



## PRIVACY POLICY

*For those involved in a University of Notre Dame Australia (UNDA) degree or course, UNDA Policies and Procedures also apply.*

### Introduction

This privacy policy explains how Te Kupenga collects, stores, uses and shares personal information. Openness and transparency are important to us. The Privacy Act 2020 requires us to be clear about the personal information we collect and how it is used. All those who engage with Te Kupenga should have confidence that we handle their personal information lawfully and carefully.

Student studying with Te Kupenga – Catholic Theological College should refer to the *Catholic Theological College Privacy Statement*, which identifies how specific student information collected and used, and how to address any possible breaches or complaints.

### Guidelines

These guidelines were drafted in reference to the New Zealand Catholic Bishops Conference (NZCBC) Privacy Policy, following the introduction of the Privacy Act 2020.

1. When we collect personal information about an individual, we make known the purpose of collecting it, who will have access to it, and whether it is compulsory or optional information. We advise that individuals have the right to request access to, and correction of, their personal information.
2. We only collect personal information:
  - a. For purposes connected with the function of the entity, and only when it is necessary to have this information.
  - b. Directly from the person concerned, or, if a minor, their parent or guardian, unless it is publicly available from elsewhere, or the person's interests are not prejudiced when we collect the information from elsewhere.
  - c. In a transparent and respectful manner.
3. We have reasonable safeguards in place to protect personal information from loss, unauthorised access, use, or disclosure. These safeguards include the use of individual logins for computers, and lockable filing cabinets. We may require volunteers and third-party contractors to sign confidentiality agreements.
4. If an individual wants access to information we hold about them, we provide it. Individuals may request correction of this information or, when not corrected, that a record of the request is attached to the information.
5. We take reasonable steps to make sure personal information is correct, up to date, relevant and not misleading.
6. We only keep information for as long as it is needed, and for the purposes for which it was obtained.
7. Information is only used for the purposes for which it was obtained except in certain circumstances (for example, for statistical purposes where the person's identity is not disclosed).

8. We safeguard people's information and we do not release that information to third parties unless we are allowed, or required, to release information by law. This covers disclosure to persons other than those able to legitimately access material about others (such as a guardian of a minor).
9. As a general rule, information about any person is not given to a third party without the person's knowledge, unless:
  - The information is already publicly available.
  - It is being passed on in connection with a purpose for which it was obtained.
  - The right to privacy is over-riden by other legislation.
  - It is necessary for the protection of individual or public health and safety.

### **Records required by legislation**

Personnel files will be kept for at least six years and financial and pay records seven years, as per the Employment Relations Act 2000.

### **Guidelines for Legal Holds: preserving records during litigation or investigations**

When litigation, an audit, or investigation occurs or is reasonably anticipated, a written notice (referred to as a "Litigation Hold Notice" or "Legal Hold") will be issued to appropriate staff. All records, whether official records, information copies, working documents, or transitory records, potentially relevant to the matter must be retained until the Litigation Hold is terminated. The effect of this notice is to freeze or suspend the destruction or alteration of records, electronically stored information, and other materials identified in the notice.

The Motu Proprio by Pope Francis, *Vos Estis Lux Mundi*, Article 2, §2 also provides for data protection in relation to complaints of sexual abuse matters.

Records relevant to the matter may not be destroyed - even if the retention period in relevant Retention and Records Disposal Schedules have expired or expires during the Litigation Hold - until the action is resolved and a notice terminating the Hold has been issued. There are serious legal consequences for individuals that destroy or alter records under a Litigation Hold or know of a pending issue and do not halt destruction.

### **Guidelines for privacy breaches**

Privacy breaches are the loss of personal information to a third party that has no right to that information. If a privacy breach is identified, the first step is to report to the Director of the Nathaniel Centre, John Kleinsman, who is Te Kupenga's Privacy Officer. The email address to use is [jkleinsman@nathaniel.org.nz](mailto:jkleinsman@nathaniel.org.nz) or phone 04 499 2251.

The Privacy Officer will work through four steps:

- Contain the breach and make a first assessment.
- Evaluate the breach, in consultation with the Chief Executive (or the Director of Catholic Theological College (CTC), if the breach involves CTC student data).
- Notify affected people if necessary.
- Prevent the breach from happening again.

If a privacy breach has caused (or is likely to cause) serious harm, the Privacy Officer will need to notify the Office of the Privacy Commissioner and affected individuals as soon as possible. Under the Privacy

Act 2020, it is an offence to fail to inform the Privacy Commissioner when there has been a notifiable privacy breach.

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, the nature of the harm that could arise, and any other relevant matters.

### **Guidelines for compliance notices**

Under the Privacy Act 2020, the Privacy Commissioner will be able to direct agencies to provide individuals access to their personal information. The Privacy Officer is responsible for liaising with the Privacy Commissioner and any relevant entity should a compliance notice be received.

### **Guidelines for websites**

The websites of all Te Kupenga entities must be compliant with the Privacy Act 2020. The following guideline is provided as a template to inform website visitors about their privacy rights:

- If you access our website, we may collect additional personal information about you in the form of your IP address and domain name.
- Our website uses cookies. The main purpose of cookies is to identify users and to prepare customised web pages for them. Cookies do not identify you personally, but they may link back to a database record about you. We use cookies to monitor usage of our website and to create a personal record of when you visit our website and what pages you view so that we may serve you more effectively.
- Our website may contain links to other websites or usage of third-party websites. We are not responsible for the privacy practices of linked websites and linked websites are not subject to our privacy policies and procedures. We are not responsible for risks and liabilities when engaging in any third-party websites like Facebook, Twitter or Google. Please refer to the Terms of Use on individual websites for further details.

### **Ensuring compliance**

We will not disclose private information to any individual or organisation other than for the purposes outlined in this statement, except with written consent. Reference is made to the principles of the Privacy Act 2020 whenever questions concerning confidentiality or privacy arise.

Te Kupenga's Privacy Officer is expected to have read the Privacy Act 2020, be familiar with it, and ensure that Te Kupenga is following its principles. This includes ensuring that Te Kupenga staff members understand the privacy statement and its requirements.

### **Review and approval**

The Privacy Statement is subject to the normal three-yearly review. Review and approval is the responsibility of the Governance Board.

Issued: 4 December 2020

Reviewed: October 2023

Next review date: October 2026