All children can be capable and free-thinking contributors in their world when offered a voice and choice in learning.

ENKINDLE VILLAGE SCHOOL

INFORMATION MANAGEMENT PROCEDURES

Statement

Enkindle Village School is committed to ensuring that complete and accurate records are created, managed, stored and disposed of in accordance with legislative and agreed organisational requirements.

Purpose

This document outlines the procedures undertaken at this school to manage information. Enkindle Village School is committed to establishing, maintaining and continually improving its records management practices, processes and culture, and strives to establish a compliant, effective and efficient records management program led by the Executive Committee.

Status: Version 2	**Supersedes:** Version 1
Authorised by: Board Chair	**Date of Authorisation:** July 2025

Documentation/Reference

- Enkindle Information Management Policy

Review Date: Annually	**Next Review Date:** July 2026
Policy Owner: Townsville Independent School Association Inc.	

Procedures

Based on the principles from the Information Management Policy:

1. Records Management must be systematic and comprehensive.
2. Records Management is everyone's responsibility.
3. Records must be full and accurate and the systems that make, manage or keep them reliable and secure.
4. Records must be retained for as long as they are required and disposed of in a lawful, planned and approved manner.

- A Privacy Officer is appointed by Enkindle Village School annually, who will be charged with reviewing privacy compliance.
- An annual review of privacy procedures will occur using the review templates.
- Enkindle Village School will provide access to an individual's personal information not withstanding exceptions as per Australian Privacy Principals. Notice to access should be in writing to the Privacy Officer or the Principal.

Student Information collection and storage

- All electronic student enrolment and application information including medical information will be kept in secure databases on SharePoint with restricted staff access. All paper-based student enrolment and application information, including medical information will be kept in a locked file cabinet in the administration office, with restricted staff access.
- Birth certificates are sighted by the Principal and date of birth entered into the student database – signed off by the Principal. Hard or electronic copied are not kept by the school after 12-months.
- Immunisation status reports are sighted by the Principal and entered into the student database. Hard or electronic copied are not kept by the school after 12-months.
- All parents are to be provided with a standard collection notice on admission.
- All parents are to receive and sign the photo and permission form.
- An annual review of the data will be completed with parents to provide any information changes to the office.

Staff Information collection and storage

- All electronic staff information will be kept in secure databases on SharePoint with restricted staff access. All

paper based staff information will be kept in a locked file cabinet in the staff office, with restricted staff access.

- All staff and volunteers or contractors are to be provided with a standard collection notice on application. See Appendix 2 and 3.
- Understanding of the Privacy Policy is to be included as part of staff induction to the school in order to uphold the standard of the policy.

Data Breach

- A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure.
- As Enkindle has obligations under the Privacy Act we are required to report certain breaches under the notifiable data breaches scheme (NDB Scheme).
- A data breach is an 'eligible data breach' (EDB) if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach.
- An adapted version of the OAIC Data Breach Response Summary (Appendix 4) setting out the steps to provide guidance for schools regarding data breach.
- The Data Breach Summary is to be followed alongside the Data Breach Risk Assessment (Appendix 6). A Data Breach Response Plan (Appendix 5) is also to be completed.

Appendices

1. **Standard Collection Notice**

I. The School collects personal information, including sensitive information about pupils and parents or guardians before and during the course of a pupil's enrolment at the school. This may be in writing or in the course of conversations. The primary purpose of collecting this information is to enable the school to provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the school.

II. Some of the information we collect is to satisfy the school's legal obligations, particularly to enable the school to discharge its duty of care.

III. Laws governing or relating to the operation of a school require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health [and Child Protection]* laws.

IV. Health information about pupils is sensitive information within the terms of the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988*. We may ask you to provide medical reports about pupils from time to time.

V. The school may disclose personal and sensitive information for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the school, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the school;
- anyone you authorise the school to disclose information to;
- and anyone to whom the school is required or authorised to disclose the information to by law, including child protection laws.

VI. Personal information collected from pupils is regularly disclosed to their parents or guardians.

VII. The school may use online or 'cloud' service providers to store personal information and to provide

services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the school's use of on online or 'cloud' service providers is contained in the school's Privacy Policy.

VIII. The school's Privacy Policy, accessible on the school's website, sets out how parents or pupils may seek access to and correction of their personal information that the school has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the school's duty of care to the pupil, or where pupils have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.

IX. The school's Privacy Policy also sets out how parents and pupils can make a complaint about a breach of the APPs and how the complaint will be handled.

X. The school may engage in fundraising activities. Information received from you may be used to make an appeal to you. [It may also be disclosed to organisations that assist in the school's fundraising activities solely for that purpose.] We will not disclose your personal information to third parties for their own marketing purposes without your consent.

XI. On occasions information such as academic and sporting achievements, pupil activities and similar news is published in School newsletters and magazines, on our intranet [and on our website]. this may include photographs and videos of pupil activities such as sporting events, school camps and school excursions. The school will obtain permissions annually from the pupil's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet.

XII. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the school and why.

2. Employment Application Collection Notice

I. In applying for this position, you will be providing Enkindle Village School with personal information. We can be contacted at PO BOX 17, James Cook Drive, James Cook University, 4814; mobile: 0428018754; or email principal@enkindleschool.qld.edu.au .

II. If you provide us with personal information, for example, your name and address OR information contained on your resume, we will collect the information in order to assess your application for employment. We may keep this information on file if your application is unsuccessful in case another position becomes available.

III. The school's Privacy Policy, accessible on the school's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the school has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.

IV. We will not disclose this information to a third party without your consent unless otherwise permitted.

V. We are required to conduct a criminal record check; collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection law. We may also collect other personal information about you in accordance with these laws.

VI. The school may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as email services. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the school's use of on online or 'cloud' service providers is contained in the school's Privacy Policy.

VII. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the school and why.

3. Contractor / Volunteer Collection Notice

I. In offering, applying or agreeing to provide services to the school, you will be providing Enkindle Village School with personal information. We can be contacted at PO BOX 17, James Cook Drive, James Cook University, 4811; mobile: 0428018754; or email principal@enkindleschool.qld.edu.au .

II. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.

III. You agree that we may store this information for two years

IV. The school's Privacy Policy, accessible on the school's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the school has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.

V. We will not disclose this information to a third party without your consent unless otherwise permitted.

VI. We are required to conduct a criminal record check; collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection law. We may also collect other personal information about you in accordance with these laws.

VII. The school may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the school's use of on online or 'cloud' service providers is contained in the school's Privacy Policy.

VIII. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the school and why.

4. Data Breach Summary

Definition of a Data Breach: A data breach involves:

- Unauthorized access or disclosure of personal information.
- Loss of personal information likely to result in unauthorized access or disclosure.

Legal Obligations:

- Enkindle is subject to the Privacy Act 1988 and must comply with the Notifiable Data Breaches (NDB) Scheme.
- A breach is considered an Eligible Data Breach (EDB) if it is likely to result in serious harm to affected individuals.

Response Framework:

1. Data Breach Summary – Adapted from the Office of the Australian Information Commissioner (OAIC) guidelines.
2. Data Breach Risk Assessment – Conducted to evaluate the severity and impact of the breach
3. Data Breach Response Plan – A formal plan to manage and mitigate the breach

Privacy Oversight:

- A Privacy Officer is appointed annually to oversee compliance.
- Annual reviews of privacy procedures are conducted using standardized templates.

Information Security Measures:

- Electronic records (student and staff) are stored securely on SharePoint with restricted access.
- Paper records are kept in locked cabinets with limited access.
- Sensitive documents like birth certificates and immunization records are sighted but not retained.

Communication and Transparency:

- Parents and staff are provided with collection notices and informed about how their data is used.
- The school's Privacy Policy outlines procedures for accessing, correcting, and complaining about personal data handling.

5. Data Breach Response Plan

This Data Breach Response Plan outlines the procedures Enkindle Village School will follow in the event of a data breach. It ensures compliance with the Privacy Act 1988 and the Notifiable Data Breaches (NDB) Scheme.

Roles and Responsibilities

- Privacy Officer: Oversees breach response, coordinates investigations, and ensures compliance.
- IT Administrator: Assists in identifying and containing breaches involving electronic systems.
- School Leadership: Communicates with affected individuals and external authorities.
- Staff: Must report suspected breaches immediately to the Privacy Officer.

Breach Identification and Containment

- Identify the nature and scope of the breach.
- Secure systems and records to prevent further unauthorized access.
- Isolate affected systems and revoke compromised credentials.
- Preserve evidence for investigation.

Risk Assessment

- Assess the type and sensitivity of the information involved.
- Determine the potential harm to affected individuals.
- Evaluate the likelihood of misuse.
- Use the Data Breach Risk Assessment template (Appendix 6) to document findings.

Notification Procedures

- Notify affected individuals if the breach is likely to result in serious harm.
- Provide details of the breach, recommended actions, and contact information.
- Notify the Office of the Australian Information Commissioner (OAIC) if required.
- Use the Data Breach Summary and Response templates (Appendices 6 and 7).

Review and Prevention Steps

- Conduct a post-breach review to identify root causes.
- Update policies and procedures to prevent recurrence.
- Provide staff training on data protection and breach response.
- Review and test the response plan annually.

6. Data Breach Risk Assessment

This risk assessment outline is designed to assist Enkindle Village School in assessing the risks associated with a data breach. It should be completed as part of the school's Data Breach Response Plan.

Breach Description

Provide a detailed description of the breach, including when and how it was discovered.

Type of Data Involved

List the types of personal or sensitive information involved (e.g., names, addresses, health records, student data).

Potential Harm

The exposed data could be used for identity theft, phishing scams, or unauthorized contact with students or their families. There is a risk of emotional distress to the affected families.

Affected Individuals

Identify the individuals or groups affected by the breach (e.g., students, parents, staff).

Likelihood of Serious Harm

Moderate to High.

Recommended Actions

Immediately contact the unintended recipient and request deletion breached data.
Notify affected families and provide support resources.
Report the breach to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches scheme.
Review and reinforce staff training on data handling and email protocols.
Implement additional safeguards such as email recipient verification tools.