent or guardian.

NB: A board may exclude a pupil who is unclean or has a communicable disease and must, in addition to informing the parents, advise the Medical Officer of Health (section 19, Education Act 1989).

(c) *Using Group Special Education (GSE) staff and RTLB's.*

Schools may call on outside specialist services when they have difficulties with a student. This may be through GSE or the use of RTLB's in a cluster.

Two issues may arise:

- Should they gain parental consent prior to consulting with a specialist service about a student?
- Can a principal provide personal information to a specialist service?

Should you gain parental consent prior to consulting with a specialist service?

Under section 77 of the Education Act 1989

> The principal of a State school shall take all reasonable steps to ensure that:
>
> (a) students get good guidance and counselling

This is the principal's direct responsibility. In calling in GSE the principal is using a specialist service. In this instance the legislation could be said to override the need for the child/parent concerned to be told initially. This will allow the principal to discuss the situation in the first instance.

Section 77 then goes on "and

> (b) a student's parents are told of matters that in the principal's opinion ..."

Once the principal has discussed the matter with the specialist service the the principal must ensure that they have parent/caregiver permission before referring a student to that service..

Can a principal provide personal information to a specialist service?

The information provided to the visiting teacher has been collected for education purposes and to meet the requirements of section 77 (a). Passing this information to the specialist service for assistance to deal with problems related to the education of a student can be seen as one of the purposes for which this information was collected. It therefore fits within principle 11.

(d) *Guidance Counsellor*

- Guidance counsellors employed by a board of trustees are part of the school. Generally they are employed in secondary schools and are performing the principal's role under section 77 of the Education Act so that they may talk to the child without the parent's prior consent.
- Guidance counsellors employed in a separate guidance unit, perhaps attached to a school but serving a number of schools in the same area are in the same position as specialist services.

- Guidance counsellors in the course of talking to students may collect information about parents/caregivers, especially in a sexual abuse or assault allegation.

Parents may request that information. A relevant section in considering such a request may be (section 29(1)(a)) Privacy Act which allows an agency to refuse disclosure where the disclosure of the information would involve the unwarranted disclosure of the affairs of another person i.e. the student. In more serious cases, consider section 27(1)(d) which allows an agency to refuse disclosure if that would be likely "to endanger the safety of any individual".

Reporting ill-treatment or neglect of a child to a social worker or Police where the counsellor genuinely believes that he/she has been or may be harmed, is covered by section 15 of the Children, Young Persons, and Their Families Act 1989. No civil, criminal, or disciplinary proceedings will lie against the counsellor in such a case (section 16 of Children, Young Persons, and Their Families Act 1989).

- In the case of both guidance counsellors and specialist services, care should be taken in disclosing information. The responsibility for providing guidance and counselling is the principal's, with the additional responsibility of advising the parents of matters which prevent or slow the student's progress or harm the student's relationships with others. Such information should not be disclosed to the board unless it is necessary for the board to be told in order for it to perform one of its functions e.g. section 14: where the principal suspends a student, the board (as well as the parents) must be advised of the reasons for the suspension.

(e) *Ministry of Social Development (including Work and Income New Zealand)*

The Ministry of Social Development sometimes approaches boards [or staff] for personal information about families it suspects of benefit fraud. The information sought may include who pupils are living with, whether guardians functioned as parents or as single parents or whether parents/guardians were perceived as married or de facto couples.

Under section 11 of the Social Security Act 1964 the Ministry of Social Development has the right to obtain certain information held by boards of trustees. Also, section 66 of the Children, Young Persons, and Their Families Act 1989 Part II can be used as an authority for disclosure of certain information. In these circumstances, the Department of Social Welfare is able to obtain personal information and the board is required to supply it.

Neither party breaches any of the information privacy principles as a result because of section 7(1) and 7(4) of the Privacy Act (refer to Section One - No. 5 The Impact of Other Laws on the Act).

Where a board (or staff) receives a request for information in terms of the above, a copy of the authority (which also indicates the type of information able to be requested) should be sought from the agency requesting the information. This will ensure that only the information which the legislation authorises, is actually provided by the board or staff.

(f) *Education Review Office*

Under the Education Act 1989, the Education Review Office is given certain powers of entry and Inspection (see sections 327 and 328). This includes the power to require any person to produce documents or information relating to any service provided, or people to whom such a service is (or has been provided) and permits the review officer to make copies or extracts of the documents or information.

These powers override principle 11, restrictions on disclosure.

This power also extends to requiring any applicable person of the organisation to make or provide statements in any form and manner the review officer specifies about any matters relating to an applicable service.

Section 328 requires any review officer entering a place under the authority of section 327 to, on first entering and if requested at any later time, produce the review officer's "certificate of designation."

(g) *Truancy (attendance) Officers*

Truancy officers are generally employed by boards for the specific purpose of ensuring attendance at school of certain students. Provision of addresses etc to truancy officers is not a breach of the Privacy Act.

This is because education is compulsory for every child aged 6-16: they must enrol at a school (section 20 Education Act 1989, with certain exceptions) and must attend school whenever it is open (section 25 Education Act 1989). The Education Act 1989 further requires every board to take all reasonable steps to ensure such attendance and enables it to appoint an attendance officer (section 31 Education Act 1989) to ensure attendance. Use to ensure attendance, including disclosure to any truancy officers, can therefore be said to be one of the reasons, or a related reason, for collection of addresses.

(h) *Police*

The Police have no special powers to compel boards [or staff] to provide information to assist with inquiries. The Police rely heavily on the co-operation of the community at large to help solve crime and prevent offending.

However, if the Police ask a board (or staff) to provide personal information to assist with an investigation, the school will usually be able to meet the request without breaching the Privacy Act 1993. Similarly if a board (or staff) knows about a matter which it believes the Police ought to be made aware of (e.g. suspected child abuse), again it can tell the Police about it without breaching the Privacy Act. In either case what matters is that the board (or staff) is satisfied that the information it discloses is necessary to avoid prejudice to the maintenance of the law. This is provided for by principle 11 (e)(i) of the Privacy Act 1993. The maintenance of the law includes the prevention, detection, investigation, prosecution, and punishment of offences.

In most cases the reason for the request will be obvious. For example, a police officer may approach a board (or staff) with a shop's security camera photograph showing a pupil in school uniform stealing, and ask if the board (or staff) can identify the pupil. It is clearly obvious that if the board (or staff) does not supply the pupil's name and address, it will not be possible to identify the offender and the offence will go unsolved, which is clearly prejudicial to the maintenance of the law.

Similarly if a school teacher identifies signs of abuse in one of his or her pupils, it is clearly important and in the child's interests to inform Police. Disclosure maybe necessary in such a case to prevent or lessen a serious or imminent threat to the pupil concerned (principle 11 (f)). Again if the Police are not told, officers will not be able to investigate the matter and an offender may not be brought to justice. This too is clearly prejudicial to the maintenance of the law.

However, if a board (or staff) is unsure why the Police are asking for information, it ought to ask the officer involved to explain further. It is important that the board (or staff) knows why the information is being requested and how the maintenance of the law will be prejudiced if it is not supplied. In the event that a complaint is laid with the Privacy Commissioner over the disclosure, the board (or staff) will need to be able to supply this information in order to show its actions conformed with principle 11 (e)(i).

If a board (or staff) receives a complaint concerning the disclosure of personal information to the Police, and any assistance is required to confirm compliance with principle 11 (e)(i) e.g. to corroborate the information supplied by the board (or staff) about the nature of the police inquiry, contact should be made with the police officer involved. The Police will always be happy to provide such support.

It is important to remember that the while the exceptions to principle 11 mentioned above may **permit** the disclosure of information, they do not **require** it. If a board (or staff) decides for any reason not to supply information to the Police, their request may be refused. If a request by the Police is refused, the Police may then seek a search warrant. If a search warrant is obtained, it will be compulsory to provide the items detailed in the warrant.

11. STUDENT INFORMATION

Records: Students are entitled to request access to any information held about them by the board (or staff) under principle 6. Unless a good reason exists to refuse, students must be given access to their records. If a student believes that the information about themselves is incorrect, they may also ask to have it corrected.

To ensure that access requests are able to be dealt with efficiently, the privacy officer should:

- find out what records are held by the school, who holds that information and why
- keep only relevant information
- ensure as far as possible that only information about the particular child is kept on that child's file
- ensure, as far as possible, information is accurate
- ensure information is not kept longer than necessary.

Boards should note that ex-pupils may ask for references later. It is suggested that boards check their copy of the "School Records – Retention / Disposal Schedule" to work out how long information should be kept.

Websites and School Publications: In recent times more information is being made available electronically. Boards need to ensure that where information or material (photos) is placed "online" that sufficient safeguards are in place. The MoE recommends[23] that each school adopt an online publication policy that addresses the implications of publishing students' images and schoolwork online. In particular:

1. Schools with primary students should obtain the written consent of each student's parents or legal guardians before publishing any information about the student (including photographs) or any of the student's copyright material on the Internet.
2. Schools with secondary students should obtain the written consent of the student as well as that of the student's parents or guardians (if the student is aged under 20 years) before publishing similar information or material on the Internet.
3. These consents should be sought for each student upon enrolment or, for students already enrolled, when the issue of publication first arises for that student.
4. A school needs to exercise prudent judgment and common sense before publishing a student's material on the Internet. Firstly, the school should check that they hold the student's/parent's consent before publishing the student's material online. Secondly, publication may have legal consequences. As publisher, the school needs to ensure the material does not infringe copyright, does not defame, is not objectionable from a human rights point of view, and is not obscene.

As a minimum a web privacy policy is required which sets out the parameters of how information is used and protected (See Appendix Six).

[23] Ministry Guidelines for Schools for the Online Publication of Student Images and School Work 2000

SECTION THREE - BOARDS AS EMPLOYERS

12. GENERAL

The Act has major implications for boards as employers and in the running of their school.

These implications include the following:

As employers:

- Boards must not collect irrelevant information from job applicants (principle 1).
- Boards must collect information directly from the job applicant unless the person has authorised collecting the information from another source, or another exception applies (principle 2).
- Boards must advise the applicant of the purpose for collecting the information, and the other matters required by principle 3 (principle 3).
- Boards must not collect information about applicants by unlawful, unfair or reasonably intrusive means (principle 4).
- Boards have responsibility to ensure storage and security of employee information is adequate (principle 5).
- Employees can request access to information about themselves kept by the board of trustees (principle 6).
- Employees can seek to have such information corrected if it is not correct (principle 7).
- Boards are required to take reasonable steps to make sure personal information is correct, up-to-date, relevant and not misleading before they use it (principle 8).
- Boards can keep information only for as long as it is necessary for the purposes for which it may lawfully be used (principle 9).
- Boards may not use information for a purpose other than that for which it was collected, except in certain specific circumstances (principle 10).
- Boards must not disclose information about employees unless an exception applies (principle 11).

13. COMMONLY ASKED QUESTIONS

Some of the commonly asked questions in relation to the Privacy Act 1993 and to employment are listed below:

What do boards have to do to collect information about an applicant from the applicant?

- Boards should make applicants aware of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipients of the information, the name and address of the agency collecting the information, the agency that will hold the information, the consequences (if any) for that individual if all or part of the requested information is not provided, and the rights of access to, and correction of, personal information provided by these principles (see principle 3).

  It is recommended that boards, on any application form for a vacancy, add a sentence which states that the information will be used by the board only for the purposes of determining the suitability for the position.

Can boards collect information which may be personally detrimental to an applicant, from the applicant, to avoid making inappropriate appointments?

- The general requirements on what boards have to do to collect information about an applicant from an applicant continue to apply (as indicated above).

- There is, however, a necessity for boards to avoid, as far as is reasonably practicable, the possibility of making inappropriate appointments to vacancies, which could place students at risk (e.g. persons considered unsuitable for employment in a school because of a history or record of child molestation).

It is recommended that boards use the template application form available from the NZSTA website www.nzsta.org.nz for any application or short listing for a vacancy.

In terms of a criminal conviction, the Criminal Records (Clean Slate) Act 2004 provides applicants do not have to disclose certain convictions, when:

- they have not committed any offence within 7 (consecutive) years of being sentenced for the offence; and
- they did not serve a custodial sentence at any time (this would exclude serious offences such as murder, manslaughter, rape, and causing serious bodily harm), and
- the offence was not a specified offence (specified offences are in the main sexual in nature); and
- they have paid any fine or costs.

> Custodial sentences include a sentence of preventive detention and corrective training. Non-custodial sentences include fines, reparation orders, community-based sentences, and suspended sentences. Applicants are not obliged to disclose convictions if they are an eligible individual but can do so if they wish. If they are uncertain as to whether they are eligible they may contact the Ministry of Justice."

For examples of an application form see NZSTA website

What does a board have to do to collect information from another person about an applicant?

- The board should ensure that if it is collecting information from another person about an applicant (principle 2(2)):

  - the information is publicly available information; or
  - the individual concerned authorises collection of the information from someone else; or
  - the non-compliance would not prejudice the interests of the individual concerned; or
  - compliance would prejudice the purposes of the collection; or
  - compliance is not reasonably practicable in the circumstances of the particular case.

In particular it is recommended that application forms or requests for information from an applicant contain an authority for boards to approach referees and present and past employers to ask about the suitability of the employee for the position.

- Inquiries should not be made of other people before this authorisation has been obtained. From a practical point of view, boards otherwise run the risk of prematurely disclosing the fact of an application to a current employer.

- Waiting for the authorisation will provide the applicant with the opportunity to explain circumstances that may be behind an adverse reference.

What right of access to personal information about themselves does an employee have?

- Employees have a right to request access to information on their personal file and may request correction of the information. Boards are required to give reasonable assistance to employees requesting information and a decision on whether to grant a request must be made within 20 working days. Unless specifically authorised by the Privacy Commissioner, public sector agencies are not allowed to charge for handling information privacy requests: private sector agencies may make a reasonable charge for supplying information or correcting it

What right to seek correction of personal information about themselves does an employee have?

- Employees are entitled to seek correction where any information is considered inaccurate. If a person believes that the personal information the agency holds about them is incorrect they can ask that agency to correct it. Boards have a responsibility to ensure that the personal information that they hold is accurate, up-to-date, complete and not misleading. Where an agency believes that the information that it holds is correct, it may refuse to correct it. The person may then ask that a statement of the correction requested and the board has refused to make, be attached to the information. Where this occurs the board must attach the statement to the personal information in such a way that it will always be read at the same time as the information in issue.

- Where information is corrected, or a statement of requested correction is attached to disputed information, boards must take reasonable steps to advise anyone to whom the inaccurate/disputed information has been disclosed.

Does an employee then have access to notes of disciplinary/competency procedures?

- The Privacy Act gives a right of access to personal information unless there is a good reason under the Act to withhold it. The only reasons which may be relied on to withhold information are contained in sections 27-29 of the Act.

- It should be noted that if disciplinary action is contemplated against an employee, rules of procedural fairness must be followed in order to avoid a successful personal grievance action being taken. This may require giving the employee the opportunity to comment on any adverse information. Nevertheless, there may be occasions where material that can be described as evaluative material can be withheld.

Can a board provide private information to NZSTA on employment matters?

- Boards are bound by principle 11 of the Privacy Act 1993 which provides that an agency that holds personal information shall not disclose the information to a person or body or agency.

- There will be instances relating to employment matters when a board will need to seek the advice of NZSTA. Boards can do this and ensure compliance with the Act in most cases by ensuring that the information is not used in a form in which the individual concerned is identified.

- There may, however, be specific cases where this is not reasonably practicable and the individual can be identified. If a board requires assistance to comply with the provisions of a legally enforceable employment agreement, boards will need to disclose the information to NZSTA. The disclosure could reasonably be seen as one of the purposes in connection with which the information was obtained. In this case information obtained for the purposes of employment (including contract) is disclosed to ensure that the best employment arrangements or contract are made.

Is NZSTA's advice to boards on disciplinary matters able to be withheld from a board's employee[s] who approach NZSTA or the board for the information?

- When a board employee requests access to NZSTA's advice to the board regarding an employment matter relevant to him or her, section 29(1)(b) of the Privacy Act would generally be considered grounds for refusal of the request. This provides that a request may be refused

where disclosure of the information identifying the person who supplied it, being evaluative material (see discussion below), would breach an express or implied promise which was made to the person who supplied the information and which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence.

- In employment matters the information between NZSTA and its client [the board] may be treated as confidential between the two parties in certain circumstances. Where a legal adviser is involved then privilege applies.

When may a board refuse an employee access to information?

- A board may refuse the employee access to the information in certain circumstances (section 27 and 29). These instances include where the disclosure of the information would be likely to:

  - endanger the safety of any individual (section 27 (1)(d));
  - involve the unwarranted disclosure of the affairs of another individual or deceased individual (section 29 (1)(a)); or
  - disclose evaluative material (section 29 (1)(b) – see above).

  An example of evaluative material would be a reference. References that have been supplied pursuant to a promise of confidentiality may therefore be withheld. It is a good idea to ask the person, at the time the reference is supplied, whether that person requires the information to be held in confidence.

  Whether or not material is evaluative must be decided on a case-by-case basis, not because of the type or category of information in question, and it is again recommended that boards review their policies and practice to ensure compliance with the Act.

- Under the Act personal information may be withheld where the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise:

  (i) Which was made to the person who supplied the information; and
  (ii) Which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence.

The term "evaluative material" is defined as evaluative or opinion material compiled solely:

(a) For the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates:

  (i) For employment or for appointment to office; or
  (ii) For promotion in employment or office or for continuance in employment or office; or
  (iii) For removal from employment or office (refer to section 29(3) for the full text).

- Where an employer refuses access to information, the employee is entitled to know the reasons why their request has been refused, and to be informed that they have a right by way of a complaint to seek an investigation/review of the refusal by the Privacy Commissioner.

What requirements are there on boards with regard to storage of personal information?

• Principle 5 of the Privacy Act 1993 requires that personal information is secure against loss, modification, or misuse to the extent that is reasonable in the circumstances.

1. What information can be kept on personal files?

The type of information that can be kept on personal files includes name, address, and tax file number, and information that is relevant to the employment of the individual (e.g. where it contains a disclaimer regarding convictions).

Warnings given to an employee should be recorded and placed on the file (some employment agreements require this to be sighted and signed) and it may also be appropriate to note any special commendation received, together with comments on work attitude and/or ability (this may be in the form of a performance appraisal).

Information on files should always be accurate, up to date, complete, relevant, and not misleading. Files should therefore be checked on a regular basis to ensure that this occurs.

It should be noted that warnings generally have a limited lifespan and while a record should be kept that one was given, the use of a warning to justify a particular disciplinary action where the warning is some months old can be difficult. Boards should check with the NZSTA if in such a situation.

2. Should information be kept on ex-employees?

No information is to be kept longer than necessary for the purposes for which it may lawfully be used. This time limit varies for the different types of information. For example, information used as a basis for a demotion or dismissal should 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 submitted. Wage and time records must, as now, be retained for 7 years.
A complaint under the Human Rights Act may be made within 1 year of an alleged discriminatory action being taken. This period can be extended with leave of the Human Rights Commission. However boards should always refer to the “School Records – Retention / Disposal Schedule” as it may require boards to keep records for a longer period than required by other legislation. For example in the cases discussed above records should be kept for seven years.

3. May a former employer provide a prospective employer with a reference without the employee's consent?

- The ex-employee's permission will be needed before a reference can be provided (principle 11) because the general rule is that (with certain exceptions) informationmust be collected directly from the individual concerned.
- It would be good employer practice to obtain permission from employees to allow references to be given in future without seeking their specific consent.

4. May employers continue to maintain personal files in alphabetical order?

Employers may still list files alphabetically with the employee's name attached. However, a unique identifier may only 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.

SECTION FOUR - PROCESSES AND REQUIRED PROCEDURES

14. GENERAL

Boards and management have a responsibility to ensure that the school's policy and procedures comply with the Privacy Act.

To do this they will need to:

- appoint a privacy officer;
- review current policy and practice to ensure compliance with the Act (this may be the task of the privacy officer); and
- develop specific policy and procedures to ensure compliance with the Act.

SECTION FIVE - PRIVACY OFFICER

15. GENERAL

Each school must appoint a privacy officer.. Privacy officers are responsible for:

- encouraging compliance with the information privacy principles by the board and staff
- dealing with requests made to the board and staff for personal information
- working with the Commissioner when complaints are investigated
- otherwise making sure that the school complies with the Act.

The principles relate to personal information, i.e. information about an identifiable individual.

Privacy officers have an important role in making sure that compliance with the Act occurs. Initially the role will require some work in checking that the procedures the school follows are in line with the Act. Once good procedures are in place, however, the role is likely to consist of monitoring the existing procedures, answering specific inquiries, and troubleshooting.

There is training and advice available for privacy officers from the Privacy Commissioner's Office on www.privacy.org.nz. They provide information fact sheets and privacy officers can subscribe to a mailing list. In the appendices of these guidelines privacy officers can find some useful forms and templates.

16. CHECKLIST FOR PRIVACY OFFICERS

This is a suggested checklist for privacy officers. Some of the steps may not be relevant to your school and you may need to add others.

1. Find out and catalogue the personal information held by the school about individuals. It is likely to fall within three broad categories of personal information:

    - about staff
    - about pupils, and
    - about the families of pupils

It may be useful to break the information into subcategories, for example: academic information, other information about pupils (sporting, discipline, arts, etc.), performance appraisals on staff, disciplinary action in respect of staff, leave information, etc.

Identify who holds this information in the school - some will be held at the office, other information may be held by the class teacher, school guidance counsellor, ESOL teacher, special needs department, principal, etc. You may find that pockets of personal information are held that the board/principal did not know existed.

2. Establish the purpose for which each category of information is collected. There may be more than one. It may be useful to check against the following:

    - what does the school use the information for?
    - does the school need to be able to pass this information on to another agency? Is it necessary to collect the information for that purpose?
    - are the right questions being asked to collect the information we need?

3. How does the school collect this personal information?

- What information is collected directly from the individual concerned?
- What information do we receive from other agencies?
- Which exception to principle 2 is likely to apply to the information collected from people or agencies other than the individual concerned?
- Do we need to get authorisation at the point of collection from the individual to use/disclose their information in the way we wish to?

4. What do people know about the personal information we collect directly from them?

Have we taken steps that are reasonable in the circumstances to inform them:

- that we are collecting the personal information [with our address, i.e. the name and address of the agency collecting it and the agency that will hold it]?
- why we are collecting it?
- who will receive it?

If not, which exception to principle 3 do we rely on to collect it?

If not, have we collected similar information from the same individual recently?

5. If so, check that the method of collection is:

- not unlawful nor unfair
- not in a manner that is unreasonably intrusive

6. Is the personal information we hold stored in a reasonably secure way?

- Do we have clear rules about who in the school may see different categories of personal information?
- Is personal information stored so that only authorised people have access to it?
- Do authorised people know of their obligations under the Privacy Act?
- Is information safe from vandalism and theft?
- Are VDU screens, printers, or files positioned so that they are not able to be seen by the public or unauthorised staff?
- Are there procedures in place to monitor access to sensitive data?
- Are external agencies used to collect, process, hold, or dispose of personal information? If so, what steps are taken to ensure they are complying with the privacy principles?

7. Is the personal information we hold accurate, up to date, complete, relevant, and not misleading?

- What steps have been taken to ensure that it is?
- When personal information is received from a third party what steps are taken to make sure it is accurate, up to date, complete, relevant, and not misleading?
- At what point(s) is it checked to ensure accuracy; when first recorded, during storage, before use, periodically?

8. Do we still need to keep this information?

- Can all or some of it be purged from the system?
- What process do we have for destroying personal information which is no longer required? Does it ensure that the information remains confidential?

9. Is information used for a purpose other than the one for which it was collected? (What did we tell the individual we would be using the information for when it was collected?)

- If it is, what exceptions to principle 10 apply? For example, do we have the individual's authorisation to use it for a different purpose?

10. List the situations in which the personal information we hold about individuals may be disclosed to other agencies.

    - Did we tell individuals that the information would be disclosed when it was collected?
    - Did we tell the individuals concerned at the time of collection that the information would be disclosed in this way?
    - Is such disclosure directly related to the purposes in connection with which the information was obtained?
    - Has the individual authorised the disclosure? Does any other exception to principle 11 apply?

11. Do we assign unique identifiers to individuals (other than their names)?

    - Is it necessary to do so to carry out one of the agency's functions?
    - Is it the same as another agency has assigned to the individual?
    - Do we take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identity is clearly established?
    - Do we require individuals to disclose any assigned unique identifiers?
    - If yes, is that one of the purposes for which the identifier was assigned or a directly related purpose?

SECTION SIX - FURTHER INFORMATION

17. GENERAL

Legislation

Boards of trustees can access a copy of the Privacy Act 1993 online at www.legislation.govt.nz.

Privacy Commissioner

Advice and information fact sheets regarding the Act may also be obtained from the Privacy Commissioner, www.privacy.org.nz -

PO Box 466, Auckland 1140 ph: (09) 302 8680, fax: (09) 302 2305	PO Box 10-094, Wellington 6143 ph: (04) 474 7590 fax: (04) 474 7595	Enquiries Line From Auckland: 302 8655 From outside Auckland: 0800 803 909

The Privacy commission has also produced ***Privacy at work - A guide to the Privacy Act for employers and employees***. This book uses examples and discussion to illustrate some of the major privacy questions at work, and how to resolve them.

It can be downloaded in a pdf version of the book, or you may order copies of this book from the Commission.

Ministry of Education

The Ministry have produced resources to assist schools in developing a policy for the online publication of student images and schoolwork. This document provides schools with guidelines for the online publishing of student images and schoolwork.

http://www.tki.org.nz/r/governance/curriculum/copyguide_e.php#ack

NZSTA Advisory Service

Boards of trustees may also contact the NZSTA Helpdesk, ph 0800 STAHELP (0800 782435), helpdesk@nzsta.org.nz for further information, or for employment related issues the NZSTA Industrial Advisors.

APPENDIX I: FUNCTIONS AND PRINCIPLES OF THE PRIVACY ACT 1993

Functions of the Privacy Act:

- Promotes and protects individual privacy
- Is concerned with the privacy of information about people rather than physical intrusions into privacy
- Establishes 12 information privacy principles regulating the collection, storage, use and disclosure of personal information and giving people the right to access, and request correction of, their information
- Allows the Privacy Commissioner to issue industry specific codes of practice – Health, Telecommunication, Credit Information
- Sets out rules for information matching between Government agencies
- Provides a set of principles regulating how information on public registers can be used
- Sets up a complaints procedure
- Provides for the appointment of a Privacy Commissioner and sets out her role and functions.

Part 2—Information Privacy Principles

6. Information Privacy Principles

The information privacy principles are as follows:

Principle 1

Purpose of Collection of Personal Information

Personal information shall not be collected by any agency unless:

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

Principle 2

Source of Personal Information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds:

(a) that the information is publicly available information; or

(b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or

(d) that non-compliance is necessary:

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) that compliance would prejudice the purposes of the collection; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

(g) that the information:

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) that the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3

Collection of Information from Subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of:

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) if the collection of the information is authorised or required by or under law:

(i) the particular law by or under which the collection of the information is so authorised or required; and

(ii) whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds:

(a) that non-compliance is authorised by the individual concerned; or

(b) that non-compliance would not prejudice the interests of the individual concerned; or

(c) that non-compliance is necessary:

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that compliance would prejudice the purposes of the collection; or

(e) that compliance is not reasonably practicable in the circumstances of the particular case; or

(f) that the information:

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4

Manner of Collection of Personal Information

Personal information shall not be collected by an agency:

(a) by unlawful means; or

(b) by means that, in the circumstances of the case:

(i) are unfair; or

(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5

Storage and Security of Personal Information

An agency that holds personal information shall ensure:

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6

Access to Personal Information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled:

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 7

Correction of Personal Information

(1) Where an agency holds personal information, the individual concerned shall be entitled:

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8

Accuracy, etc, of Personal Information to be Checked Before Use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9

Agency not to Keep Personal Information for Longer than Necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on Use of Personal Information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds:

(a) that the source of the information is a publicly available publication; or

(b) that the use of the information for that other purpose is authorised by the individual concerned; or

(c) that non-compliance is necessary:

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to:

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information:

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) that the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11

Limits on Disclosure of Personal Information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds:

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary:

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to:

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information:

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12

Unique Identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

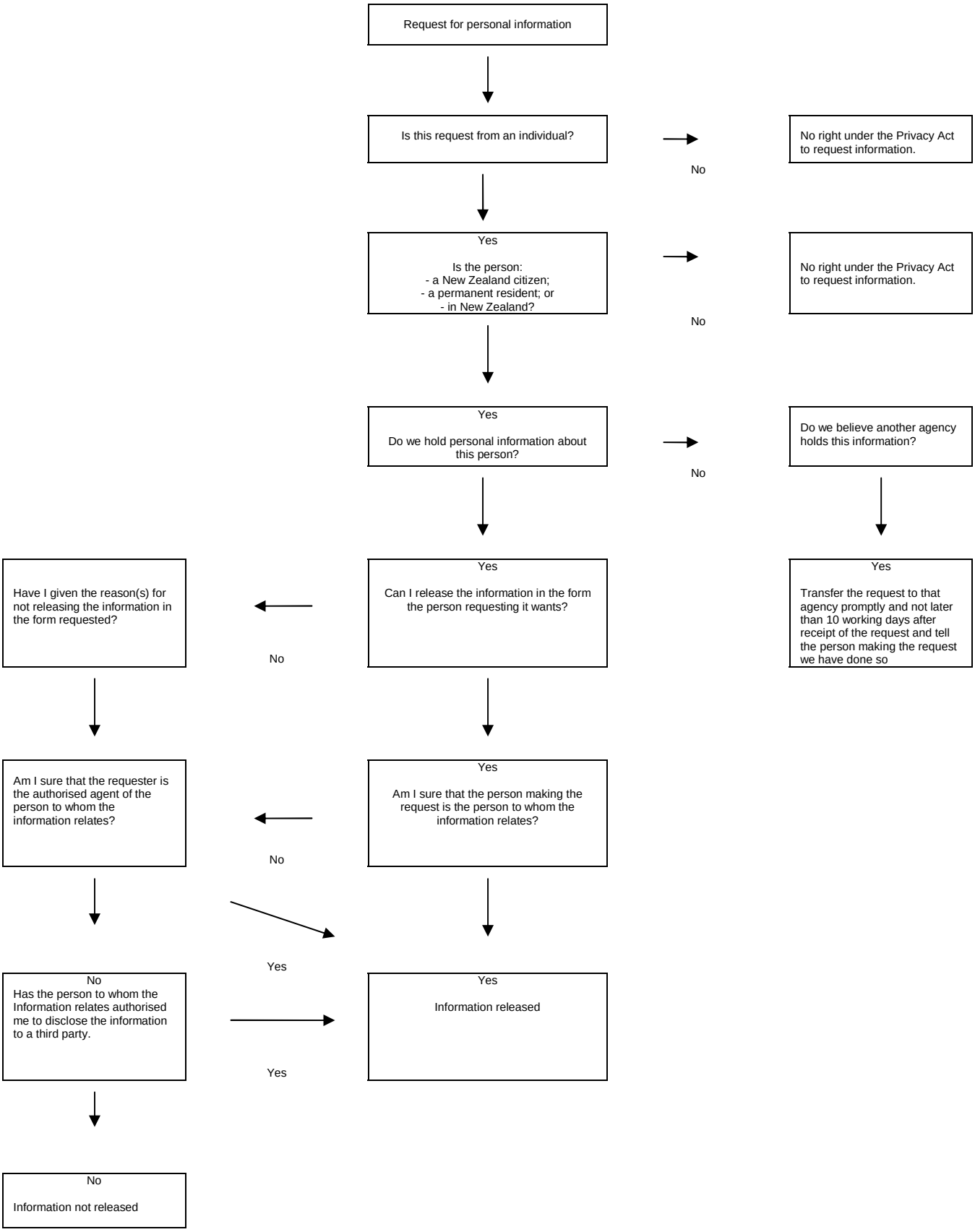
(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007 (to the extent to which those rules apply for the whole of that Act excluding the 1973, 1988 and 1990 version provisions).

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

APPENDIX II: REQUESTS FOR PERSONAL INFORMATION FLOWCHART

Requests for Personal Information



APPENDIX III: TEMPLATE ACCESS TO PERSONAL INFORMATION REQUEST

Access to Personal Information Request

Requested by: _____	*Date* _____
Employer response options	*A response must be made within 20 days.*
1 Access granted Applicant advised (date):	*In the case of a request being transferred to another agency, that response must be within 10 working days.*
2 Request transferred To: By: Date: Applicant advised (date):	*The request shall be transferred if the information is not held by the agency, but is believed by the person declining the request to be held by another agency or more closely connected with the functions or activities of another agency.*
3 Access is refused	*Check reasons for refusal sections 28, 29, 32, 43, 44 of the Act consider 'evaluative material', and whether information is readily retrievable.* *Advise applicant of right to make a complaint to the Commissioner.*
4 Extension of time is required Extension to (date): Note to applicant sent (date):	*An extension of time to retrieve the information may apply where the request is for a large quantity of information, search for the information within the original timeframe would unreasonably interfere with the operations of the agency, or where time is needed to make a decision on the request which cannot reasonably be made in the original time-frame,* *(see section 41 of the Act for details).* *The extension of time must be reasonable.* *Notice must be given to the applicant of the time of the extension - reasons - right to complain to the Commissioner.*
5 Advise the applicant how access will be achieved	*Where - when - by whom the information will be made available.*

NB Only the person whom the information is about can ask for access and correction of that information (either directly or through a representative). The Act calls this person "the individual concerned." The Privacy Act does not provide rights to access or correct information about other people.

APPENDIX IV: TEMPLATE EEO INFORMATION COLLECTION FORM

Collecting EEO Statistical Information

So that we can more effectively monitor our EEO programme we would like you to provide the following information.

There is no compulsion on you to comply with any or all of this request – if you do then all the information will be treated in confidence and does not form part of any selection criteria

Position applied for:

Date of application:

1. Gender	□ Male □ Female
2 Date of birth	
3. Ethnic group	Tick one or two boxes from the list below: □ New Zealand European/Pakeha □ New Zealand Māori □ Samoan □ Cook Island Māori □ Tongan □ Chinese □ Indian □ Niuean □ Tokelauan □ Fijian □ Other European (such as British, Australian, Scottish, Dutch). Please specify….. □ Other ethnic group (such as Vietnamese, Kenyan). Please specify…….
4. Do you live with the effects of injury, long-term illness, or disability?	□ Yes □ No
5. If yes, what does your disability/injury/illness affect?	□ movement □ vision □ respiration/breathing □ hearing (tick all that apply) □ speech □ emotional and mental health □ concentration □ other (please specify)
6. Do you need any technical aids or equipment, or adaptations to your work place, to make your work easier or to increase your work performance?	□ Yes □ No
7. If yes, please specify	