Privacy Breach Policy and Procedure - New Zealand

Purpose

The purpose of this Policy is to ensure that the College complies with its obligations under the NPB Scheme and takes a best practice approach to the identification, escalation and management of actual and suspected Privacy Breaches at the College.

Applicability

This Policy applies to all employees of the College.

Definitions

"**CEO**" means the College of Law Group Chief Executive Officer.

"College" means the College of Law New Zealand Limited (NZBN 9429036109722).

"College of Law" means the College of Law Limited (ABN 61 138 459 015).

"**Commissioner**" means the New Zealand Privacy Commissioner.

"**COO**" means the College of Law Chief Operating Officer.

"Privacy Breach" means:

- unauthorised or accidental access to, or disclosure, alteration, loss or destruction of Personal Information; or
- an action that prevents the College from accessing Personal Information either on a temporary or permanent basis.

"**Notifiable Privacy Breach**" has the meaning given to it in section 112 of the Privacy Act and means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals, or is likely to do so.

"**NPB Scheme**" means the Notifiable Privacy Breach scheme established by Part 6 of the Privacy Act.

"**Personal Information**" has the meaning given to it by the *Privacy Act* and means information about an identifiable individual.

"**Privacy Act**" means the Privacy Act 2020 including the Information Privacy Principles in section 22 of the Act.

"SEC" means the College of Law Senior Executive Committee

"Sensitive Information" means: information or an opinion about an individual's: racial or ethnic origin; or political opinions; or membership of a political association; or religious

beliefs or affiliations; or philosophical beliefs; or membership of a professional or trade association; or membership of a trade union; or sexual orientation or practices; or criminal record; that is also Personal Information; or health information about an individual; or genetic information about an individual that is not otherwise health information; or biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or biometric templates.

Personal Information in the College context

Personal Information is regulated, and the College is obliged to protect it, whether or not it is available in the public domain. Personal Information is not the same as confidential information.

The following is a non-exhaustive list of what may constitute examples of Personal Information in the College context:

- course information related to some customers, such as grades and assessment results
- customer work experience and clinical experience placement details
- details such as email addresses, residential and work addresses, ID photos and phone numbers related to staff, customers, suppliers and other third parties that may deal with the College such as students, job applicants and contractors tendering for work
- identification document details such as passports and driver's licences
- credit card details
- employee records such as bank account details, identification documents and Inland Revenue Department numbers
- assessments and predictions relating to individual or groups, for example, if the College forms a view that a particular practitioner may be interested in a particular course or program, and/or
- Sensitive Information about employees or customers, such as employee trade union membership (provided the information or opinion otherwise meets the definition of Personal Information).

Information that is not about an identified individual perhaps because it is not linked to a name address or unique identifier, can become Personal Information when it is combined with other information, if the combination makes the subject reasonably identifiable.

What is a Privacy Breach in the College context?

The following is a non-exhaustive list of what may constitute examples of a Privacy Breach in the College's context:

- loss or theft of physical devices, for example, a laptop or paper records that contain personal information
- unauthorised access to Personal Information by an employee

- inadvertent disclosure of Personal Information due to human error, for example, an email containing Personal Information that is sent to the wrong person, the wrong attachment (containing personal information) is attached to an email, the members of a mailing listed are cc'd rather than bcc'd, thereby disclosing the email addresses and membership of the group to each addressee
- disclosure of an individual's Personal Information through unauthorised third party access to the College's systems, for example, where an employee does not maintain a strong password, shares a password, or falls victim to a phishing scam resulting in unauthorised access to College systems via compromised credentials or installation of malware on College systems, and
- sharing information with third parties in a manner that is inconsistent with the College's Privacy Policy, for example, providing third party access to personal information to a third party service provider without imposing restrictions on the use and disclosure in line with the College's Privacy Policy.

What are the potential consequences of a Privacy Breach?

An individual may be at risk of serious harm when their personal information is involved in a Privacy Breach.

Examples of serious harm to individuals arising from a Privacy Breach may include:

- emotional or psychological distress, including humiliation, damage to reputation and relationships (a particular risk if the individual is susceptible or vulnerable)
- financial fraud including bank account fraud and unauthorised credit card transactions
- identity theft causing financial loss or personal distress resulting in emotional and psychological harm, and
- physical harm or intimidation, for example, where the person is protected by a court order or holds a potentially contentious office and the address and/or contact details of the individual are not in the public domain.

A Privacy Breach also has the potential to negatively impact on the College's business, brand and reputation. If the College is perceived as unable to keep Personal Information secure in accordance with its privacy obligations, members of the public may elect not to engage with the College.

What is the purpose of the NPB Scheme?

The primary purpose of the NPB Scheme in Part 6 of the Privacy Act is to ensure transparency in the handling of Personal Information by making agencies directly accountable to affected individuals and the Commissioner when there is a NPB.

Affected individuals and the Commissioner must be notified as soon as practicable if there is a Privacy Breach that it is reasonable to believe has caused, or is likely to cause, serious harm to an affected individual. See below (Assessment of likelihood of serious harm) for factors to consider in assessing whether or not serious harm is likely, and (Notifying individuals affected by the Privacy Breach) for exceptions and qualifications on the obligation to notify affected individuals.

Internal escalation of Privacy Breaches

If any staff member becomes aware of or suspects:

- unauthorised or accidental access to Personal Information held by the College
- unauthorised or accidental use or disclosure of Personal Information held by the College
- unauthorised or accidental loss, alteration or destruction of Personal Information by the College, and/or
- the College being prevented from accessing Personal Information (either on a temporary or permanent basis),

the staff member must notify the NZ Privacy Officer immediately by completing the Privacy Breach Form which will immediately trigger a notification to the NZ Privacy Officer for investigation, containment and assessment.

It is the responsibility of every staff member to escalate all cases of actual or suspected Privacy Breaches as soon as practicable to the NZ Privacy Officer for review and assessment.

Managing actual and suspected Privacy Breaches after escalation to the NZ Privacy Officer

Each actual or suspected Privacy Breach will need to be dealt with on a case-by-case basis with an understanding of the risks posed by the breach and the actions that would be the most effective in reducing or removing the risks. The NZ Privacy Officer is responsible for coordinating the completion of the following steps in response to an internal escalation of a suspected or actual Privacy Breach as applicable.

1. **Investigate** the suspected Privacy Breach to determine whether an actual Privacy Breach has taken place.
2. **Contain** the Privacy Breach to prevent any further compromise of Personal Information.

3. **Assess** the Privacy Breach by gathering the facts and evaluating the risks, including potential harm to affected individuals.
4. **Remediate** the risk of serious harm for some or all affected individuals.
5. **Notify** affected individuals and the Commissioner if serious harm has, or is likely, to occur, in accordance with Part 6 of the Privacy Act.
6. **Review** the incident and consider what actions can be taken to prevent further breaches.

Where the actual or suspected Privacy Breach has occurred with the involvement of College Shared Services, the NZ Privacy Officer must refer the matter to the COO to coordinate the completion of the following steps.

The NZ Privacy Officer is responsible for notifying the NZ CEO of any actual or suspected Privacy Breaches.

Appointment of Privacy Breach response team

In some cases, the nature and scale of the Privacy Breach and the potential risk posed to the College by the Privacy Breach may be such that a response team will need to be appointed. The NZ CEO will make an assessment as to whether a response team is required and, where deemed necessary, is responsible for the appointment of the response team. While the functions represented on the response team will vary depending on the nature of the Privacy Breach, any appointed response team may include:

Role	Responsibilities
Team leader	Leading the response team and reporting back to the business
Project manager	Coordinating the response team and providing support to members
External legal support	Identifying legal obligations and providing advice
Risk management	Assessing the risks arising from the Privacy Breach
Information Technology	Establishing the cause and impact of the Privacy Breach where systems have been involved/ reviewing security and monitoring controls relating to the breach
Human Resources	If the Privacy Breach was due to the actions of a staff member

Media/communications	Communicating with affected individuals and dealing with the media/external stakeholders

Investigating suspected Privacy Breaches

Where a suspected Privacy Breach has been escalated internally, an investigation will be commenced into whether an actual Privacy Breach has taken place. How this investigation takes place will depend on the nature of the suspected Privacy Breach but may, for example, involve the engagement of a third party to conduct a forensic investigation of a system, or an internal examination of system logs or records.

The College will consider the following factors before undertaking a forensic investigation:

- the potential benefits of having an independent third-party examine and report on the evidence
- the need to preserve evidence regarding the state of systems at the time of the breach and associated records, and
- the potential exposure of the College to third party claims as a result of the Privacy Breach and, accordingly, whether any report obtained for the purpose of legal advice make the report subject to legal professional privilege.

If the investigation phase reveals that an actual Privacy Breach has taken place, the College will move to contain the Privacy Breach to prevent any further compromise of Personal Information.

Containing Privacy Breaches

If an actual Privacy Breach has taken place, action will be immediately taken to limit the Privacy Breach, for example, stop the unauthorised practice or shut down the system that was breached. The following questions will be addressed in the "contain" phase.

- Has all evidence associated with the incident been preserved for analysis and review?
- How did the Privacy Breach occur?
- Is the Personal Information still being shared, disclosed or lost without authorisation?
- Are there indications of who has or may possibly have obtained access to the Personal Information? If so, what does that indicate about the possible risk to data subjects?
- Is there evidence of exfiltration of data? If so, what data was involved and what was the extent of exfiltration?

- Has the system been tampered with, for example, has a false account been created to facilitate later or ongoing access? Is the data stored by the system accurate and complete or has it been damaged?
- If data has been lost, what can that data be used for? What is the risk to data subjects?
- What can be done to secure the information, stop the unauthorised access or disclosure and reduce the risk of harm to affected individuals?

Assessment of likelihood of serious harm

The College is required to conduct an assessment of any Privacy Breach in order to determine whether the Privacy Breach is likely to cause serious harm to an individual whose Personal Information was part of the Privacy Breach (which will determine whether the Privacy Breach is a Notifiable Privacy Breach).

When assessing whether or not the Privacy Breach is likely to cause serious harm, the College must consider the following factors which are based on the matters set out in section 113 of the Privacy Act:

- whether there has been any action taken by the College to reduce the risk of harm following the breach:
- whether the personal information is sensitive in nature:
- the nature of the harm that may be caused to affected individuals:
- the person or body that has obtained or may obtain personal information as a result of the breach (if known):
- whether the personal information is protected by a security measure:
- any other relevant matters.

The NZ Privacy Officer (or team leader, if a response team is appointed) will provide advice to the NZ CEO as to whether or not the Privacy Breach is a Notifiable Privacy Breach after completing this assessment.

Notification requirements for Notifiable Privacy Breaches

The College is required to notify the Commissioner and individuals affected by the Privacy Breach, as soon as practicable after it becomes aware that a Notifiable Privacy Breach has occurred.

There are limited exceptions to the requirement to notify affected individuals, and limited grounds on which notification to affected individuals could be delayed. These are set out in section 116 of the Privacy Act.

Any decision to:

- notify the Commissioner; and/or
- notify (or to not notify or delay notification to) affected individuals,

must be made by the NZ CEO**.**

A Notifiable Privacy Breach occurs when the following criteria are met:

- there is unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, Personal Information held by the College; **or**
- there is an action that prevents the College from accessing Personal Information held by the College on either a temporary or permanent basis; **and**
- the action was caused by a person inside or outside of the College, or is attributable in whole or in part to any action by the College, or is ongoing; **and**
- this has or is likely to result in Serious Harm to any of the individuals to whom the information relates.

One of the factors in determining whether or not serious harm to an individual is likely to result includes "any actions taken by the agency to reduce the risk of harm following the breach". Therefore a Privacy Breach may not be a Notifiable Privacy Breach if the College is able to take actions to reduce the risk of harm, such that the Privacy Breach will not be likely to result in serious harm to any data subject.

For example:

- if an email is sent to the wrong recipient and the recipient agrees to delete it and not keep any copies
- if accounts can be locked and passwords can be changed before unauthorised access takes place, or
- if a security system can be used to disable access to a system or device.

Having regard to all the circumstances, the College may decide to notify data subjects of the incident even in circumstances where it may not be required to do so under the NPB Scheme.

Notification requirements: College students in international programs

The notification requirements apply to any Notifiable Privacy Breach that relates to Personal Information held by the College. This includes where the Privacy Breach relates to a student in an international course (e.g. College of Law Australia or College of Legal Practice

students) or to the employee records of a College of Law Australia or College of Legal Practice staff member and whether or not the Personal Information was collected from a person in New Zealand or outside New Zealand.

Notifying the Commissioner

In the case of a Notifiable Privacy Breach, the NZ CEO is responsible for notifying the Commissioner, such as through the Commissioner's website. Notification is to be given as soon as practicable after becoming aware that a Notifiable Privacy Breach has occurred.

The notification to the Commissioner must include the particulars set out in section 117(1) of the Privacy Act. These include:

- a description of the Notifiable Privacy Breach, including:
  - the number of affected individuals (if known); and
  - the identity of any person or body that the College suspects may be in possession of personal information as a result of the Privacy Breach;
- explain the steps taken or intended to be taken by the College in response to the privacy breach, including whether notice has, or will be given to affected individuals (and if this is by public notice, the basis on which the College is relying on for giving public notice);
- whether the College is relying on an exception to giving the affected individuals notice, or is delaying notification, and the reasons why;
- any other agencies the College has contacted about the Privacy Breach (for example, this could include the police); and
- details of a contact person within the College for inquiries.

Notifying individuals affected by the Privacy Breach

In the case of a Notifiable Privacy Breach, the College is required to give notice to affected individuals. Notifying individuals affected by a Privacy Breach gives an affected individual the opportunity to take steps to protect their Personal Information following a Privacy Breach. Each incident needs to be considered on a case-by-case basis to determine what notifications are required and how notification should take place.

Factors that will be considered include:

- the obligations of the College under the NPB Scheme
- the most appropriate method of notification (generally this should be directly to the affected individual in person, by email or telephone, but public notice can be given if it

is not reasonably practicable to notify an affected individual or each member of a group of affected individuals)
- the form and content of the notification, and
- whether the incident triggers reporting obligations to other entities (for example, any contractual obligations the College may have with its service providers or insurers).

Under the Privacy Act, an affected individual in relation to a Privacy Breach means the individual to whom the personal information that is the subject of the Privacy Breach is about. It covers individuals in New Zealand and overseas, and also includes a deceased person.

There are very limited exceptions to the obligation to give notice of a Notifiable Privacy Breach to affected individuals. These are set out in section 116 of the Privacy Act. These include where the notification could endanger the safety of any person or where the affected individual is under the age of 16 and the College believes that notification would not be in that individual's interests. Notice can be delayed if notice would have risks for the security of personal information held by the College and those risks outweigh the benefits of notifying affected individuals.

Before any decision to rely on an exception to the requirement to give notice, or to delay notice, is made, careful consideration of the provisions of section 116 of the Privacy Act is required.

If the College intends to give public notice of a Notifiable Privacy Breach, it must be given in a form in which the affected individuals are not identified, and it must comply with any regulations made under the Privacy Act.

Notification to an affected individual is required to:
- describe the Notifiable Privacy Breach and state whether the College has or has not identified any person or body that the College suspects may be in possession of the affected individual's personal information (but the identity of such person/body can only be disclosed if the College believes this is necessary to prevent or lesion serious threat to the life or health of the affected individual or another individual);
- explain the steps taken or intended to be taken by the College in response to the Privacy Breach;
- where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any);
- confirm that the Commissioner has been notified under section 114 of the Privacy Act;
- state that the individual has the right to make a complaint to the Commissioner; and

- give details of a contact person within the College for inquiries.

Review of Privacy Breaches

Every Privacy Breach will be reviewed after the event and the College should consider what actions it can take to prevent further breaches. This phase may involve:

- engaging a third party to complete a security review
- the creation of a prevention plan to prevent similar incidents in the future
- the scheduling of regular audits to ensure that the prevention plan has been successfully implemented
- a review of policies and processes to reflect the lessons learned from the review, and/or
- improvements to staff training and awareness.

When reviewing a Privacy Breach incident, it is important to use the lessons learned to strengthen the College's Personal Information security and handling practices, and to reduce the chance of reoccurrence. A Privacy Breach will be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies, procedures or staff training and awareness.

Documentation and record keeping

The NZ Privacy Officer is responsible for keeping the details of any actual or suspected Privacy Breaches up to date on the College's Privacy Breach Register. Details of internal reviews, decisions and supporting evidence relating to any suspected or actual Privacy Breaches will be stored securely along with any documentation or implementation plans prepared in the review phase.

Communication about Privacy Breaches

The NZ Privacy Officer is responsible for:

- notifying the NZ CEO, the COO and the Company Secretary of any suspected or actual Privacy Breaches at the time of notification
- keeping the NZ CEO, the COO and the Company Secretary up-to-date with the progress and results of any Privacy Breach assessments, investigations, notifications or reviews, and
- notifying the impacted Business Unit leader(s) of the progress and results of any Privacy Breach assessments, investigations, notifications or reviews that may be pertinent to that Business Unit.

	The NZ CEO and/or the Company Secretary is responsible for communicating any relevant details of actual or suspected Privacy Breaches to the Board of Governors and/or to the Audit, Risk and Compliance Committee as appropriate. The COO is responsible for reporting any NZ Privacy Breaches to the SEC. SEC members are responsible for following through on any relevant requirements or obligations under agreements with third parties that may arise from the Privacy Breach in their area of the organisation, for example, insurance policies and/or service agreements.
NZ Privacy Officer involvement in Privacy Breach or unavailability	Where the NZ Privacy Officer has been involved in the actual or suspected Privacy Breach or is otherwise unavailable, the NZ CEO will nominate an alternative staff member to discharge the responsibilities of the NZ Privacy Officer under this Policy.
Related documents	*Access Direction and Compliance Notice Procedure (NZ)* *Cookies and Electronic Marketing Policy (NZ)* *Data Security Policy* *Personal Information Access and Correction Policy (NZ)* *Personal Information Collection, Storage, Use and Disclosure Policy (NZ)* *Privacy Act 2020* *Privacy Breach Register (NZ)*