RECORDKEEPING, RETENTION AND DESTRUCTION POLICY

1 INTRODUCTION

Minaret College (the **College**) must keep adequate records to contribute to meeting its legal obligations, such as meeting its duty of care to keep children safe. Recordkeeping is important because it means the College has the information it needs. Appropriate recordkeeping also contributes to protecting the privacy of individuals.

The College must delete, destroy or de-identify Information once it is no longer needed, unless it is required to keep documents for set periods of time as set out in this Policy. The retention periods in the Schedule to this Policy are the minimum retention periods required by the College This means documents must be retained for this period of time.

Information must be destroyed when the retention period ends.

2 PURPOSE AND SCOPE

The purpose of this Policy is to set expectations around how Staff create and maintain records, and to facilitate the compliant and effective archiving and destruction of Information which minimises administrative burden and ensures the College meets the Public Record Office Victoria Recordkeeping Standards.

This Policy applies to all Information held by the College and all Staff.

This Policy applies to digital and hard copy records.

3 RECORDKEEPING OBLIGATIONS

3.1 CHILD SAFETY

The College creates, maintains and disposes of records relevant to child safety and wellbeing to ensure the College can identify risks, implement risk controls and risk treatments and ensure child safety is embedded in the College's culture. This includes child safety risk assessments and child safety policies and procedures.

3.2 CHILD ABUSE COMPLAINTS, CONCERNS, ALLEGATIONS AND INVESTIGATIONS

The College must ensure full and accurate records are created to document all aspects of allegations and investigations about incidents, complaints and allegations of child abuse. This includes the child safety risk register and internal reporting. Records about allegations and incidents of child abuse must:

document how the incident or allegation was investigated, responded to and managed. This includes places, times, dates, names of people, observed behaviours or evidence of risks and document conversations and actions; and

a) be detailed, objective and include contextual and supporting information;

b) be retained **securely** and **permanently**.

3.3 RECORDS IN CASE OF FUTURE ALLEGATIONS

The College creates and maintains records which may be relevant to future allegations, such as records about overnight stays and homestays that involve students, even where no child safety allegation or concern has arisen. This is because allegations may be made many years after an incident and overnight stays involve a higher risk of child sexual abuse.

The Schedule of Retention Periods include details about what documents and Information is retained under this category.

4 SECURITY OF RECORDS

The College needs to keep its records secure to ensure the College:

a) has access relevant records in the event of future allegations of child abuse; and
b) protects individuals' privacy, the confidentiality of Information about Operational Matters and the integrity of all records.

Security measures need to be appropriate according to the sensitivity of Information. This means, to decide what is appropriate security, Staff should consider what could go wrong if that Information was lost or stolen. The more serious the consequences, the stronger the security measures need to be.

- High Risk (e.g. identity theft, fraud, child safety risks) = stronger security measures
- Lower Risk = less security measures required

To securely store digital records, the College must ensure the records:

a) when stored or hosted by a contractor or third-party, remain in the custody and control of the College;
b) are in formats that are readable using suitable technologies; and
c) are protected from outages to power which could cause data to be lost, and there are adequate backups and restorations arrangements.

To securely store physical devices which store digital records (servers, hard drives), and physical records, the College must store the devices in appropriate locations protected from environmental conditions, such as fire, mould, pests and dust.

5 QUALITY OF RECORDS

It is important the College's records are of a high quality. This means records need to be accurate, up-to-date and complete.

For records to be complete, Staff should consider WHO, WHAT, WHEN, WHY, HOW.

Opinions: Opinions can be included in records. When opinions are included in records, Staff need to clearly identify what is an opinion, what was observed, and what they were told by someone else.

Use the exact words: When a record is recording a disclosure of child abuse, or another risk in the College environment, Staff should try, as much as possible, to record the exact words used by the person making the disclosure.

Documenting conversations: Staff should document conversations or verbal exchanges (such as a meeting with parents) to ensure there is a record of what was said and agreed. This is particularly important when conversations are about a student's behaviour, discipline or reasonable adjustments.

6 RETENTION

The Schedule specifies the timeframes for which Information must be retained (**Retention Period**). Staff must not destroy Information prior to the Retention Period in the Schedule ending. These Retention Periods are based on business needs, child safety requirements and other laws such as the Ministerial Order 1359.

It is not permitted to scan records and destroy originals.

Exception: Information may be retained after the Retention Period ends when there is an ongoing organisational need to keep the Information, for example, there could be possible legal proceeding for which the document or Information is relevant.

1) If a Staff member thinks there is an ongoing organisational need to keep Information beyond a Retention Period, they must seek approval from the Executive Principal to keep that Information.
2) Once there is approval, the Information should be retained with a record of why it was retained beyond the Retention Period. This explains to other Staff why it was retained and can assist with understanding when the Information can later be destroyed.
3) Appropriate security measures should be considered regarding this Information.

7 DESTROYING INFORMATION

Information must be destroyed when:

a) the Retention Period ends;
b) it is no longer needed;
c) the Information is not the subject of pending litigation or a disposal freeze; and
d) for Information that is not Routine Matters, internal authorisation has been obtained.

It is the responsibility of Executive Principal to ensure ongoing, regular and systematic destruction of Information according to the Schedule of Retention Periods. This includes assessing when Information needs to be destroyed, which method of destruction is appropriate, and documenting destruction when required in the Information Destruction Register.

Requirements for destruction are different for Routine Matters.

Routine Matters	All other Information types
Routine Matters can be destroyed without internal authorisation.	All other Information types require internal authorisation noted in the Information Destruction Register.
Destruction does not need to be documented.	Destruction must be documented in the Information Destruction Register at the end of this Policy.

When it is time to destroy Information (when a Retention Period in the Schedule has ended), Staff must consider the appropriate method of destruction. This will depend on the format and type of record. See the below table:

Type	What destruction should look like
Hard copy records (paper)	Shredding documents prior to disposing of them in a garbage bin.
Hardware no longer needed such as hard drives, laptops or computers	Health Information and Personal Information is erased or deleted (including from the Deleted folder) prior to permanently disposing of these physical hardware items. This is called 'sanitising' hardware.
Information given to third-party providers such as a contracted camp provider (for example, Student Records, Health Information, Employment Information)	Take steps to verify the third-party provider has destroyed the Information. Example: include destruction requirements in your agreement, and check with the contractor to ensure this contractual obligation is met.

Information stored digitally (held in an electronic format)	Irretrievably delete Information (and delete from the digital waste bin) OR Put Information 'beyond use' by surrounding the Information with technical and physical security measures (access controls, access logs and audit trails) so no one can access or disclose the Information.
CDs and DVDs	Physically destroyed by cutting or crushing.
Film	Shredding, cutting, crushing.

7.1 WHAT IS 'BEYOND USE'?

Information is **beyond use** when it is no longer accessible or useable due to additional security and control measures. Putting Information beyond use instead of making it irretrievable is relevant for digital records where technical limitations apply.

7.2 WHY IS DESTROYING INFORMATION IMPORTANT?

Destroying information in a timely manner is important to:

a) reduce the risk of the Information being released inappropriately (data breaches);

b) minimise storage costs and administrative overheads; and

c) comply with privacy requirements.

8 DEFINITIONS

Information includes all the categories of information set out in the table below, such as Financial Information, Health Information, Personal Information, Routine Matters and Operational Matters.

This table sets out the different types of Information referred to in this Policy.	
Child Safety Information	**Child Safety Information** means information about protecting children from child abuse, managing the risk of child abuse, providing support to a child at risk of child abuse, and responding to suspicions, incidents, disclosures and allegations of child abuse. Examples: Child Safety Risk Register, investigations into allegations of reportable conduct, records of training provided to staff about child safety. See the Schedule for more detail.

Employment Information	**Employment Information** means information about Staff. Examples: contracts of employment, information about training, discipline and professional development, information about any accidents, complaints or insurance claims in relation to a Staff member.
Financial Information	**Financial Information** means all information held by the College in relation to financial matters, including salaries, payroll matters, commercial contracts, budgets and projections.
Health Information	**Health Information** means information or an opinion about— (a) the physical, mental or psychological health (at any time) of an individual; or (b) a disability (at any time) of an individual; or (c) an individual's expressed wishes about the future provision of health services to him or her; or (d) a health service provided, or to be provided, to an individual— that is also Personal Information. Examples: injuries, illnesses, disabilities, reasonable adjustments, mental health plans, individual learning plans.
Personal Information	**Personal Information** means any information about a reasonably identifiable individual Member, including sensitive information about that individual Member. It may be an opinion, whether true or not, and it does not need to be in material form. Verbal or pictorial information is also personal information. Examples: name, contact details, address. Student Records, Health Information and Employment Information are types of Personal Information.
Routine Matters	**Routine Matters** means material of a facilitative nature created, acquired or collected by Staff while performing their duties, but does not include Information which is captured by any other category. It includes: (a) drafts of documents which has been reproduced and incorporated in the College's record keeping system; (b) working papers consisting of rough notes and calculations used only as a means to assist in the preparation of other records such as correspondence, reports and statistical tabulations; and/or (c) additional copies of materials such as documents, emails, videos, photographs and publications preserved solely for reference purposes. As a general rule, no more than 3 – 5 copies of any materials need to be kept. This can apply to records duplicated across multiple archives.

Student Records	**Student Records** means Information about students that is not Child Safety Information. Student Records will also be Personal Information.
Operational Matters	**Operational Matters** means matters concerning the operations and governance of the College. Examples: Board agendas, minutes and resolutions.

Retention Period is the time frame for which a record must be retained, listed in the Schedule.

Staff means an individual working in the College environment as an employee, a contracted service provider or a minister of religion, religious leader or employee of a religious body associated with the College, and specifically includes a Volunteer.

Volunteer means a person who performs work without remuneration or reward for the College in the College environment.

9 BREACH

Staff must follow this Policy. Breach of this Policy can result in disciplinary action.

10 RELATED POLICIES, LEGISLATION AND STANDARDS AND PROCEDURES

- Minaret College Privacy Policy
- Public Records Office Victoria Guide to Creating, Managing and Retaining Records of Child Sexual Abuse Allegations
- PROS 19/05 Create, Capture and Control Standard
- PROS 19/08 Organisational Response to Child Sexual Abuse Incidents and Allegations RDA
- PROS 10/13 Destruction Guideline
- PROS 10/13 Disposal Standard
- PROS 20/02 Storage Standard

DOCUMENT CONTROL

Doc ID: POL-ADM-04
Version 1.0
Reviewed: June 2022
Review Cycle: Annual
Approved: June 2022

Appendix: Schedule of Retention Periods

Interpretation note: Where a document is captured by multiple categories, retain the document, information or record for the longest Retention Period.

Type of Information	Destroy after
Child Safety Information – Retention Periods are required by the Ministerial Order 1359.	
Information relating to child safety policy, strategy and procedures. This includes Board papers and minutes.	Do not destroy. Retain permanently. PROS 19/08.
Records of complaints, concerns, allegations and investigations relating to child abuse and the response to the College. This includes Reportable Conduct, mandatory reporting, and internally reported child safety concerns and/or breaches of the Child Safety Code of Conduct. Includes Child Safety Risk Register and disclosures, complaints and reports made by students.	Do not destroy. Retain permanently. MO1359 clause 11.3.
Information relating to training and development on child safety by the College.	Destroy after 45 years. PROS 19/08.
Risk-based Retention Periods in relation to potential future child abuse claims, taking into account PROV and CAARA principles relating to high risk activities	
Records relating to **overnight stays or homestay** involving children (in case of future allegations) including: - personnel and work placement records, including working with children checks; and - rosters, attendance sheets, absence records or organisational charts that would assist in determining whereabouts of an alleged abuser. Example: which adults went on which overnight stays with which students.	Do not destroy. Retain permanently.
Other documents that might support a future allegation of child safety or wellbeing allegations; - incursions where contractors come onto the College premises; - medical reports or other records received from medical practitioners, health	Destroy 7 years after event.

professionals, teachers, counsellors and other such third parties - names and periods of engagement of any contractors (out of hours care programs, maintenance, cleaning services).	
Attendance of students at the College and out of hours care programs associated with the College.	Do not destroy. Retain permanently.
The below Retention Periods are a guide and can be adjusted by the College depending on risk assessments and privacy impact assessments.	
Student Records	Refer to the Australian Society of Archivists - Records Retention & Disposal Schedule for Non-Government Schools for Student Records. However, follow this Policy where there is any conflict between this Policy and the Archivist Guide.
Employment Information	
Work Health and Safety incident reports, Accident reports and Worker's Compensation records	Destroy 75 years after birth of a Staff member.
Summary information about Staff, including: - reference checks, qualifications, evidence of registration; - position description; - application and contract; and - employment or engagement history (dates of when the Staff member worked at the College and leave requests). - rosters, attendance sheets and permission slips; - who attended which off-site visits, day-trips and excursions.	Do not destroy. Retain permanently.
Negotiation and implementation of enterprise agreements	Do not destroy. Retain permanently.
All other Employment Information. Does not include any Child Safety Information.	Destroy 7 years after employment or engagement relationship with the College ends.

Financial Information	
Salaries, payroll matters, commercial contracts, budgets and projections. Does not include Operational Information covered below.	Destroy 7 years after creation. However, some financial information (i.e., certified business plans) will be captured by Operational Information below and required to be retained permanently.
Operational Information	
Delegations and authorisations	Destroy 7 years after delegation expires.
Formal documentation of establishment, ongoing governance and registration and closure of the College. Includes: - certificate of Incorporation; - strategic planning documentation; - consultation; - legal documents; - registration documentation; - compliance monitoring; - VRQA Audits; - policies and procedures; - information about the Board and committees, including minutes of Board meetings and Board papers; - legal or financial advice on major issues; - major litigation matters; - annual financial reports; and - acquisition of land and construction activity.	Do not destroy. Retain permanently.
Routine matters	
- Accounting records and income and expenditure, grants, payroll, debt recovery - Asset valuations - Documents used to compile annual reports - Funding applications - Setting of fees and charges	Destroy after 7 years.
Taxation matters, land tax, payroll tax, payment of tax	Destroy after 5 years.
Refurbishment and maintenance of College premises and property	Destroy after 7 years.