PROCEDURE C.32.-P32.1

Information Management

1.0 INTRODUCTION

1.1 Related Policy

Information Management

1.2 Purpose

This procedure provides for the operationalisation of the information management policy which supports the functions and activities of the Scentia Group.

1.3 Scope

The information management policy includes:

- creation and management
- storage and integrity
- retention and disposal and
- risk and business continuity.

This policy applies to all Scentia staff including AIM, ABS and ACHW staff, temporary employees, contractors, visitors and third parties globally who manage Scentia information.

This policy applies to all business systems, services or applications used to create, manage, and store information, including Scentia endorsed information and records management systems, cloud services and email systems, internal and external websites, social media applications, collaboration applications and databases.

This policy does not override any legal, regulatory, or statutory requirements that Scentia is bound to comply with.

1.4 Scope Exceptions

None

2.0 RESPONSIBILITIES

1. All those referred to under the Scope of this policy are responsible for complying with its terms and procedure.

2. The Chief Financial Officer is responsible for ensuring Scentia retains all records required under the Corporations Act 2001. This includes retaining financial records for at least seven years.

3. The Head of Human Resources is responsible for ensuring that Scentia meets the Fair Work Act 2009 and Fair Work Regulations 2009 for information and records management of staff including employment and payroll (seven years) and superannuation records (five years).

4. Contract Owners of Managed Service Providers responsible for the approval of the procurement of IT managed services must ensure that suitable contract provisions require the provider to comply with the provisions of this policy. Contract owners must ensure compliance by the provider throughout the contract term.

5. Executive Directors of AIM, ABS and ACHW are responsible for ensuring staff comply with Scentia information and record keeping requirements and relevant legislation and standards.

6. All staff are responsible for complying with this policy.

7. The Data and Information Security Committee is responsible for the review of this Policy and Procedure in consultation with the Head of Technology.

8. The Head of Technology has overall responsibility for:

    a. the implementation of this Policy and Procedure; and
    b. providing information management facilities as required for Scentia.

3.0 PROCEDURE

3.1 Creation and Management of Records

1. All Information Owners must:

    a. assess, document and review Scentia records that will be created and captured as part of the processes that they are responsible for, and determine how long these records need to be kept to meet the requirements of the Scentia Information Management policy;

    b. ensure that the records they are responsible for are reliable, accurate, usable, stored and appropriately protected within the Scentia Approved Information System (Shared Drives) or a compliant secure storage area (for physical records) if required;

    c. comply with the *Privacy of Student Information and Records* and *Privacy of Staff Information and Records* policies

    d. ensure that email folders, share drives, personal drives, external storage media or unsupported cloud-based storage services (e.g. drop-box) are not used to store Scentia records as they lack the necessary record-keeping functionality to protect the records. Scentia records held in these systems must be incorporated into Scentia's Approved Information System to prevent them from being inaccessible, lost, leaked, prematurely deleted or over-retained. Records with a

high or medium risk rating must be stored in Scentia's Approved Records Management System;

e. ensure that documents are created and managed using approved Scentia templates, file naming conventions and version control requirements;

f. ensure that official records, including records of Scentia Board Committee and sub-committee meetings, that will be share or distributed to external bodies, agencies or parties have been reviewed and endorsed by relevant managers and in accordance with governance and delegation requirements where required;

Records storage and integrity

1. All digital records are stored securely and managed digitally in Scentia's Learning Management Systems, Customer Relationship Management System, Student Information and Records Management Systems, Finance, HR and marketing systems, and approved Scentia Share Drives.

2. All digital records are protected by unique login, secure password access and multifactor authentication.

3. Records are further protected by maintaining up to date virus, firewall and spyware protection software.

4. Scentia is committed to maintaining and safeguarding the accuracy, integrity, confidentiality of student records. They are protected against theft, fire, flood, vermin or any other pests. (Refer to the *Scentia Business Continuity Plan*)

5. Digitally stored records are maintained off site and backed up on a regular basis.

6. Scentia collects personal information of students for education purposes and creates and maintains records related to enrolment, progress, communications and certification in accordance with relevant legislation and standards. For additional information on student records, refer to the *Privacy of Students Information Policy*.

7. Scentia Group collects, manages, uses, discloses, protects, and disposes of the personal information of staff, in accordance with the Privacy Act 1988 and keeps records as required under the Fair Work Act 2009, Section 535.

Records Retention and Disposal

1. Records are stored digitally on Scentia's systems and approved partner systems and are permanently deleted as required dates for retention have passed.

2. Retention periods for Scentia records are set by relevant legislation and standards including: The Corporations Act (section 286), Fair Work Act 2009, Fair Work Regulations 2009, the National VET Regulator Act 2011, the Higher Education Act 2001 and where relevant the NSW State Archives and Records Retention and Disposal Authorities, legislated under the State Records Act 1998 (NSW).

3. Destruction of Scentia Records prior to completion of the minimum retention period is prohibited under the State Records Act 1998 (NSW) and relevant Commonwealth legislation including the Corporations Act 2001 and the Fair Work Act 2009, which also prescribes penalties and exceptions for early destruction.

4. Records or documents having limited or incidental relevance can be destroyed in accordance with normal administrative practice by document owners. Use of security bins is provided for this purpose for paper records.

5. Destruction of Scentia records must be authorised, secure, timely and documented to minimise risks associated with records being accessible beyond their requirements.

6. Destruction of paper-based records after they have been scanned/digitised is acceptable providing the conditions outlined in the NSW state records disposal authority GA45 are met, where relevant, and the digital outputs are stored in a Scentia Approved Information System.

7. The Chief Executive Officer has sub-delegated the authority for approving the destruction of records and information (refer to the Delegations Manual). The destruction authorisation process is managed by the Data and Information Security Committee.

Risk and Business Continuity

1. Scentia will ensure its Business Continuity Plans for critical processes identify the risks to high risk records and high value records, and will implement processes to monitor and manage these risks in line with Scentia's *Business Continuity Plan* and *Risk Management Policy*. This includes, but is not limited to, appropriate back-ups and disaster recovery strategies.

2. Information Owners must determine the level of risk associated with the records that they are responsible for and apply a risk-based approach when considering the best way to manage and store records.

3. High risk records and high value records must have more rigorous records management processes applied, whereas low risk and low value records have more flexibility in their record management provided that key recordkeeping and privacy obligations are met.

4. Staff must plan and facilitate the transition of records to the most appropriate person or business unit to minimise disruption of operations and loss of information prior to a staff member leaving Scentia, moving divisions, business units, or premises; or when there is a restructure.

4.0 DEFINITIONS

- **Approved Information Systems -** Refers to systems Scentia uses to manage business operations, and store and manage information and data as part of its business and to meet legislative requirements. These include: Learning Management (myAIM, myABS and myACHW), Customer Relationship Management, Student Information and Records Management, Finance and HR systems and marketing data.
- **Approved Records Management System -** Scentia supports Share Drives for the storage of approved records and cloud storage services for staff working documents.
- **Asset** – means any tangible or intangible item that Scentia owns, or has legal or other right to control and exploit to obtain financial or other economic benefit.

- **Authorised User** – means a person who has been provided with credentials to access Scentia ICT Asset /s or Information Asset.
- **ICT Services**– Any information, communications technology or audio-visual service, equipment or facility owned leased or contracted by the Scentia group that hosts, stores, transmits or presents digital information for the business and purpose of Scentia. This may include, but is not limited to:

  - email, messaging and collaboration applications;
  - any cloud-based facilities associated with the delivery of ICT activities;
  - all hardware and infrastructure (e.g. servers, workstations, voice and
  - data network, wired and wireless networks, audio visual equipment,
  - printers, and portable storage devices);
  - videoconferencing and web conferencing systems, services
  - applications; and
  - all software and applications, and services (including but not limited to internet access), and data contained or stored in any ICT facility.
  - Learning Management Systems (my AIM, myABS, myACHW)

- **Information Asset** – means a body of information, knowledge or data that has value to Scentia.
- **Information, data, records**– Any digital or paper information, digital or paper stored, transmitted or presented for the business and purpose of Scentia.
- **myAIM –** Learning Management System for students enrolled in the Australian Institute of Management Education and Training (AIM) Registered Training Organisation (RTO) offering vocational education and training (VET) courses.
- **myABS** - Learning Management System for students enrolled in the Australian Institute of Management Business School, a registered Higher Education provider.
- **myACHW** - Learning Management System for students enrolled in the Australasian College of Health & Wellness, a registered Higher Education provider.

5.0 REFERENCES AND ASSOCIATED INFORMATION

- Code of Conduct Policy (Staff and Students)
- Privacy of Staff Information and Records
- Privacy of Student Information and Records
- Scentia Risk Management Policy
- Scentia Business Continuity Plan 2021
- Scentia Information and Cyber Security
- Social Media Policy (Staff and Students)
- Staff Use of ICT Facilities Policy and Procedure
- Student Use of ICT Services Policy and Procedure

- Corporations Act 2001(Section 286)
- Copyright Act 1968 (Cth Australia)
- Education Services for Overseas Student Act 2000 (ESOS Act)
- Fair Work Act 2009
- Fair work Regulations 2009
- General Retention and Disposal Authorities (GDAs) GA-45- Original or source records that have been copied; GA-47-General retention and disposal authority: higher and further education

- Higher Education Standards Framework (Threshold Standards 2021 (HES Framework)
- National Code of Practice for Providers of Education and Training to Overseas Students (National Code 2018)
- National VET Regulator Act 2011
- Privacy and Personal Information Protection Act (PIIPA) 1998 No 133
- Standards for Registered Training Organisations (RTOs) 2015
- State and Records Authority NSW
- Telecommunications (Interception and Access) Act 1979 (Cth Australia)
- Tertiary Education and Quality Standards Act 2011
- VET Quality Framework
- NSW State Records Act 1998
- ISO/IEC 27001:2013 – Information Security Management System

6.0 POLICY/PROCEDURE OWNERSHIP

Policy Owner	Head of Technology
Status	New
Approval Authority	Scentia Corporate Board with endorsement of the ABS Corporate Board and ACHW Corporate Board.
Date of Approval	26/04/2023
Effective Date	01/05/2023
Implementation Owner	Head of Technology
Maintenance Owner	Head of Compliance
Review Due	1 March 2026
Content Enquiries	Mike Kumar – Head Technology

7.0 AMENDMENTS

Version	Amendment Approval (Date)	Amendment Made By (Position)	Amendment Details
C.32-P32	26 April 2023	Head of Technology	New Procedure
C.32-P32.1	3 April 2024	Head of Compliance	Factual correction to the retention duration of HE records

ANNEXURE: SCENTIA RECORD RETENTION REQUIREMENTS

	Record	Retention requirement	Legislation/Standard
Corporate			
1	Financial records	Seven (7) years	Corporations Act 2001
2	Employment and payroll	Seven (7) years	Fair Work Act 2009 and Fair Work Regulations 2009
3	Superannuation records	Five (5) years	Fair Work Act 2009 and Fair Work Regulations 2009
4	i. Legal records (documents such as bills of sale, permits, licenses, contracts, deeds and titles, mortgages, and stock and bond records ii. Cancelled leases and notes receivable	i. Indefinitely ii. 10 years after cancellation	
VET			
1	Records of qualifications and Statements of Attainment issued	30 years	Clauses 3.1-3.4 (RTO Standards)
2	All completed student assessment items	At least six months from the date on which the judgment of competence for the student was made.	Clause 1.8 (RTO Standards)
3	Assessment validation	Five (5) years	Clause 1.10 (RTO Standards)
Higher Education			
1	Admission, Enrolment and Completions	30 years	Threshold Standards State Records Act 1998 (NSW)
2	Results records i. Records (including marking rubrics) relating to the grading/marking of individual assessment components of a subject or course and determination of final results/grades ii. Records relating to changes of assessment results	i. Minimum of 1 year after action completed. ii. Minimum of 1 year after action completed, then destroy.	Threshold Standards State Records Act 1998(NSW)
2	Graduation Testamurs, Transcripts	30 years	Threshold Standards