Tags:
Topic
Free content

Title: Key Principles in the Privacy Act 2020

Why and how education consultants and agents must protect students' personal information

Education consultants and recruitment agents – whether in New Zealand or overseas – must by law protect the personal information of their students. The consequences of failing to protect students' information privacy can be severe – and agents operating outside of New Zealand are not exempt.

This project introduces the New Zealand Privacy Act 2020, legislation that defines the rules for information privacy and explains the legal obligations of businesses on- and offshore. You will learn about the rules around data collection, storage, and sharing, and you will learn about what will happen if you breach the Privacy Act. This project will help you explain to parents and other third parties why you may or may not share certain information about your students – even with their family.

1.	**What is personal information and why must we protect it?**
	A. What is personal information?
	B. Why is information privacy important?
	C. What is the Privacy Act?
	D. Must recruitment agents comply with the Privacy Act?
	E. What are the legal consequences if an agency breaches the Privacy Act?
2.	**What do you need to know? Important points of the Privacy Act for recruitment agents**
	A. Collecting information: Don't ask for more than you need

	B. Storing information: Keep your students' personal details safe
	C. Sharing information: Take great care when you share
	D. Every agency must have a privacy officer
3.	**What should you do if you have breached the Privacy Act?**
4.	**How can you help students with a privacy breach**
5.	**Summary**

1. What is personal information and why must we protect it?

A. What is personal information?

Any business or institution, referred to as an agency in the Privacy Act, must protect the personal information of their clients, customers, or students. Personal information identifies a living person as an individual and reveals something about the person. This includes written information such as an address, student transcript and health records, emails, or notes taken during a conversation. It also includes Unique Identifiers (OPC), typically numbers that are assigned to one person only and that are used instead of their name, for example bank account numbers, driver licence or student ID numbers. Other information not in writing, such as photos and spoken comments that you remember or that have been recorded can also be personal information. Academic information, such as grades, courses taken, withdrawals, academic warnings, suspensions or expulsion from an institution also fall into the category of personal information.

Personal information does not need to include the name to identify the person. To give an obvious example: if you have a group of nine boys and one girl, and you share that one of them is pregnant, it isn't difficult to draw the correct conclusion.



B. Why is information privacy important?

How important is it to you that your personal information remains private? Many people around the world are not too concerned about giving away their information and only start worrying about their privacy once it is gone. Here are six good reasons why the privacy of personal information must be protected. Please click on each reason to open a longer explanation.

I. Crime

The most obvious concern is that criminals can use someone's personal information – for example their credit card or bank details or unique identifiers such as one's driver license, passport or tax number – to steal the victim's money. Identity theft is another big worry: criminals pretend to be someone else to commit a crime in that person's name. They might take out a big loan or commit fraud, and they use that person's address, date of birth, middle name, and so on to verify "their" identity. Victims often suffer long-term consequences of these actions.

II. Loss of opportunities

If third parties have information about a person, even though they shouldn't have this information, the person might lose opportunities such as the chance to get a job or a scholarship. For example, a student might have applied for several scholarships in the hope to be selected for one of them. If one selection committee hears that the student is being considered for another scholarship as well, they might select another candidate.

III. Effect on other human rights

Information privacy is important for other human rights as defined in the United Nation's Universal Declaration of Human Rights, for example the right to life, liberty, and security; the right to be safe from attacks on one's honour and reputation; the right to a fair trial; or the right to freedom of opinion and expression. An example: People expressing controversial opinions can be in danger when their address is shared in public.

IV. Harassment and uninvited attention

Keeping personal information private can protect us from harassment and unwanted contact, including unwanted advertisement by mail or email and unwanted visits or phone calls, even sometimes from dangerous people.

V. Humiliation and loss of dignity and *mana*

Keeping personal information private protects people's honour, dignity, and *mana*. The wrongful publication of personal information on the other hand can result in humiliation. Sharing someone's personal information about, for example, their physical or mental health, school grades, or private thoughts can make the person feel ashamed and can cause anxiety and psychological distress. Things that we might not consider to be very private can be used to humiliate people. The law understands "loss of dignity" and "injury to feelings" to be serious matters: in 2003, the NZ Human Rights Tribunal awarded one woman $168,000 for severe humiliation she had experienced. This had to be paid to her by her former employer, who had accessed a photo which the woman had shared privately on Facebook and which the company then used to damage her reputation (see: Record damages awarded for cake photo breach).

VI. Other negative psychological effects

Humans need privacy for their mental health. Privacy is necessary so people can get along with each other in a community. Sometimes, humans don't want to be observed or recognised by others. We also have a need to keep certain information about ourselves a secret from others, and we have a need to decide for ourselves, when, how, and how much information we share about ourselves and with whom.

Our individual need for privacy can differ, depending on our culture, our personality, or our current circumstances. One person might think that sharing some information is "no big deal", while another experiences this as deeply hurtful. For example, sharing a child's photo in a brochure without their consent might make them feel embarrassed and might inspire other children to bully them.

For all these reasons, New Zealand has introduced laws for the protection of personal information. New Zealand is committed to the Universal Declaration of Human Rights ratified in 1948, which requires member states to protect people's privacy.

One piece of legislation in New Zealand is the Privacy Act, which regulates and explains how agencies – including schools, tertiary institutions, education consultants, and recruitment agents – may handle their customers' or students' information.

C. What is the Privacy Act?

The New Zealand Privacy Act contains rules of how agencies (businesses and organisations) must handle the personal information of their customers, clients, or students. Its purpose is to protect people's privacy and prevent any of the problems that we outlined above. It focuses on the privacy of personal information, and it regulates how agencies should collect, store, and share this information. It regulates what agencies must do when they break these rules, that is, when a privacy breach has occurred. It also explains the consequences for such a privacy breach.



The Privacy Act 2020 has 13 principles. Below, we will specifically look at the collection, storage, and use of personal information. The Office of the Privacy Commissioner (OPC) makes sure that agencies follow the Privacy Act. The OPC also handles complaints concerning privacy breaches, and it provides more information and learning materials about information privacy.

This project is an introduction to the Privacy Act and focuses on some of its central requirements around handling private information. However, we cannot cover all aspects, so please be aware: The Privacy Act includes rules for other important areas of information privacy not covered in this project. For example, it explains how long you may keep information, and it tells you what you must do when students want to see or change the information you have about them. To learn more about these other principles you can:

- Go to the website of the Office of the Privacy Commissioner (OPC): Privacy Act 2020 and the Privacy Principles.
- Take one of the short, free online courses provided by the OPC: Free E-Learning. The short course 'Privacy ABC for Schools' might be of particular interest to you.
- Take a look at the Privacy Act yourself: Privacy Act 2020.

Focus on the updated Privacy Act 2020

If you are already familiar with the Privacy Act and would like to focus on the changes and updates in the 2020 version only, please access the following information sheets:

- Updated Privacy Principles
- Cross-border Disclosure.

D. Must recruitment agents comply with the Privacy Act?

Maybe you are wondering whether you are such an agency and whether you must comply with the Privacy Act. And the short answer is: yes, you are an agency and must comply with the Privacy Act.

The long answer is: an *agency* is any organisation or individual person that uses other people's personal information in their work in New Zealand. It doesn't matter whether agencies make a profit or not. It also doesn't matter whether they are located in or outside New Zealand or whether they use clients' personal information in or outside New Zealand – they must comply with the Privacy Act. In fact, be aware that the most recent version of the act, which came into force in 2020, has introduced *Principle 12 – Disclosure outside New Zealand*. This principle explicitly states that the Privacy Act has "extraterritorial effect"; in other words, the rules also

apply to agencies without a physical presence in New Zealand. To learn more about the responsibilities of overseas agencies, read: Principle 12 – Disclosure outside New Zealand.

Finally, it doesn't matter whether an agency has collected information themselves or whether they have received it from other sources. They are still responsible for its protection and must follow the rules stated in the Privacy Act.

The "Code of Practice" and the "London Statement"

The Privacy Act is often indirectly included in your agent agreements with New Zealand institutions. These agreements typically point out that agents must comply with:

- **the Code of Practice**

Education institutions in New Zealand must ensure that agents comply with the *Education Pastoral Care of Tertiary and International Learners Code of Practice* – short: Code of Practice. The Code of Practice requires institutions to make sure that agents do not breach the law, which includes the Privacy Act (Code of Practice, section 38a). Contracts with agents must be terminated if agents breach the law, including the Privacy Act (Code of Practice, section 38d). You can find out more about the Code of Practice in our topic page **"Understand key Code of Practice considerations"**.

- **the London Statement**

The London Statement is a code of ethics specifically for consultants and agents working with international students. It has been signed by New Zealand, Australia, the United Kingdom and Ireland. It describes seven principles around professional and ethical business practices that agents and consultants should follow. As part of the London Statement, agents and consultants are asked to comply with relevant laws and regulations.

E. What are the legal consequences if an agency breaches the Privacy Act?

If a student thinks that an agency – for example their school or their agent – has breached their information privacy, they are encouraged to first talk to the school or agent. If they are unhappy with the response, they can make a complaint to the Office of the Privacy Commissioner (OPC). The OPC will then investigate the complaint to find out if there has been an *interference with privacy*, that is, a breach of privacy which can cause or has already caused harm to the student. Harm means that the student has experienced or might still experience specific damages such as financial loss or a physical injury, loss of (financial or non-financial) benefits such as employment or other opportunities, or emotional damage such as significant humiliation and loss of dignity (OPC – What is an adverse consequence or harm?).

The OPC will try to find a solution for the problem and reach a settlement that both parties find acceptable. Such a settlement can but does not have to involve financial compensation. See: OPC – How OPC works to settle complaints. However, if no solution can be found, the OPC will ask the Human Rights Review Tribunal (HRRT) to get involved. The Tribunal will then investigate further. If it finds the agency guilty of interference with privacy, it can decide that the agency must pay compensation to the student.



In some cases of very minor breaches, no financial compensation must be paid. Instead, the Tribunal might tell the agency to apologise and to change how they handle personal information. They might also publish the agency's name, which can damage the agency's reputation. The Tribunal awards financial compensation or damages to a person if the person has suffered a financial loss or loss of other benefits or significant emotional harm. In 2022, the OPC has stated: "Unless there's a reason to award less, though, the Tribunal has said that cases at the less serious end of the spectrum will range from $5,000 to $10,000, more serious cases can range from $10,000 to around $50,000, and the most serious cases will range from $50,000 upwards. The most the HRRT has awarded so far for a privacy matter is just over $168,000."

2. What do you need to know? Important points of the Privacy Act for recruitment agents

We will now look at four important areas addressed in the Privacy Act: collection, storage, and sharing of information, and the role of the privacy officer. Please note that we cannot cover the entire Privacy Act here. To be well-informed on all matters of the Privacy Act, please consult the website of the Office of the Privacy Commissioner (OPC), including their short self-paced e-learning options.

A. Collecting information: Don't ask for more than you need

The first four principles of the Privacy Act deal with the questions of if, how, and for what purposes agencies can collect personal information from people.

When you collect information from your students, make sure that you:

I. Only collect information that you really need for your work with the student. Don't collect unnecessary information and information that has nothing to do with the recruitment and placement process.
II. Describe the purpose of the information collection clearly. In that way, you know what you need and what you don't need. This also helps you to explain clearly to the student and parents why this information is needed.
III. Collect the information from the students themselves or from their legal guardians. If you obtain information from someone else – for example the student's school – make a note

in your files about the source.

IV. Inform the student that you are collecting information. Tell them why you need this specific information, and explain who you will share it with, for example the admissions team at a school or tertiary institution.

V. Inform the student what will happen if they do not give you the requested information. For example, you might be unable to find a school for them.

VI. Tell the student that they have the right to access and correct the information that you hold about them.

VII. Don't use students' information for purposes other than what you told them and what they agreed to.

VIII. Take particular care when working with minors, that is, children and teenagers. They are seen as particularly vulnerable in New Zealand. Also, students under 18 cannot enter any contracts or agreements, so you must ask their parents' (or legal guardians') permission.

Your privacy statement

It is best practice to have a privacy statement that your students can read on your website or on paper. If you don't have a privacy statement yet or if you want to check whether your statement is fit for purpose in New Zealand, you can use *Priv-o-matic*, a free tool provided by the Office of the Privacy Commissioner (OPC): Priv-o-matic. The OPC further suggests looking at their privacy statement as an example: OPC privacy statement.

Your privacy statement should explain the following:

- Why you are collecting information,
- What information you are collecting,
- How you will use this information,
- Whether you will share the information with others (and with who exactly),
- Whether students must provide this information or whether they can decide not to provide it (and what happens if they don't provide it),
- How students can access their own information and correct it if there are mistakes, and
- How students can contact you about this.

Please note: Even if you have a privacy statement on your website, it is still a good idea to inform students clearly every time you collect their information. This builds trust.

Let's take a look at a case study now and see which of the rules from the Privacy Act apply here.

Case study: Using information in marketing

The recruitment agency *Star Study Adventures* shares real student stories on their website to attract new clients. The stories are written by former international students who studied in New Zealand with the help of the agency. In these stories, the students describe their experiences of living and learning in New Zealand. The students submitted these stories voluntarily, and they have given written permission for these stories to be used on the agency's website in an anonymous way, that is, without showing the authors' real names. There is an event coming up: *Star Study Adventures* wants to present their services at a Study Abroad Fair. They will have a booth at the fair, and they want to decorate it with attractive posters. They also want to hand out paper brochures to interested students. They would like to include some of the stories from their

website in the brochures and on the posters. They would also like to put photos of the authors next to the stories. They still have photos of the authors in their database as part of their applications. Why not use those to create visually attractive advertisement materials?

Back to you: Can *Star Study Adventures* use the stories from the website also in print materials such as posters and brochures? Can the agency use photos from the students' applications in their advertisement materials?

Answer: *Star Study Adventures* cannot use the students' stories in their brochures and posters as the students only consented to their stories being used on the agency's website;have a look at bullet point 7 in the list above. The agency can contact the authors and ask for permission to use the stories also in this new context, but they must accept it if the students say 'no' to the request. Furthermore, the agency may not use the students' photos for two reasons. Firstly, the students only consented to an anonymous use of their stories – but the photos would identify them. Secondly, the photos were collected as part of the students' application process and cannot be used for other purposes such as advertisement.

We have learnt a lot about appropriate data collection. Now we will look at secure data storage.

B. Storing information: Keep your students' personal details safe

Safe information storage is covered in Principle 5 of the Privacy Act. Any agency that is holding people's personal information must take reasonable steps to keep this information safe from (1) loss, (2) being accessed by unauthorised people, and (3) any other type of misuse. Let's look at a short case study:

Case study: Displaying student information in the office

Eva is an education agent in Germany. She works closely with students and often meets them in her office to discuss their applications. One day, Eva receives an email from one of her students, Benjamin Schmidt, in New Zealand. Benjamin writes that he feels depressed and lonely. Eva suggests that Benjamin should see a counsellor and maybe also a doctor. She promises to check in with him in a few days to see how he is doing. To remind herself, she sticks a post-it note on the wall in her office, saying: "Benjamin Schmidt, depressed, check in Monday: benjaminschmidt@yashoo.com." In the meantime, she conducts several interviews with students in her office.

Back to you: How is Eva breaching privacy law? What could she do better to protect Benjamin's personal information? Answers can be found in the text below.

To comply with the Privacy Act, you should keep paper-based personal information in a locked cabinet. Information in digital form should be password protected. In both cases, you should restrict access to personal information to relevant staff only. You should also prevent accidental access by unauthorised people. For example, if you want to throw out paper documents that contain personal information, make sure that they are not thrown into a regular bin in one piece. They must be shredded, so that the words printed on them can no longer be read. The same is true for your old computers: if you throw out old hard drives, make sure you have erased all sensitive data.



Visitors in the office

When you have visitors in the room, don't discuss personal information on the phone. Your computer screens should also face away from visitors. Unauthorised people shouldn't be able to read what is displayed on your computer. In the case study above, Eva has written sensitive personal information about Benjamin on a post-it note, and she has placed that information on her office wall, visible to anyone coming into her office. The post-it note reveals Benjamin's first and last name, his email address, and sensitive information about his mental health. This is a privacy breach. Rather than using a post-it note visible to anyone entering the office, Eva could write a reminder in her diary or she could set a reminder in her digital calendar - but she should make sure that the reminder is not shared with others.

Electronic security

You must also take appropriate steps of electronic security. For example, you must have appropriate firewall- and anti-virus software installed, and you must follow best practice around passwords. If you are using a cloud-based service to store student information, make sure that this isn't accessible to outsiders. Some agencies think that they are too small and insignificant to attract the attention of hackers, but they might be in for a surprise. In 2016, 36 schools in New Zealand learnt their lesson about electronic security when they realised that they had been hacked and student information was put up for sale online. You can read more about it in this news article: Dozens of New Zealand schools hacked.

Now we will discuss when and how you may or may not share a student's information with other people.

C. Sharing information: Take great care when you share

What should you do if a third party asks you for information about one of your students? Should you give it to them?

The short answer in most cases is: no, you shouldn't. You may not share a student's

personal information with third parties unless the student has told you explicitly – and preferably in writing – that you may do so. Even if people put pressure on you, you should not disclose any information that can identify an individual student.

A safe solution: Refer requests to the student's institution

To stay on the safe side, the best approach for education agents is usually to refer any information requests to the student's school or tertiary institution. Even if the request seems legitimate under the Privacy Act, you should at least consult with the institution.

Usually, it is best to leave the decision with the student's school. Typically, education institutions in New Zealand have clear rules around privacy in place, and they are better suited to make decisions about when (not) to share information about students.

If students are under 18 years of age, schools have written agreements with their legal guardians on file, detailing who is allowed to have access to a student's information. For many families, this will be the mother and father only. However, other parents might want to give extended family – for example grandparents, aunts, and uncles – permission to be involved in the education of their child. They can do so by listing specific family members by name in a written agreement with the child's school.

Quick tip: Ask the schools and tertiary institutions you work with about their critical incident procedures. These often include rules around the disclosure of students' personal information.

But what about family?

Some parents approach education agents to find out what their child is up to in New Zealand. If the student in question is 18 years of age or older, agents are not allowed to give parents access to the student's information – unless the student has given expressed (written) permission to do so. This includes academic information, such as grades, withdrawals, course changes, suspensions, or expulsions. If you give students' personal information to their parents without expressed permission, you are breaking the law. This is true even if the parents live outside New Zealand. As explained above, if you, the education agent, are conducting business in or with New Zealand, you must follow New Zealand law, including the Privacy Act.

In some cases, information about students who are not yet 18 years old can also be withheld from their own parents. This can happen when sharing the information with family members might cause harm to the child, for example in situations of family violence. Health information is also a special case in New Zealand: once a child turns 16, they can ask for their health information not to be shared with their parents. Please read more in the OPC's blog post: OPC – Putting children first.

Some recruitment agents find it difficult to explain this to parents who feel entitled to all

information about their adult child. After all, parents are family and they might even be paying the student's school fees and living expenses.

If you are approached by parents of adult students with an information request, you can explain that New Zealand laws - stated in the Privacy Act - prevent you from sharing students' personal information. You can also refer parents to the students' school or tertiary institution. Overall, please remember that it is not your job to mediate between adult students and their parents, if their communication has broken down. Parents should ask their adult children directly if they want to know what is going on in their lives.

There are always exceptions to the rule.

Exceptions: Circumstances when you may share information

There are some rare circumstances when you may disclose students' personal information to third parties. For example, you may share personal information if a student seems to be a danger to themselves or others. You may also share information if required by law - for example if Oranga Tamariki requests information about an underage student or if the police approach you with a warrant. This is also mentioned in the Code of Practice (Code of Practice, section 75, 1c).

If an adult student is injured in an accident, the school or tertiary institution will have an emergency contact on file. As this contact was provided by the student themselves, permission has been given to contact the person in case of an emergency. For minors, schools have emergency contacts on file as well.

However, we want to stress that it is best to refer any information requests, even by the police, to the student's school or institution. You should at least consult with the institution, as it isn't always clear whether the police are really entitled to the requested information. You can learn more on the OPC's website: OPC – Principle 11: Disclosure of personal information. To find out more about what schools are allowed to share about their underage students, please have a look at the OPC's website: OPC – Back to School FAQ.

Students' access to their own information

When students ask you to see the information you have about them, you are legally obligated to provide it. If you refuse to give them access, you are breaching the Privacy Act. If you want to learn more about the right to access one's own information, have a look at the OPC's website: OPC – If someone requests their personal information, do I have to give it to them?

D. Every agency must have a privacy officer

Every agency must have a privacy officer (Privacy Act - 201 Privacy Officer), including agencies located outside New Zealand (OPC Ask Us). The privacy officer doesn't need a degree or certificate, but they should know the rules around the protection of personal

information in New Zealand described in the Privacy Act 2020. The privacy officer makes sure that the agency complies with the Privacy Act. They also handle information requests and work with the Office of the Privacy Commissioner (OPC) in case of a privacy complaint. To learn more about the role of the privacy officer, please read the OPC's answers to the question: OPC – What is a privacy officer? Am I required to have a privacy officer?

Your privacy officer can learn about information privacy through the e-learning modules provided by the OPC: OPC – Free online learning.

Case study: Sharing student information with potential clients

Ashok is an education consultant in India. He is in discussion with a young man interested in doing his undergraduate studies in New Zealand. The family of the young man is very involved in the process. They ask Ashok for the contact details of a former student to get first-hand information about the quality of Ashok's services, life in New Zealand, and the programmes Ashok is recommending. Ashok provides brochures and directs the family to his website, which displays several student testimonials. However, the family insists that they want to hear directly "from the horse's mouth".

Back to you: Can Ashok hand over contact details of a former student to this family? What could he do instead?

Answer: Ashok may not give out any information about students he worked with previously. Students' personal information must be kept confidential, unless they have given expressed (written) permission for their contact details to be shared. Ashok has a few other ideas: he directs the family to *Education New Zealand*'s (ENZ) Facebook presence under *Think New – Study with New Zealand*. Here they can read the posts from Kiwi ambassadors – students from different countries currently studying in New Zealand. These ambassadors are happy to answer questions on Facebook and via direct messaging. Ashok also explains that he is an ENZ Recognised Agent and directs the family to the ENZ website: Find an education agency. Finally, he puts the family in touch with the student recruitment teams at several institutions. Here, they can inquire further about study options and about the institutions' satisfaction with Ashok's services.

3. What should you do if you have breached the Privacy Act?

If you discover that your agency has breached the Privacy Act, you must notify the affected person and you must report the breach to the Office of the Privacy Commissioner (see Privacy Act sections 114 and 115). Go to the OPC's NotifyUs webpage to learn more and to make a report if necessary: NotifyUs. If you notice that you have committed an interference with privacy but do not report it to the OPC, you are again in breach of the law and can be prosecuted. Please take note of the OPC's short pdf-brochure on the matter: Privacy Breach Information (PDF)



"I had to show the transcript of my undergraduate studies to a company for an internship. I couldn't find it, so I asked my recruitment agent if he could give me a copy. He emailed it to me really quickly, which is nice, but it turned out that it was someone else's transcript. I could see the student's grades and personal details. I actually knew the student, and seeing her grades made me wonder how she managed to get a scholarship. I told the agent that it was the wrong transcript, and he sent the correct one. But he didn't ask me to delete the wrong one. I didn't know what to do at the time. I think, if that ever happens again, I'll report it to the Privacy Commissioner."*

(Nicole, postgraduate student from Switzerland)

*If you wonder what to do when sending information to the wrong person, see: OPC – What should I do if I've sent an email to the wrong address?.

4. How can you help students with a privacy breach

If students feel that their right to information privacy has been breached, they might ask you for advice. For example, a student might notice that their school is using their name and photo in a promotional brochure without their permission to advertise the institution overseas. To support the student, you can suggest the following (please click on each point for additional information):

- **Secondary students: Talk to the school**
  A good first step for secondary students is to talk to school staff in charge of international learners to resolve the problem.
- **Tertiary students: Contact the student association and advocacy services**
  Tertiary students can get advice and support from the advocacy services provided by the student association at their institution.
- **Get free legal advice from the Citizens Advice Bureau**
  Students can also get free legal advice at the *Citizens Advice Bureau* (CAB). To start, they can visit the CAB website and find answers through the "Ask Us" function, by entering search terms such as "privacy breach" or "international student": Citizens Advice Bureau.
- **Make a complaint with the Office of the Privacy Commissioner (OPC)**
  If the problem cannot be resolved, students can make a complaint with the OPC. They can find the online complaint form and learn more about the process on the OPC's webpage: Making a complaint.

5. Summary

In this project, we have discussed why it is important for education consultants and agents to protect the personal information of students and how this is done in New Zealand. We have introduced the Privacy Act 2020, and we have explained why you are legally responsible to comply with it - even if you are located outside of New Zealand or if you are sending information to someone located outside of New Zealand. The project has outlined some important points of the Privacy Act that are relevant to recruitment agents, including rules around data collection, storage, and sharing, and the role of the privacy officer. We have discussed what constitutes a privacy breach and what you must do if you think that you might have breached the Privacy Act. The project has also provided ideas of how agents can support students who feel that their school or tertiary institution has mishandled their personal information. Several case studies have provided opportunities for you to apply your theoretical knowledge around the protection of students' information in realistic scenarios. Finally, the project has provided further tools and resources for you to use and to learn more about the topic.

Heoi anō tāku mō nāianei - that's all for now!

References:

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411-249.

All other references included as hyperlinks in the text.

Notes to web designers:

Please note that most or all decorative pictures are taken from pixabay and are copyright free. However, they are just suggestions, providing an idea of the situation, atmosphere, and emotions to be depicted in the ideal photo. It is up to the designer to find an alternative that fits the design requirements. If a photo is under a different copyright license, it is indicated in a comment. This means that I haven't found a photo without copyright or under creative commons but I find that a similar photo should be included to make a point or depict something important (e.g. the tsunami markings on New Zealand roads).

Regarding comments: Some pop-up comments functioning as definitions or further information contain an indication of the source. This is presently indicated as the source name followed by a long URL. The idea is that the source name will be the anchor text for the URL. The link is only included in full because comments in Google Docs don't allow linked anchor text.

Please note that a project might contain graphics that should be used and

that should not be replaced by alternatives. To be safe, please check copyright.