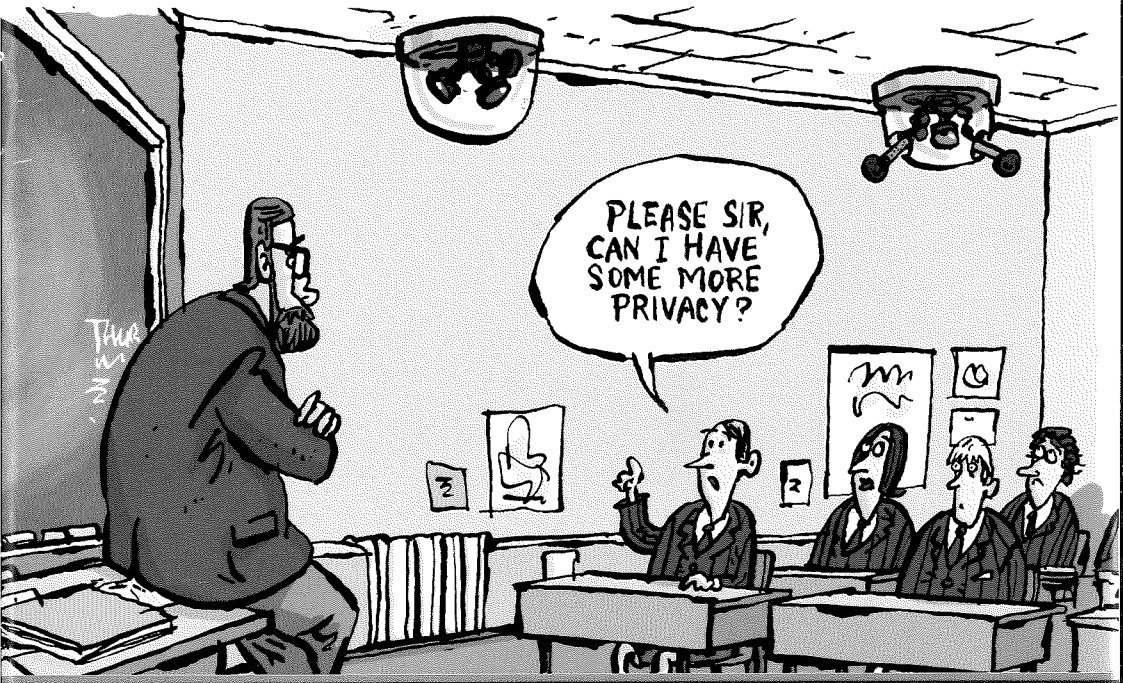
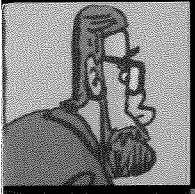
Privacy Commissioner
Te Mana Matapono Matatapu



PRIVACY in schools

A guide to the Privacy Act for principals, teachers and boards of trustees

By Kathryn Dalziel



Privacy Commissioner
Te Mana Matapono Matatapu

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

ISBN 0 478 11728 0

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

Printed by Lithoprint Ltd
Wellington

Price: $20

About the author

Kathryn Dalziel is one of New Zealand's leading privacy lawyers and works as an associate with Christchurch law firm Taylor Shaw specialising in privacy law, employment law and civil litigation. Her publications include the first edition of this work and she has co-authored the chapter on health information in S P Johnson's "Health Care and the Law".

Kathryn presents seminars and provides privacy advice to a wide variety of agencies including schools and universities.

Foreword

Schools rely on information about people. The moment a school collects information about a student, or a student's family, there may be issues about the way the information is collected, how it is stored, how it is used and how it is disclosed. Good information handling is a foundation stone of the trust that needs to exist between everyone who participates in the life of the school. Of course most schools are attuned to the needs of their students, their family or caregivers, and their staff, so handling information well usually comes naturally to them. But, as with all personal relationships, situations can arise where finding the 'right' answer is not so straightforward.

In 1995 Kathryn Dalziel wrote a book called "The Privacy Act for Schools" to help boards of trustees, principals and teachers to understand the privacy principles and to apply them to typical situations in schools. The book was popular and proved very useful. It was obvious, though, from our many calls from schools and their advisers that there was still a strong need for practical advice about handling personal information in schools.

However, simply reprinting the book was no longer going to address some of the concerns that schools face. In 2009, mobile technologies and the use of the internet (both by students and in the classroom) have created new challenges for privacy protection. In addition there are new systems for managing student enrolment, health records, and immunisation programmes. Schools are telling us that they need some help with these issues and they need it now.

So we approached Kathryn to see if she was willing to revise and update her earlier book – "Privacy in Schools" is the result. We have been delighted to work with her on the project and hope that you find the book useful.

Marie Shroff
Privacy Commissioner

Contents

Introduction

Welcome to "Privacy in Schools" – a book designed to help New Zealand primary and secondary schools and their associated units find solutions to issues involving privacy.

The starting point for New Zealand privacy law is the Privacy Act 1993, and at the heart of this Act are 12 information privacy principles. While the privacy principles are law that schools must follow, they are not so much hard and fast "rules" as basic guidance, with agreed exceptions, on how schools should handle personal information. These privacy principles are based on internationally accepted ways of how best to protect privacy. For instance, you'll find the same ideas in Australian, Canadian, British, Hong Kong and South Korean law, to mention only a few.

To apply the privacy principles in your school, first of all you need to understand them. In this book you will find a discussion of each of the privacy principles, with examples to help with the explanation. The principles are all reproduced in Appendix A, page 38.

Secondly, you need to work out if there is other relevant law. This is because you must follow other legislation first if it requires you to handle personal information in a particular way. For example in the situation where a student is expelled, all schools (including state, private and integrated) need to comply with the Education Act by notifying the Ministry of Education. In this book you will find more examples where other legislation takes precedence over the privacy principles.

From there, you need to be able to apply the principles and any other relevant law to a particular situation. So, under the heading "Application of the privacy principles", page 26, you will find discussion of how the principles and other law applies to common issues such as enrolment forms, reporting to parents, and behaviour modification or disciplinary processes. While the Privacy Act is not about creating a paper war of authorisations and consents, I have also provided some draft forms in Appendix B, page 47, to help schools develop their own forms.

Finally, acknowledging that there are times when mistakes or errors are made, there is some information on complaints and reference to further resources.

Of course, I cannot anticipate or answer every privacy question for schools and this book is not a complete guide to education law. Some situations may well require more detailed analysis of education law and indeed the Privacy Act itself and in that situation schools should seek legal advice.

I have also limited the discussion on privacy to students and their families but of course schools also need to deal with privacy issues involving staff. For further assistance in respect of employment matters within a school, please refer to *Privacy at Work – a guide to the Privacy Act for employers and employees*, Office of the Privacy Commissioner, 2008, Wellington.

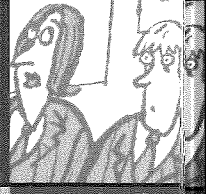
In summary, this book provides a working knowledge of the privacy principles so that some of the guesswork is taken out of the issues. Once you are familiar with the principles you will see that reasonableness can and will prevail and it is only a matter of incorporating respect for individual privacy into the culture of the school, just as schools have incorporated anti-discrimination rights under the Human Rights Act.

Education and Privacy: two fundamental aspects of human development and human dignity. It is a privilege to bring them together.

Acknowledgement

The author acknowledges the wonderful assistance and support together with peer review and contribution from Katrine Evans, Assistant Privacy Commissioner in the writing, development and publication of this book.

Important definitions



Agency

"Agencies" are people or organisations that have to comply with the privacy principles. Nearly everyone who handles personal information is an agency. There are some exceptions. For instance, Members of Parliament acting in an official capacity are not agencies and nor are Courts and Tribunals, or news outlets in relation to their news activities.

All types of schools are agencies and therefore must comply with the privacy principles.

Collect

A school is not "collecting" personal information when it receives unsolicited information. However, once a school *holds* unsolicited information, it must apply good information handling policies to that information – including proper storage and checking accuracy before use.

Confidentiality

It is important to separate the concepts of privacy and confidentiality. Confidentiality is an obligation often associated with professions such as teachers, lawyers and doctors. Confidentiality is the duty to protect and hold in strict confidence all information concerning the person who is the subject of the professional relationship. There are times when confidential information may be disclosed, but those occasions are limited.

At the date of publication, the New Zealand Teachers Council Code of Ethics records the following relevant matters in terms of confidentiality and privacy:

- Teachers' commitment to learners includes protecting the confidentiality of information about learners obtained in the course of professional service, consistent with legal requirements.
- Teachers' commitments to parents/guardians and family/whānau of learners includes encouraging active involvement in their children's education, acknowledgment of their rights including consultation on

the care and education of their children, respect for their privacy (*author's note: not confidentiality*), and respect for their rights to information about their children, unless that is judged to be not in the best interests of the children.

Document

Document is defined widely to include:

- writing on any material;
- information on a tape-recorder, computer etc;
- a label;
- a book, map, plan, graph, or drawing; or
- a photograph, film, negative or tape.

Individual

An individual is a natural person who is alive. The Privacy Act does not govern information about companies, other corporate bodies or deceased people.

Although they have no privacy rights under the Act, companies and other corporate bodies are agencies and must comply with the Act.

Personal information

Personal information means information about an *identifiable* individual. So obviously anything with an individual's name attached will be information about that individual. But sometimes information will clearly be about a particular individual even though that individual is not named.

Details about an individual's circumstances, what that particular individual said or did, what others said or thought about them, or what their rights or responsibilities are, would be personal information about that person.

Information

'*Information*' is not defined in the Privacy Act or in the Official Information Act.

This prompted Justice McMullin to say:

"From this it may be inferred that the draftsman was prepared to adopt the ordinary meaning of that word. Information in its ordinary dictionary meaning is that which informs, instructs, tells or makes aware."

Commissioner of Police v Ombudsman [1988] 1 NZLR 385,402

Privacy officer

All agencies must have a privacy officer. A privacy officer is the person responsible for handling privacy issues in the school. The best person to be a privacy officer is someone reasonably senior within the school who can influence the school's policies and practices for handling personal information and who can advise other staff about what they need to do.

The privacy officer will need to:

- be familiar with the privacy principles and relevant sections of other legislation which affects the way the school manages personal information (for example the Education Act);
- lead development of a privacy policy for the school and update that policy where appropriate;
- deal with complaints about breaches of privacy;
- train other staff in privacy;
- deal with requests for access to personal information or correction of personal information; and
- work with the Privacy Commissioner, particularly if there is a complaint.

(See chapter on "Application of the privacy principles", page 26, for more information on the role of the privacy officer.)

Other legislation

The privacy principles are subject to all other legislation. In other words, the Privacy Act can be trumped by other statutes. So, if another statute requires you to handle personal information in a certain way, then you must comply with that statute even if it would normally breach the privacy principles. This book highlights some relevant examples including the Official Information Act and the Education Act.

Privacy principles

The backbone of the Privacy Act is the 12 privacy principles. It is to these principles that you should turn when dealing with:

- collection of personal information;
- storage of personal information;
- use of personal information;
- disclosure of personal information; and
- access to and correction of personal information.

This chapter summarises and explains the 12 privacy principles. The full text of the principles is set out in Appendix A, page 38.

You will see that although there are 12 principles, there are a number of exceptions to the principles which make them guidelines to the implementation of the Privacy Act rather than rigid statements of law.

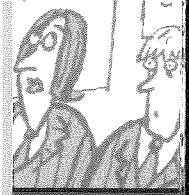
One important exception to the principles is that the Privacy Act is subject to all other legislation. Therefore your obligations under the Education Act must be met before you consider the Privacy Act. For example, all schools are required to comply with the requirements for enrolment records under the Education Act and all schools are required to report any expulsion to the Ministry of Education. It is anticipated that in 2010, primary and intermediate schools will be required to report to parents on how their child is doing against new National Standards in reading, writing and maths.

If you have any questions about the principles or if you wish to make a complaint then you should contact the Office of the Privacy Commissioner. For contact details, see page 37 and the Commissioner's website, www.privacy.org.nz.

Principle 1 – only collect information that you need to have

When collecting personal information about students, their parents, caregivers, or families, you must be sure you are collecting it for lawful purposes of the school and the information is necessary for those purposes.

So what are lawful purposes of a school?



It is perhaps easiest to define lawful purposes as those that are not unlawful. So, for example, if a purpose is to breach the anti discrimination obligations of the Human Rights Act or the purpose is for criminal activity, then obviously neither of these will be a lawful purpose.

The more challenging aspect to principle 1 is identifying when it is necessary to collect the information.

A good starting point is the teaching profession's ethical code.

At the date of this publication, the New Zealand Teachers Council Code of Ethics describes the goal or purpose of teaching which is to attain the highest standards of professional service in the promotion of learning.

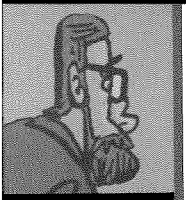
The Code also recognises that this complex professional task is undertaken in collaboration with colleagues, learners, parents/guardians and family/whānau, as well as with members of the wider community.

Another document to consider is the school's charter or strategic plan that identifies the school's mission (vision or purpose), aims, objectives, directions, and targets together with its values or principles (kaupapa and tikanga). From there, the school needs to identify what it needs to know about students and their families to meet those purposes.

A good approach for schools is to consider whether or not the information is needed to complete a process such as enrolment or an application to attend a school camp. If so, then the school probably needs to collect the information. A further check is to see if other schools are collecting the same information in the same circumstances.

An obvious example is a student's home address. That information will be necessary to complete the enrolment process and it is information collected by other schools.

To give another example, some schools set the celebration of achievement as part of their vision. That value may mean that one of the purposes for collecting information is the identification of a student (maybe with a photograph) and the publication of that student's results or other success as part of the celebration of achievement. In that scenario, can a school ask for a photograph or consent to use a photograph?



To answer that question, a school should ask itself if it is able to complete enrolment if a parent/guardian or child refuses to provide a photograph or consent to a photograph being used. If a school can complete enrolment then the information sought is probably not necessary but optional. If a school cannot complete enrolment without this information, then the information sought must be provided. To check this position, the school should see if the Ministry of Education has set any guidelines or requirements and the school should see what other schools are doing.

Anticipating when a school must *disclose* information is a useful part of identifying purposes. Many questions about privacy can be resolved if schools can anticipate when they need to disclose information and then simply identify that disclosure as part of their purposes for collection. For example, if the school needs to report information to the Ministry of Education, or needs to forward school records to other schools when a student transfers then these will be part of the school's legitimate purposes for collecting information.

With enrolment and the mission of the school in mind, set out below are some ideas, in terms of purposes, that you might like to consider for your school. Do not forget that just because it is a lawful purpose, this does not automatically mean that collection is necessary for that purpose and a school may need to obtain consent before information can be used for a particular purpose. For instance, it is arguable that collection of information for an alumni association is not a necessary activity for a school but a useful adjunct to providing education. On that basis you would expect to see on a form, "*Do you consent to your information being passed onto the Alumni Association?*"

Examples of purposes:

- meeting curriculum requirements;
- recording and maintaining student records of academic progress;
- reporting to parents/guardians;
- maintaining the school-home partnership;
- celebrating/recording achievement/success;
- recording and maintaining accounts;
- providing services such as health, information technology (IT), library and sports/recreation;

- enabling discipline/behaviour management programmes;
- reporting/disclosing information to government bodies or other agencies for the purposes of funding or to meet contractual/ legislative obligations (eg Ministry of Education, Work and Income, and Child, Youth, and Family);
- providing accurate information to other education providers to ensure proper and safe student transfer;
- maintaining alumni records (see comment above);
- marketing/public relations (although you should always get consent from an individual if the school wishes to use his/her name/photo for publicity);
- maintaining school websites; or
- administration and planning of human resources (this is relevant to collecting information as part of recruitment).

Principle 2 – get the information from the individual concerned

When collecting personal information, schools should collect that information directly from the individual concerned unless one of the exceptions applies. Involving the individual from the outset and telling them why you need his or her information and how you are going to look after it (see principle 3) is all about building good and honest communication. This also leads to trust and confidence which is essential to all relationships in the education environment. This principle is also about accuracy. Usually the best person to tell you about him or herself is the individual concerned.

However, the reality is that schools collect significant amounts of information about students from parents or guardians. Schools also collect information from students about their families in a variety of circumstances, including classroom exercises. Sometimes the individual concerned is not the best person to give information about him or herself – for example, the student cannot write or give information accurately or you want to investigate a theft which may involve asking one student to reveal what he or she saw another student doing.

The exceptions cover these situations, although schools should not lose sight of the starting idea of building relationships of trust, confidence and good communication.

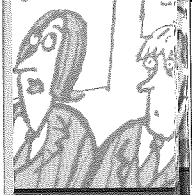
A school does not have to collect information directly from the individual when:

- non-compliance would not prejudice the interests of the individual concerned for example, collecting enrolment information from parents/guardians;
- compliance is not reasonably practicable in the circumstances of the particular case, for example, collecting enrolment information from parents/guardians;
- compliance would prejudice the purposes of the collection, for example, the investigation of breaches of school rules/policies;
- the school collects information from a publicly available publication, for example, the telephone book or the internet;
- the individual authorises collection of the information from someone else, for example, a student authorises a teacher to seek a peer performance evaluation from another student; and
- the information will not be collated in a way that identifies the individual concerned, for example, statistical information.

Principle 3 – tell the individual what you are doing

When collecting information from an individual, it is important that the individual should be aware:

- that the information is being collected. For instance, schools should not, as a general rule (there are exceptions), video or audio tape a person without that person's knowledge;
- why it is being collected and what is going to be done with it, including whether the school is going to disclose it (and, if so, to whom and why);
- who will see the information. Only the people who need the information to do their job should see it (see principle 5);
- who is collecting the information and where it will be stored;
- if the collection is a legal requirement and whether the supply of the information is voluntary or compulsory;
- the consequences if the information is not supplied; and
- the individual's rights of access to and correction of the information.



Although there are situations when a school does not have to comply with this principle (see Appendix A, page 38), in the school context it is advisable that all forms used to collect information contain the information required by principle 3. In Appendix B, page 47, there are some draft forms for consideration.

Principle 3 is all about transparency. Individuals cannot control their information if they do not know it has been collected, why it has been collected and who has access to it. They need to know that they have a right to access their personal information and request correction, if the information is incorrect.

Complying with this principle also creates trust. If a school is open and transparent about its information handling practices then people are more likely to share relevant and accurate information.

The chapter "Application of the privacy principles", page 26, has some further information about forms.

Principle 4 – use lawful, fair and reasonable methods to collect information

Schools must not collect information by any unlawful or unfair means.

For example, schools should not, as a general rule, audio or video tape someone without their knowledge (see also principle 3). Even overt filming or taping can cause problems especially in areas where there is a strong expectation of privacy like a toilet or changing area. The chapter "Application of the privacy principles", page 26, has some further information about security cameras/CCTV.

Another example involves the school office counter. School office/ reception staff need to be careful about asking questions in a public area that require answers about highly personal and sensitive matters.

The collection of information must not unreasonably intrude upon the personal affairs of the student or the student's family. Care is needed when approaching matters of particular sensitivity (eg health, sexuality, or matters of religious significance). Check that you do need to collect the information, and, if so, think about the individual's needs in the process of collecting it. This approach is consistent with a school's obligation under the Human Rights Act to not ask questions that suggest the school may discriminate on any of the prohibited grounds.

Principle 5 – store and transmit information securely

Schools have an obligation to take care of the personal information they hold. There need to be reasonable measures in place to avoid loss of information or unauthorised access or use. Nobody wants their information to end up in the wrong hands or to be tampered with. This can happen when, for example, an enthusiastic computer studies student hacks into confidential school records or student files are left unattended on a teacher's desk in a classroom. Schools need to have secure systems for electronic records as well as paper records.

Obviously mistakes do happen, but the key is to take reasonable steps to prevent those mistakes. Schools are busy places with high use areas which are not just limited to the classroom. It is therefore important to have good information handling policies that work in the school environment, based on good practice and which reflect the nature of providing education.

The starting point is to identify where information is held, who has access to those areas, who has access to the computers including the level of access (some systems provide tiered access with access restricted at different levels), and how information needs to be shared across the school. You may need to consider these ideas for separate areas of the school, for example the office, the staffroom, the offices of school administrators including principals, deputy principals and assistant principals, counsellors' offices and classrooms.

Some other matters to think about include:

- Physical security: use of lockable filing cabinets, locking offices/ classrooms when not in use, hosting electronic information off-site (eg digital storage), work taken home by staff.
- Operational security: restricting access to personal information to appropriate staff, putting confidential/sensitive information in separate files, using track and trace systems to identify who has been accessing the information.
- Security of transmission: careful use of pigeonholes and noticeboards, use of encryption for emails (think of email as sending a postcard – it is not secure), the use of pre-programmed email addresses and fax numbers; not identifying students when seeking peer support.

- Disposal or destruction of personal information: see the discussion under principle 9 which is about how long personal information should be held and the impact of the Public Records Act on state schools. If information may be destroyed then schools should consider the best approach for disposal. Schools need to be particularly careful with computer records as simply deleting them does not necessarily mean the record is removed from the hard drive of the computer.

Principle 6 – give people access to their information

Any person has the right to ask a school if it holds information about him or her and, in most cases, to have access to that information. This is an important aspect of privacy – people should be able to check what information is being held about them so they have some measure of control over their personal information.

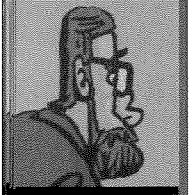
The request can be in writing or an oral request. The school must:

- provide assistance to the requester;
- transfer the request to another agency if the school does not hold the information but knows someone else does;
- respond within time limits (as soon as practicable but no later than 20 working days);
- inform the individual of the decision; and
- in most instances should make information available in the form requested.

State schools cannot charge a person for this request. Other schools may charge a reasonable fee for providing the information.

There is some personal information which may be withheld under the Privacy Act (see sections 27–29 of the Privacy Act. In Appendix A, page 38, there are some excerpts from sections 27 and 29). The most relevant withholding grounds for schools are set out below. If you are considering refusing information, it is recommended that you consult with your legal advisers.

- Disclosure will mean the unwarranted disclosure of the affairs of another person (eg a school may wish to withhold from a student who is being investigated for a breach of school rules, the name of an informant).



- The information is an evaluation or an opinion compiled solely for the purposes of awarding scholarships or awards, honours or other benefits and the evaluation or opinion was given in confidence.
- Disclosure will mean a breach of legal professional privilege. For example, the Board of Trustees may withhold its lawyer's legal opinion with respect to a student's expulsion.
- The request is obviously not made for any legitimate reason, or the information requested is trivial. While this withholding ground is designed to address vexatious requests, which are designed purely to create trouble, schools should not use this withholding ground just because the school finds the request annoying.
- Disclosure is contrary to the interests of an individual under the age of 16. This does not mean that a student under the age of 16 cannot access his or her information. It means a school may withhold a student's personal information, when that student is under the age 16, if it is contrary to his or her interests.

When a parent asks a school for information about him or herself, it is a request under principle 6. When a parent asks a school for information about his or her child, it is a different matter. The chapter "Application of the privacy principles", page 26, has some further information about reporting to parents/guardians. In Appendix C, page 50, there is a "Request for access to information checklist".

Principle 7 – dealing with incorrect personal information

Any person has the right to ask a school to correct any of the information held about him or her. If the school does not think the information is wrong then the person has the right to have a statement of the required correction/s placed with the original information.

For example, a school principal might record the behaviour of a student in a meeting, describing the student as angry. The student might disagree with this assessment and ask for the record to be corrected. This does not mean the school principal has to change the record, if he or she is satisfied that the statement was correct. The school need only hold the student's view of the behaviour alongside the principal's view.

If there is inaccurate material, a school does not have to wait for a request for correction. If the school is aware that a record is incorrect then the school must amend it.

Principle 8 – checking for accuracy before use

Before using personal information, a school must take reasonable steps to check that the information is:

- current;
- relevant;
- complete;
- accurate; and
- not misleading.

For example, throughout the year, schools might like to put reminder notices in the school newsletter asking parents/guardians to update any change in their contact details.

Another example might be when a school receives unsolicited information like a complaint about the after-school behaviour of a student. Before relying on this information, the school should check for accuracy, not only by making enquiries of other witnesses, but also by asking the student concerned.

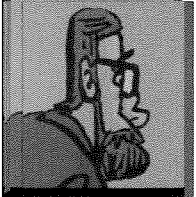
Principle 9 – retaining information for as long as necessary

Personal information must not be held for longer than is necessary for the purposes of the school. In other words, once a school no longer needs the information then it should not be retained.

This principle, like other principles, is subject to other legislation. Schools need to keep records for certain periods of time to comply with legal requirements, for example tax administration legislation.

Under the Public Records Act, state schools also have broader responsibilities to retain some school records for archival purposes, and schools cannot destroy or dispose of any school records without Archives New Zealand's authorisation.

The Ministry of Education together with Archives New Zealand has prepared the School Records Retention/Disposal Information Pack (available at www.minedu.govt.nz/NZEducation/EducationPolicies/Schools/SchoolOperations/PlanningAndReporting/SchoolRecordsSchedule.aspx), which identifies school records that can be discharged or destroyed, and those which must eventually be sent to Archives New Zealand.



These guidelines will also be of benefit to private schools as they set the standard for record retention/disposal.

Apart from keeping records as required by law, schools may want to retain information in order to provide references, answer requests for academic records and maintain an alumni record long after the student has left the school as a service to former students. Retaining information digitally makes this less of a paper war, but it is over to the school to decide how long it keeps information for this purpose, as long as this is with the knowledge and consent of the former student.

Principle 10 – use personal information for its purposes

Schools should only use personal information for the purpose for which it was collected.

For example, if a student consents to being photographed for a school project, the school may not subsequently use the photograph for promotional advertising without consent.

Another example would be where parents/caregivers have provided their contact names and addresses to the school, a member of the Board of Trustees may not use this database to promote his or her business.

Again there are exceptions to this principle, namely where the alternative use is:

- directly related to the reasons for which the information was obtained; or
- authorised by the individual; or
- necessary for the maintenance of the law including the prevention, detection, investigation, prosecution and punishment of offences; or
- necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life or health of any other person; or
- the information is publicly available; or
- the information will not identify the individual.

Principle 11 – limits on disclosure of personal information

The starting point is that a school must look after students' information and not release that information to third parties.

This principle, like other principles, is subject to other legislation. For

example, under the Education Act schools are required to collect essential information on enrolment and to pass this information on to any school to which the student transfers.

Under the Children, Young Persons and their Families Act, if a care and protection co-ordinator from Child Youth and Family seeks information in relation to care and protection matters, then this information must be released.

Courts also have the power to order schools to release information. The most common example is a search warrant under the Summary Proceedings Act. A search warrant is a document issued by a Judge, Court Registrar or Justice of the Peace authorising the Police to enter a specified property to seize goods or documents. If Police have a search warrant you must let them execute the warrant, without interference.

There are exceptions to principle 11. For instance the school **may** release information if the school has reasonable grounds to believe:

- It is one of the purposes for which information was collected in the first place, for example, reporting to parents.
- The information is in a publicly available publication.
- The disclosure is to the individual, for example a student rings the school asking for a result in a test. The school should be reasonably satisfied that it is the student who is seeking information about him or herself.
- The disclosure is authorised by the individual.
- The disclosure is necessary for the maintenance of the law including the prevention, detection, investigation, prosecution and punishment of offences. This can include providing information to the Police and to court appointed "lawyer for child". The chapter "Application of the privacy principles", page 26, has some further information about releasing information to the Police and other government agencies as well as information about releasing information to "lawyer for child".
- The disclosure is necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life or health of any other person, for example, the release of information to the Police or Child Youth and Family about suspected child abuse.
- The disclosure will not identify the individual.

You can see the word "may" is emphasised. Just because the school may release information does not mean it must. For example, many parents/caregivers will have their telephone and address in the local telephone directory, which is a publicly available publication. This means that if a person rang the school and asked for the home phone number of a parent, the school may be able to release that information. However, it does not have to release the information. As a matter of policy most agencies do not provide home phone numbers upon request, even if the phone number is in the telephone directory.

Before releasing information, schools should ensure they are not in breach of a school policy or another law or legal obligation, for example breach of confidentiality under a professional code of ethics (see "Important definitions", page 7).

Principle 12 – use of personal identification numbers

A school cannot create a *unique identifier* – that is a serial number or PIN – for a student unless it is necessary to the efficiency of the school. If the school does apply a number to a student because it is necessary, then this number must be unique and *not the same* as another agency's unique identifier for that person, for example, a public library card number or IRD number. The school cannot insist that this number be revealed to anyone else.

An automatic numbering system by a computer on entering enrolment information or a school library code number is not a breach of this principle as long as the student's name is clearly identifiable from the input of the code number.

In 2006, the Education Act was amended to empower the Ministry of Education to create a unique National Student Number (NSN) for every student.

Part 30 of the Education Act 1989 sets out that the NSN can only be used for the following purposes:

- monitoring and ensuring student enrolment and attendance;
- ensuring education providers and students receive appropriate resourcing;

- statistical purposes;
- research purposes; and
- ensuring that students' educational records are accurately maintained.

An example of an agency that has access to the NSNs is the New Zealand Qualifications Authority that uses NSNs to record credits and qualifications gained by learners on the National Qualifications Framework.

Given the limited purposes of the NSN, schools may want to give students a separate number or identifier for the purposes of school administration but should only do if this is necessary.

Relationship between the Official Information Act and Privacy Act

State sector schools in New Zealand are subject to both the Official Information Act (OIA) and the Privacy Act. This means that they have some additional obligations to provide information on request.

If a person asks a school for information about him or herself, this is governed by principle 6 of the Privacy Act (see the earlier discussion on principle 6, page 17).

If a person asks a school for information about someone else (or about school policies, facilities, or other things that do not involve information about a human being), the OIA applies. The most common example is a parent asking for information about a child – the parent is asking for information about someone other than him or herself, and you therefore need to think about that request under the OIA.

There are three things you have to consider:

1. The starting point under the OIA is that the school should presume it has to make the information available.

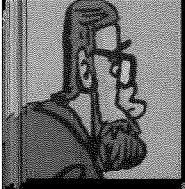
2. However, there are good reasons not to provide information in some circumstances. Protecting privacy is one of the reasons why a school might choose not to release information in response to a request.

   For instance, while there are usually very few privacy difficulties in sharing information about students with their parents, occasionally disclosing information to a parent may have a serious impact on that student, or would otherwise breach their privacy. One common example is information that the student has disclosed in confidence to a school counsellor. There are strong privacy interests in that information. The school should ask the student about releasing the information to the parent (after all, the student might not mind). This will help it decide whether it is necessary to withhold the information from the parent on privacy grounds. The school also needs to take into account the confidentiality obligations of the school counsellor. The chapter "Application of the privacy principles", page 26, has further discussion about the school counsellor's position with respect to privacy.

3. Finally, consider whether, despite the fact you are concerned about privacy, there is nevertheless a strong public interest in making the information available. If that public interest outweighs the concerns about privacy, then you should release the information.

   For instance, schools occasionally attract media attention as a result of an incident, or an investigation into the school's practices. The media – rightly – will want to provide information to the public about what is going on and may well ask questions about staff or students. Care is definitely needed around release of that information. For instance, information about employment or disciplinary matters is highly sensitive. It is very rare that any public interest in knowing that type of information would be strong enough to outweigh the needs of privacy. However, it is something that you should seriously consider. There is useful discussion for state schools about this issue on the Privacy Commissioner's website, www.privacy.org.nz/checklist-for-ministers-and-departmental-officials-2/.

Sometimes requesters ask for copies of documents that contain information about them but also contain information about other people. In this situation the Privacy Act applies to some of the information, and the OIA applies to the rest. This appears confusing at first sight, but the reasons for refusing a request are very similar under both Acts. The outcome may well be exactly the same.



Application of the privacy principles

When confronted with a privacy issue within a school, the first step in addressing the problem is to identify whether or not it is a question about the collection, storage, use or disclosure of personal information.

This part of the book is an attempt to identify some of the common privacy issues for schools and then apply the principles to the situation to assist schools in making their own decisions. It is not meant to be a statement of the law or a definitive legal opinion and if you have any doubt, you should contact the school's legal advisers or the Office of the Privacy Commissioner.

The Board of Trustees is empowered under the Education Act to manage its school while meeting its statutory obligations. In terms of the Privacy Act, the Board will have to consider the following issues.

Appointment of a privacy officer

Each school is required to appoint a privacy officer. Once appointed, the privacy officer should:

- Attend a training course and make contact with the Office of the Privacy Commissioner (see www.privacy.org.nz for contact details and information on training/seminars).
- Undertake an audit of the way the school is handling personal information including collection, storage, use and disclosure.
- Undertake a review of forms used by the school to ensure compliance with the collection principles (1-4).
- Undertake a review of the way information is collected in the school to ensure fairness including:
    - opportunities for parents to discuss the forms or obtain assistance;
    - opportunities for parents/students to discuss matters in private, away from the front reception desk; and
    - videotaping, audio taping or photographing any person (including students) on school grounds with consent or on notice (eg security cameras).

- Undertake an audit of the way information is stored in the school and shared amongst staff. There should be reasonable safeguards to avoid unauthorised access, use, modification or disclosure. Access to information should be limited to staff who need the information for their job.
- Develop policies or checklists to deal with information requests from individuals, guardians/parents or other parties.
- Develop a process for updating records to ensure they are accurate (eg a half-yearly check with parents to ensure contact details are correct).
- Undertake a review of information held to determine if it should still be retained.

Board meetings

Board meetings are usually open meetings at which observers can attend. There are also minutes from the meetings, which are publicly available documents.

If there is to be discussion about an individual at a board meeting, then it is acceptable practice for a resolution to be passed that observers/ non-board members be excluded from all or part of the meeting in order to protect the privacy of that individual.

The relevant part of the minutes needs to be separated from the public copy of the minutes and identified as a confidential document.

Forms

A sample enrolment form is set out in Appendix B, page 47.

As a matter of practicality, information about students and information about parents/guardians will ordinarily be collected from the parents/ guardians. On occasion, information will be collected from the student directly.

In considering questions on an enrolment form, schools should look at each question to work out the information being sought and whether or not it is necessary for the school's purposes (see principle 1).

Schools should also follow any rules issued under the Education Act in relation to enrolment records. The Education Act requires principals of registered schools to ensure that enrolment records are kept and that they contain information as specified by the Minister. When a student moves from one registered school to another, the principal of the first school must take reasonable steps to send the student's enrolment record to the principal of the second school. The Ministry of Education has developed a centralised electronic register (ENROL) to facilitate these obligations.

Identifying the purposes will assist in the framing of questions. For example, there are usually two purposes in obtaining a person's name: identification and communicating with that person. Asking a person's full name may not achieve the second purpose if the first name given is not the name by which the person is known. There will be a barrier to communication if the school uses the name incorrectly. A form should ask for a person's name and the name by which he or she likes to be known.

As noted in the discussion under principle 1, a good test in assessing each question on a form is whether or not the school will be able to complete enrolment if a parent or guardian refuses to answer the question. If the completion of enrolment is not dependent on the answer to the question, then the question is optional.

The school should consider whether or not some aspects of the form are detachable to recognise that sensitive personal information needs to be separately stored to avoid unauthorised access.

It should be clear that there is a right of students and parent/guardians to access and correct their own personal information. This does not mean that guardians/parents have an automatic right to see their children's information (see discussion on the role of parents/guardians, page 30).

A separate form should be used on each occasion that information is collected outside of the purposes identified in the enrolment form. For example, a school should have a new and separate form for extra curricular activities such as a school camp. It is a good idea to do this anyway as it allows the school to check for accuracy before using information (principle 8).

Disciplinary investigations and hearings

Collecting information about a breach or breaches of school rules may not require notification to the person under suspicion in the first instance – particularly if it involves interviewing other people. However a person about whom an allegation has been made should be notified of the investigation as soon as practicable, and as a matter of natural justice.

The information should not be collected in an unfair way. For example, tactics such as frightening or threatening students into giving information or misleading students as to the purpose for collecting information may well mean that the information collected is not reliable or usable. Principals and teachers should remember that, particularly in primary schools, there is a significant power imbalance between people in authority and students. It is pretty scary being asked questions by a grown up! There are also issues about the nature of the questions for example, open questions are better than leading questions which suggest the answer.

If a school wishes to search a person or their property (eg bags), schools need to be aware that it is a right under the New Zealand Bill of Rights Act that a person be secure against unreasonable search or seizure. Generally, consent is needed. The circumstances must justify the search and legal advice should be obtained before a search is conducted.

In conducting a disciplinary hearing, the board should identify from the outset a proper procedure, including fair and reasonable notice, and written notification of any complaint. The board should also identify what information will be released to the complainant at the end of an investigation, including any penalty imposed on the individual.

Usually, the identity of the complainant will be revealed although there may be some circumstances where a complainant's identity remains secret as it is not necessary or relevant to the hearing. For example, there may be sufficient evidence of a breach so that involving a complainant is not necessary. Complainants cannot be guaranteed confidentiality.

Under the Education Act, the principal is required to advise the Ministry of Education and a parent of the student of any stand-down, suspension, exclusion, and expulsion.

Reporting to parents/guardians

One of the purposes of a school is to report to parents/guardians. The Education Act requires schools to report if there is anything affecting the student's progress or harming the student's relationships.

A parent's role as custodial or non-custodial parent does not change a school's duty to report to parents/guardians.

This information is usually shared throughout the year in Parent/Teacher/Student Learning Conferences, release of learning journals or portfolios and end of year reports.

This does not mean that parents are automatically entitled to all information relating to their child. There are times when information may remain confidential between the school and a student.

In one case concluded by the Chief Ombudsman, the child, who was described as an intelligent and well-adjusted teenager, had had no contact with the non-custodial parent for five years and was adamant that the parent not be given the school report. Following consultation with the Privacy Commissioner, the Chief Ombudsman formed the view on the particular facts of this case:

- Releasing the report to the parent would be an infringement of the child's privacy in terms of the withholding ground in the Official Information Act.
- In considering whether there was a public interest in release, it was relevant to consider the Education Act which requires schools to advise parents of matters that are slowing a student's progress or harming their relationships with teachers or other students. In this case there was no evidence of such matters and therefore no public interest in releasing the report to the parent.

The Chief Ombudsman suggested to the school that it write to the parent explaining that the child was doing well at school and there were no matters that needed to be reported on in terms of matters that were slowing the student's progress.

Lawyer for child

Lawyer for child is a lawyer who has been appointed by the Court. The lawyer will represent the child in custody and access matters if a dispute has not been resolved through counselling and mediation and it seems likely the dispute will go to a court hearing. Lawyer for child reports to the Court in the child's best interests.

The New Zealand Law Society (NZLS) has issued a protocol, *Liaison between Counsel for Child and Schools: A Guide for Lawyers Representing Children, (2002)*, which sets practice guidelines for lawyer. It can be found at www.lawsociety.org.nz/home/for_lawyers/resources/guidelines.

Lawyer for child is effectively the duly authorised agent of the child and so the school should see evidence of the appointment. Any request from lawyer for child is a request from a duly appointed agent, so the school has to consider the request under principle 6.

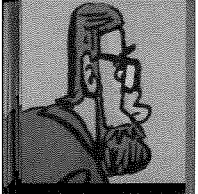
A request for access to information from the school counsellor is a different matter as it will often be a request for health information. This is governed by section 22F of the Health Act and the school counsellor's professional obligation of confidentiality. Sometimes lawyer for child may be refused access to the health information.

As a result, many schools have established their own guidelines for dealing with lawyer for child seeking information about a student.

The NZLS protocol recommends that lawyers make all enquiries in relation to a student through the school principal. Arrangements to interview teachers or school counsellors or to view school records should also be made through the principal. While the consent of the child's parent or guardian to disclose information is not legally required, the NZLS protocol identifies that the best practice is to seek the consent of each parent or guardian of the child. It further advises that consideration should be given to obtaining the consent of the child, having regard to the child's age and maturity.

Transfer of records between schools

Under the Education Act, schools are required to share enrolment information and other school records if a student transfers to another school. The difficulty appears to be deciding whether or not to share



other information that is not required to be shared as a matter of law. This is something that can be anticipated and incorporated into the purposes for collecting personal information. A principal should consider principle 11 and professional codes of conduct/ethics when making a decision about disclosure to a forwarding school.

Counsellors and health information

If the school offers a counselling service, this aspect of the school service is generally considered a health agency for the purposes of the Health Information Privacy Code. This is a Code of Practice issued by the Privacy Commissioner under the Privacy Act and it governs the collection, storage, use and disclosure of health information and it gives individuals the right to access and request correction of their health information. While there are many similarities between the principles in the Privacy Act and the rules in the Health Information Privacy Code, there are some significant differences that are beyond the scope of this book to explore.

There is also other law governing health information held by the counsellor including the Health Act and professional obligations of confidentiality.

It is recommended that the school's counsellor and privacy officer attend training on the Health Information Privacy Code (see the Office of the Privacy Commissioner's website, www.privacy.org.nz for information on training/seminars).

Concerns regularly raised by counsellors involve:

- uncertainty about sharing information, for example, bullying, suicide threats, inappropriate sexual activity, sexual abuse, contraception and abortion; and
- pressure from within the school or by parents/guardians to share information.

Some of these matters are resolved by the professional obligation of confidentiality and a school should not expect a counsellor to offer a service that requires him or her to breach confidentiality. However there are times when a counsellor may share information without breaching confidentiality and the counsellor should seek legal advice from a lawyer or his/her professional body.

Classroom activities/exercises and personal information

Many classroom activities are centred round students revealing information about themselves and their families in a public classroom. These activities are founded on well-established educational principles. For example, it is well established that students will generally learn if they feel connected to the activity. Moving from the known to the unknown is also a recognised process of learning. So a school project on a student's ethnicity/cultural background can help him or her feel connected and help him or her move from the known to the unknown as the student leans the skill of researching history.

However, there may be a good reason why a student is reluctant to share information in the classroom. For example, the student may be adopted or from an immigrant family who may feel some caution in talking about their background. Schools need to be prepared with some alternatives if the learning purpose is at risk by the enquiry into a student's background.

At the start of the school year and each term, many schools are now identifying for parents the upcoming classroom activities/projects. Schools should identify when this might involve personal information, for example family ethnicity, and ask parents to contact the school if there are any concerns about the proposed curriculum.

Volunteers

The role of a volunteer is very important in schools. However, just because someone is donating time to a school does not alter the fact that this person must comply with the school's privacy policy, just as the person must comply with health and safety policies. Volunteers should sign a form that records their understanding of the privacy policy and their agreement to abide by it. There is a draft "Notice to Classroom Helpers" in Appendix B, page 49.

Information and communications technology

The advent of the internet, the role of computers and mobile technology in teaching, does not alter the privacy rights of students. Schools need to develop clear internet, computer and cellphone policies that reflect the right to privacy. The use of the internet and cellphones can also be the subject of learning contracts within the classroom at the start of each year.

Here are some matters to consider:

1. Schools need to identify when they are collecting information and the purposes. If photographs are being taken during school activities then schools must be open and transparent if they wish to put this information on the internet.
2. Before putting information and pictures on the internet, schools need to think about the following:
    - There is no guarantee of confidentiality or security, despite the use of firewalls or other security measures including access code numbers for families.
    - A photograph or record of a child at school on the internet is an electronic footprint. It lasts forever. If one of the purposes of the school is to prepare the student for the future, schools should think about the standard of material that is posted to a website. A funny photograph may look amusing and engaging now but may be embarrassing to the student in his or her future. The same applies to written material.
    - There are child sex offenders who are using photographs of children on school websites for personal gratification and possible identification.
    - Our community is diverse with many members of our community coming from countries where privacy is essential for survival. Should they be compelled to have their child's photos on a website? Is it fair?
    - Refusal by a student or his or her family to have a photograph or other material on the internet or school web page is not a ground to refuse enrolment. This is an optional activity and consent should be obtained.
    - Is the purpose of the photo served by student identification? Can the students' faces be edited in such a way that will allow the activity to be recorded without identifying the children involved?
3. Using information and mobile technology in teaching does not authorise cyber- or text-bullying, or authorise sharing the information on the internet (including social networking sites like Bebo or Facebook). There should be consequences for any breaches of the relevant school rule/policy or learning contract.

4. Schools need to be aware that it is an offence to intercept private communications. It is also an offence to intentionally or recklessly make an intimate visual recording of another person (being a recording without the knowledge or consent of the subject person and the recording is of a private part of their body in circumstances where the subject person would reasonably expect privacy). In other words, the school policy/learning contract needs to be clear that there will be consequences if students break the law while using IT devices or cellphones.

Security cameras/CCTV

The use of security cameras or CCTV is becoming more common in schools to address issues such as vandalism and individual safety. Before installing security cameras, the school needs to consider why it wants to use security cameras and it needs to take professional advice as to whether or not this technology will meet the purpose (eg preventing vandalism). If cameras are installed, schools should display notices about the presence of cameras and schools should have clear policy guidelines about storage and access to the information collected (see principle 5).

Schools should also be aware that footage from security cameras and CCTV is often requested by Police in investigations into criminal activity in the area. Those requests are often made in person by an investigating officer or under a search warrant. If a school is uncertain about releasing information to the police, it should contact its legal advisers but should not interfere in the execution of a search warrant being a Court order which must be followed (see "Enquiries by Police and other government agencies" below).

Enquiries by Police and other government agencies

If the Police have a search warrant in which a Court has ordered release of information, then the school should comply with the terms of the search warrant.

If another government agency seeks information under its legislation (eg mandatory disclosure of information to care and protection co-ordinators under Children, Young Persons and Their Families Act), then the school must be satisfied that it is dealing with that agency and the school is entitled to ask that the agency put the request in writing

setting out the law on which it relies for mandatory release of the information.

If the request is without a search warrant, and the school is satisfied the request is from the Police or other government agency – and the information is necessary for the maintenance of the law including the prevention, detection, investigation, prosecution and punishment of offences – then the school **may** release the relevant information.

If a school is not certain about such release, then the request may be refused and the Police or other government agency can obtain a search warrant if the release is necessary.

Complaints procedure

If someone believes that a school has interfered with their privacy or their child's privacy, they may make a complaint to the Privacy Commissioner. If the Commissioner's office decides to investigate the complaint, it will contact the school.

The Commissioner's staff will try to see if the school and the complainant can resolve their dispute. The Commissioner will help the complainant identify what he or she wants to achieve (for example, getting access to personal information or getting an apology for something the school has done). The Commissioner will then help the school identify what it wants to achieve in terms of resolving the complaint (for example, accept the complaint and provide access or apologise or provide some other solution).

Sometimes, it will be necessary for the Commissioner's office to give an opinion on how the law applies. This will be a useful guide to the merits of the complaint and can assist the school and the complainant to sort out the problem.

If the problem is not resolved then the Privacy Commissioner may refer the matter to the Director of Human Rights Proceedings who may take the complaint to the Human Rights Review Tribunal.

If the Director of Human Rights Proceedings does not take the matter any further, the individual may take a complaint to the Human Rights Review Tribunal, once the Commissioner has finished his or her investigation.

Contact details for the Office of the Privacy Commissioner

Wellington Office
Level 4, gen-i Tower
109–111 Featherston Street
PO Box 10094, Wellington 6143
Telephone: 04 474 7590
Facsimile: 04 474 7595

ENQUIRIES

In Auckland, ph: 09 302 8655
Outside Auckland, ph: 0800 803 909

Email: enquiries@privacy.org.nz
Website: www.privacy.org.nz

Appendix A:
Privacy principles and sections 27 & 29

INFORMATION PRIVACY PRINCIPLES

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;

(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.

SECTIONS 27 & 29

Section 27: Security, defence, international relations, etc

(1) An agency may refuse to disclose any information requested pursuant to principle 6 if the disclosure of the information would be likely—

(a) [omitted]

(b [omitted]

(c) To prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) To endanger the safety of any individual.

Section 29: Other reasons for refusal of requests

(1) An agency may refuse to disclose any information requested pursuant to principle 6 if—

(a) The disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual; or

(b) 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; or

(c) After consultation undertaken (where practicable) by or on behalf of the agency with an individual's medical practitioner, the agency is satisfied that—

(i) The information relates to that individual; and

(ii) The disclosure of the information (being information that relates to the physical or mental health of the individual who requested it) would be likely to prejudice the physical or mental health of that individual; or

(d) In the case of an individual under the age of 16, the disclosure of that information would be contrary to that individual's interests; or

(e) The disclosure of that information (being information in respect of an individual who has been convicted of an offence or is or has been detained in custody) would be likely to prejudice the safe custody or the rehabilitation of that individual; or

(f) The disclosure of the information would breach legal professional privilege; or

(g) In the case of a request made to Radio New Zealand Limited or Television New Zealand Limited, the disclosure of the information would be likely to reveal the source of information of a bona fide news media journalist and either—

(i) The information is subject to an obligation of confidence; or

(ii) The disclosure of the information would be likely to prejudice the supply of similar information, or information from the same source; or

(h) The disclosure of the information, being information contained in material placed in any library or museum or archive, would breach a condition subject to which that material was so placed; or

(i) The disclosure of the information would constitute contempt of Court or of the House of Representatives; or

(j) The request is frivolous or vexatious, or the information requested is trivial.

(2) An agency may refuse a request made pursuant to principle 6 if—

(a) The information requested is not readily retrievable; or

(b) The information requested does not exist or cannot be found; or

(c) The information requested is not held by the agency and the person dealing with the request has no grounds for believing that the information is either—

(i) Held by another agency; or

(ii) Connected more closely with the functions or activities of another agency.

(3) For the purposes of subsection (1)(b) of this section, the term evaluative material means 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; or

(iv) For the awarding of contracts, awards, scholarships, honours, or other benefits; or

(b) For the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or

(c) For the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.

(4) In subsection (1)(c), medical practitioner means a health practitioner who is, or is deemed to be, registered with the Medical Council of New Zealand continued by section 114(1)(a) of the Health Practitioners Competence Assurance Act 2003 as a practitioner of the profession of medicine.

Appendix B: Forms

The purpose of the form on the following page is to give you some idea of the things you need to think about when looking at forms. It is not intended to be the finished article and it is recommended that you give your forms to your legal advisers before implementation. There will be some differences between information needed for primary school education and secondary school education.

ENROLMENT FORM	
Student's surname	
First names	
Preferred first name	
Gender *(circle one)*	Male Female
Date of birth *(Ministry requirement: copy of birth certificate/passport must be attached)*	
Address Suburb Postcode *(you will be required to provide proof of your residential address such as a recent power account to determine eligibility under the enrolment scheme)*	
Home phone number	
Student's cell phone number *(optional)*	
Student's email address *(optional)*	
Entry level *(for example year 1)*	
Ethnicity *(statistical)* Note: on acceptance of enrolment, you will be given an opportunity to advise the school on cultural matters which may assist us	With which of the following ethnic group(s) do you identify? (please circle) New Zealand European New Zealand Māori *(name iwi – may be more than one)*..... Pacific Islands *(state which Island Group)* ..... Asian *(please identify)* Other European *(please identify)* Other *(specify)* .....
School currently attending (or last attended) and Year level	
Country of birth	
New Zealand citizen?	Yes No
Permanent resident status *(circle one)*	Yes No
Student in NZ on a Student Visa *(circle one)*	Yes No Expiry Date.....
Language spoken at home	
Brothers/sisters at school *(names)*	
CAREGIVER 1: Name	
Relationship to student *(include guardianship status if applicable):*	
Address: (leave blank if same as student)	
Phone contact details: *(please advise if there is any problem with leaving voicemail messages)*	Home ..... Work ..... Cell phone .....

Email	
(Repeat above for second or third caregiver)	
Emergency contact person: Name Phone number/s (including cell phone) Relationship to student	
Name of student's doctor Phone *(please attach immunisation certificate with enrolment form (primary schools))*	
Custody/access arrangements about which the school should be aware	
Any medical conditions, health matters or disability about which the school should be aware (please contact us if you wish to discuss any health or disability matters in private)	
Travel to school *(please circle at least one)*	Walk Bicycle Bus Car Motorbike

The information on this form is collected and used by the school to provide education for your child, and it is also used for associated school activities. It is available to all staff of the school and to members of the Board of Trustees. Please advise the school if you have any concerns about disclosure of any of the information within the school.

The school is sometimes obliged by law to give information to government departments (eg Ministry of Education and Ministry of Health) but it will not otherwise be disclosed without your authorisation.

You have the right to request access and to request correction of information held about you by the school. We would be grateful if you could contact the school office if any details need to be changed, especially contact details.

Do you agree to your contact details being passed to the Parent Teacher Association (PTA) for social and fundraising activities within the school? (please circle) Yes No

From time to time the school takes photographs of students to record activities within the school for the students' learning journals, for the school newsletter and for the school website. It is the school's policy that any photos for publication are either positive depictions of the children/young people or the photographs are taken in such a way to avoid identification. Please advise the school if you have any concerns about publication of your child's photos.

Signed: _____ **(Parent/Guardian)**

Date: ____/_____/_____

NOTICE TO CLASSROOM HELPERS

To classroom helpers/volunteers
It is necessary when helping in the classroom that you keep confidential any information that you obtain about the students in the classrooms and not discuss the students outside of the classroom with other people.

(any other matters you might like to include eg health and safety matters, not being alone with children etc)

Appendix C:
Request for access to information checklist

ACTION	CHECK
Identify who is making the request	
Request by person for their own information? (Principle 6 – see below)	
Request by third party (see below)	
Principle 6	
Provide assistance	
Transfer request if necessary	
Decision	
Release to individual	
Information in preferred form	
Charging?	
Advise right to request correction	
Withhold information in whole or in part	
Reasons (see withholding grounds ss27 – 29 Privacy Act)	
Advise right to refer to Privacy Commissioner	
Request by third party	
Agent of individual (duly appointed in writing): treat as Principle 6 request	
Is disclosure required by law? If yes – disclose	

Is request under Official Information Act? (Request to Agency subject to Official Information Act & Information held by Agency) Yes – see below	
Does withholding ground apply eg s9(2)(a) which allows information to be withheld if disclosure would breach a person's privacy: consider principle 11 and its exceptions. Yes – see below	
Is there a public interest in releasing the information which outweighs privacy interest? Yes: disclose	

Does principle 11 allow disclosure? Yes – see below	

Does professional ethics/policy of agency allow disclosure? Yes – agency's choice	