Rhodes Business School

POLICY

Policy Name:	Information Management
Document Number:	AR 3.1.01
Approved by:	CEO
Last Approval Date:	April 2022
Review Date:	April 2024
Audience:	NIET Group (Rhodes Business School) Staff, Students and Community
Contact Officer:	ICT Manager
Related Documents:	Privacy Policy; Cyber Security Policy; Higher Education and VET Archiving Management Records Retention and Disposal Schedules ;
Legislation:	Public Records Act 2002 (Qld); Right to Information Act 2009 (Qld); Electronic Transactions Act 2001 (Qld); Telecommunications (Interception and Access) Act 1979 (Cth.) VSL Loan Act 2016; VSL Student Loan Rules 2016

1. Purpose and Objective

Rhodes Business School is committed to appropriately managing all forms of information that it creates and holds. Effective information management ensures that the right information is available to the right person, in the right format and medium, at the right time. Information that enables Rhodes Business School to perform its core functions is considered an asset.

This policy outlines roles, responsibilities, expectations and requirements for managing information at Rhodes Business School and is intended to enable Rhodes Business School to:

- improve the integration and accuracy of its information,
- improve its compliance and reduce risks associated with potential loss or misuse of information,
- make better use of information in its decision-making processes,
- provide a strong foundation for systematically managing its information assets, ensuring that information of strategic importance and high value is prioritised, and
- obtain valuable knowledge through the increased discoverability and accessibility of its information.

2. Policy Scope/Coverage

The scope of this policy covers all information in any format (physical, electronic or hybrid) that is created, collected, managed, stored and disseminated by Rhodes Business School to perform its business functions and deliver its services.

This policy applies to consumers of Rhodes Business School information and communications technology (ICT) resources and anyone creating or accessing Rhodes Business School's information assets, including but not limited to:

- Students
- Staff

- Contractors and consultants
- Visitors
- Affiliates and third parties

Consumers that are connected to Rhodes Business School networks, systems or services must comply with this policy, irrespective of location or device ownership (e.g., consumers with personally owned computers). Exceptions to this policy must be approved by the Chief Executive Officer.

3. Definitions

Data - There is a subtle difference between data and information. Raw data is a term used to describe data in its most basic digital format. Data is raw, individual facts that need to be processed. When data is processed, combined with other data, organised, structured or presented in a given context, it is referred to as information.

Information – Includes, but is not limited to, physical (e.g. paper records) or digital files (e.g. email, voicemail, meeting minutes, video and audio recordings) in any format (e.g. PDF, .wav, .docx, or .jpeg) and data recorded by University applications (often in a database of some form).

Information Asset - A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information domain – A broad category or theme under which School information can be identified and managed.

Information Standards - Define and promote best practice in the acquisition, development, management, support and use of information systems and technology infrastructure which support the business processes and service delivery of Queensland public authorities.

Record - Information in any format that has been generated or received by Rhodes Business School in the course of its activities, and which must be retained by Rhodes Business School as evidence of its actions and decisions. A record can consist of one or more pieces of information that together form a record or context of the activity, action or event.

Retention and Disposal Schedules – Legally binding documents that have been authorised by Queensland State Archives, the authority on records governance for public entities such as Rhodes Business School. They define the status, minimum retention periods and consequent disposal actions authorised for specific classes of records.

4. Policy

4.1 PRINCIPLES AND KEY REQUIREMENTS

Robust and effective information management at Rhodes Business School:

- provides for the creation, use and sharing of information in compliance with legislative requirements and mandatory standards,
- helps to ensure that the right information is available to the right person, in the right format, at the right time, and

- is fundamental to Rhodes Business School's functions and operations.

The principles and requirements in this policy are related and intended to be applied by consumers as a whole where possible.

4.2 INFORMATION IS TREATED AS AN ASSET

Information management supports evidence of Rhodes Business School decisions and activities, enables accountability and transparency, mitigates risk, and allows businesses to operate. To achieve this, Rhodes Business School ICT consumers must apply the following measures to their information management practices:

- All Rhodes Business School information assets must be clearly identified and classified.
- Maintain adequate information and records and capture this information in digital or physical management systems capable of meeting requirements of this policy and associated procedure.
- Classify all Rhodes Business School information assets.
- Manage information throughout the information lifecycle (Create, Store, Use, Share, Archive, and Dispose) in accordance with the Information Management procedure.
- Information with historic, permanent or long-term value will be archived or preserved, and not destroyed.
- Information that is of high risk or high value will be maintained and must not be destroyed without proper authorisation.

Consumers should seek to ensure digital information and records remain digital and will not be converted to a physical format unless required (the 'born digital, stay digital' principle).

Rhodes Business School will maintain facilities to enable efficient cataloguing, long term maintenance and discovery of information assets.

4.3 INFORMATION CAN BE FOUND AND ACCESSED

Rhodes Business School facilitates the creation of large volumes of information. Rhodes Business School consumers and members of the public should have access to relevant and appropriate Rhodes Business School information where necessary. To achieve this:

- Non-confidential information about Rhodes Business School will be available to the public.
- Rhodes Business School will maintain procedures for responding to requests for information from the public.
- Rhodes Business School staff will have timely access to information required to undertake their official duties.
- Rhodes Business School staff, students, contractors, consultants, visitors, affiliates and third parties who have access to Rhodes Business School networks and services will not provide or share Rhodes Business School records or information which are not in the public domain with unauthorised parties.

4.4 INFORMATION IS SUITABLE FOR ALL OF ITS USES

The quality (completeness, consistency and accuracy) of information must support Rhodes Business School's strategic objectives of academic and research excellence. To achieve this, Rhodes Business School ICT consumers should apply the following information management practices:

- Administrative records should be created as soon as possible to document an event, decision or action.
- The quality of information should be ensured at the point of collection and the information stored in a suitable location in an appropriate information management system. Rhodes Business School will establish and maintain procedures for ensuring information quality.
- Information recorded and captured should consider the primary purpose for which it is collected or created and its potential secondary uses. High quality information management should take into account potential future re-use of the information, which may not be known at the initial point of capture.

4.5 INFORMATION REMAINS COMPLIANT

To strengthen its information and records management practices, Rhodes Business School will:

- Comply with records and information management requirements in laws, regulations, contracts and agreements applicable to its operations (refer to Related Documents, page 1).
- Adhere to best practices and standards where possible.
- Establish and maintain records and information management guidelines and procedures.

Records cannot be destroyed until their retention period (as specified in the Retention and Disposal Schedules) has passed. In some instances, records must not be destroyed, even if the retention period has passed. This may occur when:

- A Disposal Freeze is issued by Queensland State Archives,
- The records are subject to legal processes such as discovery or subpoena,
- The records are required for internal or external investigation, or;
- The records are related to an application made under the Right to Information Act 2009

4.6 INFORMATION PRIVACY, CONFIDENTIALITY AND SECURITY IS ASSURED

To help protect Rhodes Business School information and its consumers, the School will:

- Ensure all information is stored, accessed, managed and used in accordance with its information security classification.
- Safeguard personal and sensitive information and maintain controls for security of information as documented in the School Cyber Security Policy.
- Establish and maintain procedures for the secure and appropriate sharing of confidential information.

Preserve and maintain records to meet administrative, legal, fiscal and archival requirements and in accordance with at least the minimum requirements of approved retention and disposal schedules.

5. Roles, Responsibilities and Accountabilities

Information management is the responsibility of all School consumers. Specifically, each information domain (e.g. Learning & Teaching, Management, or Human Resources) must have a designated officer. The officer role will usually relate to the organisational associated with the business functions primarily responsible for managing the domain's data.

5.1 CEO

The CEO must ensure RHODES BUSINESS School complies with the Public Records Act 2002 (QLD), including the principles and standards established by the Queensland State Archives. This responsibility may be delegated to relevant staff in accordance with the provisions set out below.

The CEO is responsible for:

- Interpreting the business and information needs, and strategic goals of the School and translating them into ICT initiatives that deliver value to the School.
- Setting the strategic direction for the School's ICT and information management.
- Ensuring that Information Service Providers are adequately resourced to support this policy.
- Ensuring that alleged breaches of this policy are investigated.
- Ensuring that appropriate mitigation, reparation and punitive measures are taken following investigations of misuse (e.g. the suspension of consumer accounts).
- Ensuring this policy and supporting procedures are enforced and maintained.

5.2 Compliance Director

The Director Compliance is responsible for:

- Advising consumers of best practices for effective record governance
- Assisting relevant staff with the development and implementation of standards, controls and procedures for managing official records.
- Being aware of Disposal Freezes issued by the Queensland State Archives and advising Information Stewards.
- Ensuring the records of the school are managed throughout their lifecycle in accordance with the approved retention and disposal schedules.
- Reviewing and approving the standards, procedures, and other controls required for security, lifecycle management, risk management, and quality assurance of the information they steward.
- Ensuring that the management, use and protection of information is consistent with this policy, its associated guidelines and procedures, as well as relevant legislation, contracts and agreements.
- Assigning operational responsibility for information to one or more information officers and ensuring resources are available to perform the required information management functions.
- Granting and revoking Information Consumers' and Information Service Providers' access to information and, when necessary, instructing them on the authorised uses of that information

- Ensuring that information officers are adequately trained in relation to their roles and responsibilities
- Ensuring the school information management is considered when decisions are made about systems.
- Enabling the timely detection, reporting, and analysis of security incidents where circumvention or attempted circumvention of controls takes place.

5.3 Student Service Officers

Information officers ensure the rules for managing information in the school are enforced on behalf of the Compliance Director are responsible for:

- Understanding, developing and recommending standards, procedures, and other controls for lifecycle management, risk management, quality assurance, appropriate use and security of information.
- Implementing and maintaining the information security controls that enforce the rules and procedures for information and records management, which includes identifying the security classification level of information assets.
- Performing system administration tasks including: physical site security; administration of security and authorisation systems; backup and recovery procedures; capacity planning; and system performance monitoring that ensure the reliability, integrity and functionality of business systems.
- Delivering and supporting the systems, services, and information technology infrastructure required for Rhodes Business School's information management.
- Complying with information security controls in their own work, and reporting information security breaches to the appropriate Information Officer as they arise.
- Ensuring the information asset register is accurate.

5.4 Information consumers

Rhodes Business School stakeholders accessing the school information to undertake their roles are considered consumers and are responsible for:

- Complying with the rules and procedures approved by the Compliance Directorr, for the use of information and records.
- Complying with controls implemented by Information Officers and ensuring information security breaches are reported to the Compliance Manager and appropriate Information Officer as quickly as possible.
- Understanding and complying with the school's ICT policies and procedures.
- Relinquishing access to the School information when it is no longer required to undertake their role.

5.4 Managers

Rhodes Business School managers must ensure that:

- Their staff are aware of the school's information management policies and procedures, and assign appropriate information management responsibilities to staff within their unit.
- Documented information management systems are in place, consistent with the school's information management policies and procedures, to support business processes.
- Their staff have access to the information required to perform their roles based on business needs and information security requirements.

5.6 All staff

All school staff must ensure that records are created and managed adequately to document evidence of the business events and activities associated with their work functions. Staff must also:

- Dispose of records in accordance with authorised Retention and Disposal schedules and follow the process as described in the School'sAR2.3.02 Records Management process, which may include authorisation prior to disposal activities.
- Maintain confidentiality of the school records and the privacy of personal information.
- Secure records against unauthorised access and release of information.
- Ensure all the School records in their possession at the time of cessation of employment are recorded effectively within the appropriate system or transferred to the custody of their supervisor.
- Ensure information transferred or shared with other parties and users meet the security requirements derived from its classification.

6. Monitoring, Review and Assurance

The CEO will ensure periodic review and monitoring of information management (including classification) is conducted to determine how well information management supports the school's business and strategic goals, and for its compliance with legislation. Results of this monitoring will be reported to the School Management Committee .

Rhodes Business School's Management Committee will review all ICT policies (three yearly) and procedures (annually) and ensure appropriate consultation is undertaken.

7. Recording and Reporting

Rhodes Business School will meet its data retention obligations under the Telecommunications (Interception and Access) Act 1979 (Cth.), recognising that Rhodes Business School will rely on the 'immediate circle' exclusion for any relevant services provided only to persons who are 'inherently connected to the functions of the School'.

Version History				
Review Period:		3 years from date of last approval		
Version Number:	**Approved by:**	**Approval Date:**	**Effective Date:**	**Sections Modified:**
D1				POLICY developed and documented
V1	CEO	April 2022	April 2022	Policy approved