TE AWAMUTU COLLEGE

POLICY STATEMENT ON PRIVACY ACT AND THE USE OF INFORMATION

Rationale
The Board of Te Awamutu College is required to comply with the Privacy Act 2020 in all aspects for employees, and in its role as the body with the overall responsibility for the running of the school and for the children attending the school.

Purposes
The purpose of this policy is to promote and protect individual privacy with regard to:
a. The collection, storage, use, and disclosure of information relating to individuals.
b. Access to information relating to individuals.

Guidelines
- A Privacy Officer to be appointed. (Te Awamutu College's Principal will assume this role as the person responsible for handling privacy issues in the school and dealing with privacy access requests).
- The Board and the staff of the school will adhere to the 13 Information Privacy principles (see Appendix) contained in Privacy Act 2020 in all respects of their work.
- Interference with the privacy of a person occurs where an information principle is breached, a code is breached or information matching provisions are not complied with, and the breach has caused loss, damage, etc, or significant injury to the feelings and/or well-being of the individual.
- It is a requirement for the school to report to the office of the Privacy Commissioner (OPC) if there has been a privacy breach that has caused, or is likely to cause, serious harm.
- The provisions of the Act apply to the Board, all staff who work at the school, parents/caregivers and all pupils.
- The Children and Young Persons Act, Official Information Act, Education and Training Act and other legislation concerning Police may outweigh the Privacy Act.
- Enrolment form to contain a statement for parents/caregivers to agree for school records to be passed on to subsequent or requested from previous schools.
- The Board may refuse to pass on evaluative material according to limits defined in the Act.

Implementation

Staff Information

Personal information pertaining to staff, e.g salary information, medication, curriculum vitae, to be held in a secure cabinet which remains locked unless the Principal and/or office staff are filing.

Pupil Information

All Pupils' Individual Files or cards to be kept in secure storage – access only to senior staff, classroom teacher and parents/caregivers.

- Parents/caregivers to sign an agreement to send information on to subsequent school or to elicit information from a previous school.
- Named lists which include evaluative or assessment information are not to be displayed in any public form or place.
- Classrooms will not be available to public for meetings. Exceptions may be made provided the classroom teacher is in agreement, all sensitive information is secured and other parts of the school are locked.
- Pupils are not to be discussed in front of lay people.
- Information to be given over the phone to appropriate people only and for legitimate reasons.
- Staff are to exercise discretion and common sense when dealing with Privacy Act principles and practices.

Parent/Caregiver Information

- Information stored electronically is available under a confidential password only.
- School to ensure the information kept is essential and current.
- Prior to the issue of any information parents/caregivers should be given the opportunity to object, to disclosure.

Board

- Interviews must be conducted in a completely private area.
- All applicants for positions are to be confidential until an appointment is made.
- No information is to be given about staff unless the giver is a designated referee.
- Board Meetings are usually Open Meetings at which observers can attend. There are also minutes, which are publicly available.
- If there is to be discussion about an individual, 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. (Minutes of this part of the Meeting would be identified as a confidential document and stored accordingly).

CHAIRPERSON _____ DATE 16/9/22

PRINCIPAL _____ DATE 29/8/22

24.8.2022

PARLIAMENTARY COUNSEL OFFICE
TE TARI TOHUTOHU PĀREMATA

New Zealand Legislation
Privacy Act 2020

- Warning: Some amendments have not yet been incorporated

Part 3
Information privacy principles and codes of practice

Subpart 1—Information privacy principles

22 Information privacy principles

The information privacy principles are as follows:

Information privacy principle 1

Purpose of collection of personal information

(1) Personal information must not be collected by an agency unless—

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

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

(2) If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

Information privacy principle 2

Source of personal information

(1) If an agency collects personal information, the information must be collected from the individual concerned.

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

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

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

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

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

(e) that non-compliance is necessary—

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

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

(iii) for the protection of 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

(v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; 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.

Information privacy principle 3

Collection of information from subject

(1) If an agency collects personal information from the individual concerned, the agency must take any steps that 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 authorised or required; and
  - (ii) whether 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, information provided by the IPPs.

(2) The steps referred to in subclause (1) must 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) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.

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

- (a) that non-compliance would not prejudice the interests of the individual concerned; or
- (b) that non-compliance is necessary—
  - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) for the enforcement of a law that imposes a pecuniary penalty; or
  - (iii) for the protection of 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
- (c) that compliance would prejudice the purposes of the collection; or
- (d) that compliance is not reasonably practicable in the circumstances of the particular case; or
- (e) 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.

Information privacy principle 4

Manner of collection of personal information

An agency may collect personal information only—

- (a) by a lawful means; and
- (b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons),—
  - (i) is fair; and
  - (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Information privacy principle 5

Storage and security of personal information

An agency that holds personal information must ensure—

- (a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—
  - (i) loss; and
  - (ii) access, use, modification, or disclosure that is not authorised by the agency; 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.

Information privacy principle 6

Access to personal information

(1) An individual is entitled to receive from an agency upon request—

(a) confirmation of whether the agency holds any personal information about them; and

(b) access to their personal information.

(2) If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.

(3) This IPP is subject to the provisions of Part 4.

Information privacy principle 7

Correction of personal information

(1) An individual whose personal information is held by an agency is entitled to request the agency to correct the information.

(2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances 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) When requesting the correction of personal information, or at any later time, an individual is entitled to—

(a) provide the agency with a statement of the correction sought to the information (a **statement of correction**); and

(b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

(4) If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.

(5) If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

(6) Subclauses (1) to (4) are subject to the provisions of Part 4.

Information privacy principle 8

Accuracy, etc, of personal information to be checked before use or disclosure

An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Information privacy principle 9

Agency not to keep personal information for longer than necessary

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

Information privacy principle 10

Limits on use of personal information

(1) An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds,—

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

(b) 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

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

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or

(e) that the use of the information for that other purpose is necessary—

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

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

(iii) for the protection of 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 use of the information for that other purpose is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

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

(2) In addition to the uses authorised by subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a **secondary purpose**) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

Information privacy principle 11

Limits on disclosure of personal information

(1) An agency that holds personal information must not disclose the information to any other agency or to any person 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 disclosure is to the individual concerned; or

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

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(e) that the disclosure of the information is necessary—

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

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

(iii) for the protection of 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 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 enable an intelligence and security agency to perform any of its functions; 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 necessary to facilitate the sale or other disposition of a business as a going concern.

(2) This IPP is subject to IPP 12.

Information privacy principle 12

Disclosure of personal information outside New Zealand

(1) An agency (**A**) may disclose personal information to a foreign person or entity (**B**) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if—

(a) the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act; or

(b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; or

(c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or

(d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or

(e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or

(f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B).

(2) However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1).

(3) In this IPP,—

prescribed binding scheme means a binding scheme specified in regulations made under section 213

prescribed country means a country specified in regulations made under section 214.

Information privacy principle 13

Unique identifiers

(1) An agency (**A**) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

(2) A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (**B**), unless—

(a) A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or

(b) the unique identifier is to be used by A for statistical or research purposes and no other purpose.

(3) To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.

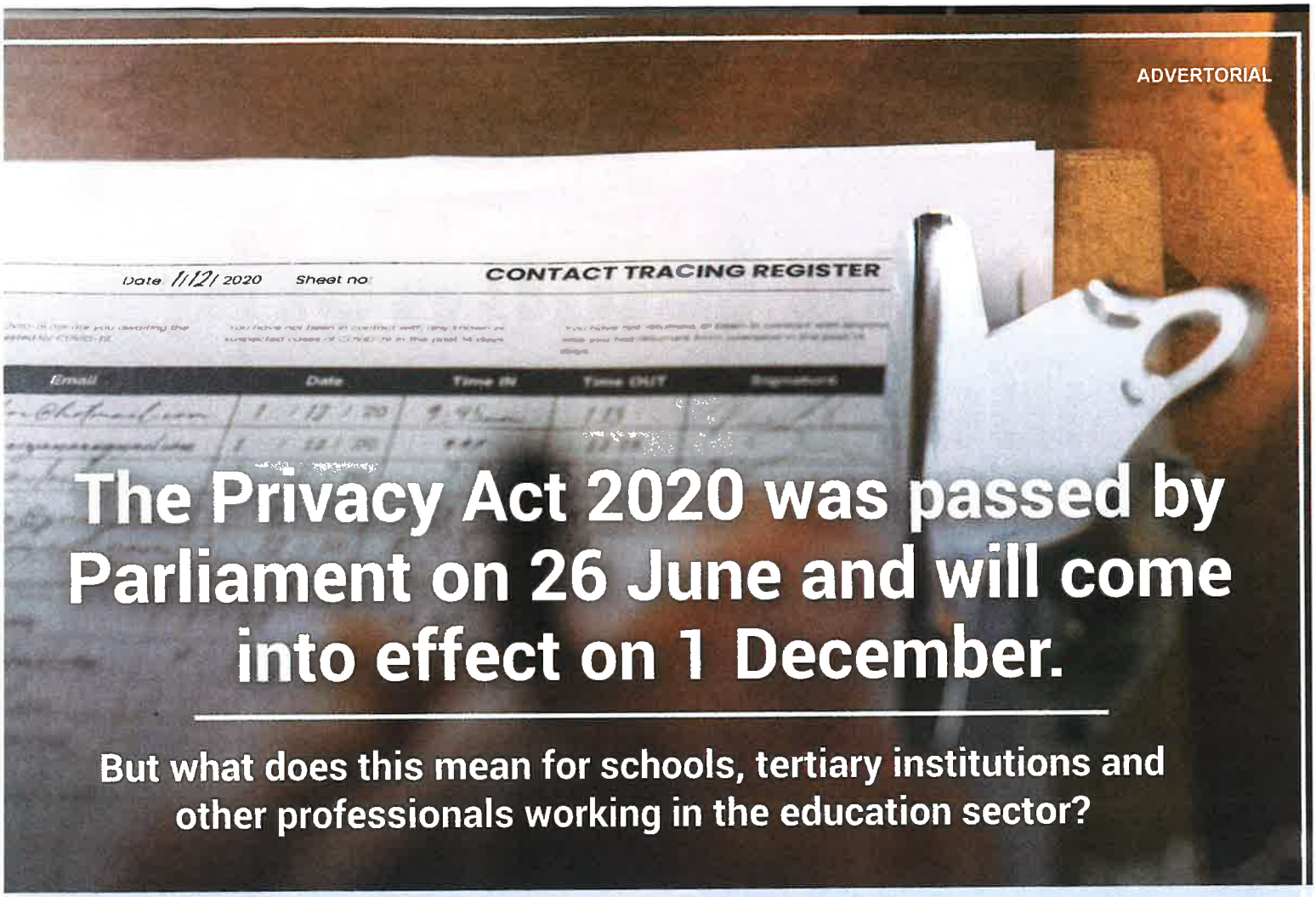
(4) A must take any steps that are, in the circumstances, reasonable to ensure that—

(a) a unique identifier is assigned only to an individual whose identity is clearly established; and

(b) the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).

(5) An agency may 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 is for a purpose that is directly related to one of those purposes.

Compare: 1993 No 28 s 6



The Privacy Act 2020 was passed by Parliament on 26 June and will come into effect on 1 December.

But what does this mean for schools, tertiary institutions and other professionals working in the education sector?

Notifiable privacy breaches

The main thing to consider is that the legal requirements when responding to a privacy breach are changing. The new Act will make it a requirement for your organisation to tell the Office of the Privacy Commissioner (OPC) if there has been a privacy breach that has caused, or is likely to cause, serious harm. Currently, reporting a privacy breach is entirely voluntary.

With this change in place, it will be an offence to fail to inform the Privacy Commissioner when there has been a notifiable privacy breach.

What is serious harm?

It is important to note that not all privacy breaches need to be reported to OPC. The threshold for a notifiable breach is 'serious harm'. This can be assessed by considering, for example, the sensitivity of the information lost, actions taken to reduce the risk of harm, and the nature of the harm that could arise.

OPC has recently launched NotifyUs—an online tool enabling businesses and organisations to easily assess whether a privacy breach is notifiable.

Resources

A new e-learning module dedicated to the Privacy Act 2020 changes is available on the OPC website, which should only take about 30 minutes to complete. OPC's e-learning modules—which include Privacy ABC for Schools—require a basic registration, but are free for anyone to do. It's a great way to bring your staff up to speed with the privacy issues affecting them.

Other resources are also available to help you understand the changes to the Act. There's a podcast series with the Privacy Commissioner and our Legal Counsel, covering all the key changes, as well as the notifiable privacy breach requirement.

Other key changes

The new Act retains the privacy principles of the 1993 legislation, with some changes. Here are the other main changes:

1. **Compliance notices**
   The Privacy Commissioner will be able to issue compliance notices to organisations to require them to do something, or stop doing something, in order to comply with the Privacy Act. Compliance notices will describe the steps that the Commissioner considers are required to remedy non-compliance with the Act and will specify a date by which the organisation or business must make the necessary changes.
2. **Enforceable access directions**
   The Privacy Commissioner will be able to direct agencies to provide individuals access to their personal information. This will allow faster resolution of complaints relating to information access. Access directions will be enforceable in the Human Rights Review Tribunal.
3. **Disclosing information overseas**
   A new privacy principle 12 has been added to the Privacy Act to regulate the way personal information can be sent overseas. Under principle 12, an organisation or business may only disclose personal information to an agency outside of New Zealand if the receiving agency is subject to similar safeguards to those in the Privacy Act 2020. If a jurisdiction does not offer similar protections, the individual concerned must be fully informed that their information may not be adequately protected, and they must expressly authorise the disclosure.
4. **Extraterritorial effect**
   The new Privacy Act now clearly states that it has extraterritorial effect. This means that an overseas organisation that is 'carrying on business' in New Zealand will be subject to the Act's privacy obligations, even if it does not have a physical presence here. This will affect businesses located offshore.
5. **New criminal offences**
   The Privacy Act 2020 introduces new criminal offences. It will now be an offence to mislead an agency to access someone else's personal information—for example, impersonating someone in order to access information that you are not entitled to see. It will also be an offence for an organisation or business to destroy personal information, knowing that a request has been made to access it. The penalty for these offences is a fine of up to $10,000.