Information Management Policy

1. Purpose

1.1   This policy provides a framework for the creation and management of information.

2. Scope

2.1   This policy applies to all staff of Perth Bible College.

3. Responsibility

3.1   It is the responsibility of the Principal for the implementation of this policy.

4. Definitions

Disposal	The process by which records are either destroyed or retained permanently. Disposal includes a range of processes associated with implementing the information management policy.
Information	Any collection of data that is processed, analysed, interpreted, organised or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form.
Record	Any form of recorded information received or created, that is of historical significance to the College, or which provides evidence of the decisions and actions made by Perth Bible College. College records may be in any form including, paper, electronic, audio, video, data within business systems, photographs, etc.

5. Policy Provisions

Principles

5.1   This policy describes methods of control for ensuring integrity and protection of Perth Bible College's information, records and data.

5.2   Perth Bible College recognises that it has legislative, regulatory and social obligations to keep certain records and protect information to:

5.2.1   maintain accurate and up-to-date records of enrolments, progression, completions and award of qualifications;

      5.2.2   prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity;

      5.2.3   document and record responses to formal complaints, allegations of misconduct, breaches of academic or research integrity and critical incidents; and

      5.2.4   demonstrate compliance with the Higher Education Standards Framework.

5.3   Perth Bible College's primary recordkeeping systems are:

      5.3.1   Student Management System -Student Internet Console;
      5.3.2   Paradigm;
      5.3.3   Induct;
      5.3.4   PRISMS;
      5.3.5   HEPCAT;
      5.3.6   HEIMS Online;
      5.3.7   Burst SMS System;
      5.3.8   Reckon Accounts Premier (non-profits);
      5.3.9   QILT Data;
      5.3.10   Moodle;
      5.3.11   Koha;
      5.3.12   Zoho; and
      5.3.13   Hardcopies on student files

5.4   This policy applies to information created and received by Perth Bible College.

5.5   This policy applies to hard copy records, soft copy records and databases.

Creation of Records

5.6   Perth Bible College ensures that records are created to document its business and are captured in recordkeeping systems.

5.7   Records must accurately reflect the activities they document and include adequate information for them to be meaningful, such as the identity of staff and the date of activity.

5.8   Records should be captured into a recordkeeping system as soon as possible after creation so that evidence is readily available to support College business.

5.9   College records created or received by email or electronic documents held on personal computers must be incorporated into a recordkeeping system.

5.10   Significant oral decisions and commitments should be recorded and incorporated into a recordkeeping system.

Security of Records

5.11   Perth Bible College is committed to ensuring that information is kept secure and all confidential information is safeguarded.

5.12   All hardcopy records are kept in a secure location.

5.13   Records held in electronic form are backed up on a regular basis and migrated to new systems when necessary so that they remain useable for as long as they are needed.

Privacy and Confidentiality

5.14   Access to personal information is provided, subject to the privacy principles in the Privacy Act 1988 and the access provisions of the Freedom of Information Act 1982.

5.15   Information about students and staff is confidential information and is not disclosed to any third party. Students are made aware that Perth Bible College will not allow access to their personal information without their written consent being obtained.

5.16   When enrolling, students sign a confidentiality waiver to allow government authorities to access their academic and personal details on demand.

5.17   Staff members and students both have the right of access to their own personal file.

5.18   Students are required to contact the College Administrator if they seek access to their personal file and staff members should contact the Principal.

5.19   Students may allow third party access to their personal file by providing written permission to the College Administrator outlining the nature of information that may be accessed.

Archiving Records

5.20   Every student file is retained in a numbered archive box for a period of five years after the student ceases to be a student.

5.21   An application to the College that has been declined will be securely kept for two years.

5.22   An application that is partially complete, so not fulfilling the requirements to be considered an application, will be securely kept for a minimum of six months.

5.23 The period of active life for each hard-copy document is stipulated by the relevant document owner. Records are retained by the document owner, before being transferred for archiving in secure storage.

Destruction of Records

5.24 Records must be destroyed by industrial disposal only at the end of that period of time at the direction of the document "owner".

5.25 Student records may be destroyed after seven years, but not before two years after the student leaves the College.

5.26 Staff records are destroyed seven years after employment has ceased.

5.27 Declined applications and records associated with them will be destroyed after two years.

5.28 Incomplete or partially completed applications and records associated with them will be destroyed after six months.

6. Policy Information

Date first approved: 23/09/2019	Date of effect: 01/12/2019	Date last amended: 19/10/2021	Date of next review: 19/10/2023
Approved by		Board of Management	
Authorised Officer		Principal	
Supporting documents, procedures & forms of this policy		*Information Management Procedure*	
Related Legislation and Codes of Practice		*Higher Education Standards Framework 2015, Part A: Standard 7.3 (Information Management) (Wellbeing and Safety)* *Privacy Act 1988* *Freedom of Information Act 1982* *Tertiary Education Quality and Standards Agency (TEQSA) Act 2011*	
Audience		Staff	

7. Version History

Review Table			
Date	**Review Type** - Scheduled - Policy amendment - Admin update	**Summary of Changes**	**Review person/group**
12/07/2019	Policy amendment	New template and amendments made	Natalie Tierney Capital Review Group consultant

17/08/2021	Policy amendment	ss. 5.23 amended to be in alignment with legislation.	Chris Burton
19/10/2021	Policy amendment	Addition of ss. 5.21, 5.22, 5.27 and 5.28	Chris Burton