STARDOM UNIVERSITY

STUDENT RECORDS MANAGEMENT AND RETENTION POLICY

Draft for Institutional Review and Approval — Supporting Regulatory Compliance Policy

Admissions and Registration / Registrar	Policy Owner
Academic Affairs and designated Compliance/Privacy Officer	Responsible Oversight
University President or authorized approving body	Approving Authority
Draft 1.0	Version
To be determined after formal approval	Effective Date
At least annually and whenever relevant legal or regulatory requirements change	Review Cycle

1- Purpose

This policy establishes controls for creating, maintaining, protecting, retrieving, retaining, and securely disposing of student academic and administrative records at Stardom University. It aims to support the accuracy of academic records, verification of enrollment and awarded degrees, protection of student privacy, and compliance with applicable legal and regulatory requirements.

2- Scope

This policy applies to student records in all formats, including paper, electronic, audio-visual, and other formats. It includes records held in the Student Information System, Learning Management System, electronic archives, email, and systems operated by approved service providers. It applies to personnel in Admissions and Registration, Academic Affairs, Student Affairs, Finance, Information Technology, faculty members, and anyone who creates, accesses, processes, or retains student records.

3- Governing Principles

• Accuracy and integrity: Records must be complete, clear, traceable, and protected against unauthorized alteration.

• Restricted access: Access is limited to authorized employees and only to the extent required for legitimate job duties.

• Confidentiality and security: Records must be protected through appropriate physical, technical, and organizational safeguards.

• Traceability: Material amendments, disclosures, corrections, and disposal activities must be documented where technically and operationally feasible.

• Retention by record type: Retention periods are determined in accordance with this policy's schedule, applicable laws, contractual obligations, and any legal hold.

• Secure disposal: Records subject to an investigation, complaint, audit, dispute, or retention obligation must not be destroyed.

4- Categories of Student Records

Responsible Office for Retention	Examples	Record Category
Admissions and Registration	Application for admission, identity verification, admission decision, prior qualifications, enrollment agreement, and supporting documents	Admissions and Identity
Registrar / Academic Affairs	Course registration, grades, assessment results, academic standing, academic progress, withdrawal, and course-equivalency decisions	Academic Record
Registrar / Admissions and Registration	Approved graduate list, degree-award decision, certificate number, certificate copy and transcript, replacement and verification register	Degrees and Graduation
Finance	Invoices, payments, refunds, balances, and related correspondence	Financial Records
Student Affairs / relevant office	Advising, complaints, appeals, disciplinary proceedings, and accommodations, with access restricted according to the nature of the record	Student Support and Conduct
Academic Affairs / Faculty	Course assignments, examinations, project assessments, and academic integrity cases	Learning and Assessment Evidence
Information Technology / Information Security Officer	Login, change, backup, verification, and security incident logs	System and Security Logs
Relevant office, with a copy retained in the official student file	Official notices and correspondence affecting admission, academic progress, grades, graduation, or student rights	Correspondence

5- Records Retention Schedule

The periods below are proposed internal retention periods for review and do not constitute a representation that every period is mandated by a BPPE regulation. Before this policy is approved, the periods must be reviewed for consistency with California requirements and those of any other applicable jurisdiction, contractual obligations, and the records and systems actually in use.

Record Type	Proposed Retention Period	Start of Retention Period	Notes
Official Transcript and Authoritative Academic Record	Permanent	Record creation / degree award	Retain courses, grades, credits, degree, and award date.
Degree and Certificate Award Register	Permanent	Degree award / certificate issuance	Retain the award decision, certificate number, and any correction or replacement.
Approved Graduate Lists and Degree-Award Approvals	Permanent	Approval / degree award	Retain the final approved list and evidence of authorized approval.
Admissions File and Signed Enrollment Agreement	At least 5 years after last attendance or end of the student relationship, or longer if required	Last attendance / end of relationship	Confirm the period against legal and contractual requirements.
Coursework, Examinations, and Grade-Change Evidence	At least 5 years after course completion, or longer if required	Course completion	Extend the period where an appeal, investigation, audit, or legal obligation exists.
Financial and Refund Records	At least 5 years after the transaction or end of the student relationship, whichever is later, or longer if required	Transaction / end of relationship	Finance must review tax, accounting, refund, and regulatory requirements.
Complaints, Appeals, and Disciplinary Records	At least 5 years after the final decision, or longer if required	Final decision	Restrict access and retain longer where a dispute, investigation, or legal hold exists.

Identity and Admissions Verification Documents	At least 5 years after the relationship ends, or longer if required	End of relationship	Apply data minimization and do not retain unnecessary copies.
Student Support Records	At least 5 years after the relationship ends, or longer if required	End of relationship	Restrict access to sensitive records.
Login, Security, and Change Logs	Proposed initial maximum of 2 years, subject to risk and law	Record creation	IT determines the actual period based on system capabilities and risk.
Backups	Under an approved backup and recovery schedule; expired copies must be securely erased	Backup creation	Backups do not replace permanent official academic records.
Routine Correspondence	At least 3 years unless related to an academic, financial, legal, or student-rights decision	Matter closed / last action	Material correspondence must be retained in the official student file.

6- Permanent Records and Credential Verification

• The Registrar or designated records officer must maintain an authoritative official record for each degree or certificate awarded, including the student's legal name, program and degree, award date, certificate number, and the approval on which the award was based.

• Corrections to an academic record must not erase the audit trail. The original entry, reason for correction, date, and name of the person authorizing it must remain traceable.

• Replacement certificates and transcripts must be recorded in a register showing the request, identity verification, approval, issue date, and a statement that the document is a replacement, together with its reference.

• A QR code or electronic verification service may be used only if it is actually implemented, tested, secured, and linked to accurate official records. This policy does not state that a QR service is currently operational.

• Verification disclosures must be limited to information the University is legally permitted to disclose.

7- Record Access, Student Requests, and Disclosure

The responsible office must handle requests to inspect, obtain copies of, correct, or verify records in accordance with approved privacy, student-rights, and complaints policies. The identity and authority of the requester must be verified; material disclosures must be documented where required; and information may be disclosed only to the extent permitted by law. No employee may release a student record to an unauthorized person.

8- Security and Backup

• Electronic records must be protected through role-based access permissions, appropriate authentication methods where available, secure transfer methods, and prompt removal of access rights when employment ends or duties change.

• Paper records must be stored in access-restricted locations and protected against loss, damage, and unauthorized access.

• Backup and recovery arrangements must be documented and tested periodically, and backups must receive appropriate protection.

• Any loss, unauthorized access, alteration, or unlawful disclosure must be reported promptly, and applicable legal notification obligations must be assessed.

9- Legal Holds, Audits, and Investigations

Upon receiving notice of litigation, a regulatory inquiry, an audit, complaint, investigation, or any other retention obligation, routine destruction of relevant records must be suspended. The Compliance Officer or designated legal counsel must notify the relevant departments and document the commencement and release of the legal hold.

10- Secure Disposal

After the approved retention period has expired and it has been confirmed that no legal hold or other obligation applies, records may be securely disposed of. Paper documents must be securely shredded or transferred to a trusted service provider; electronic records must be erased using a method appropriate to the medium and system. Where feasible, disposal must be documented, including the record category, date, method, authorizing person, and service provider, if any.

11- Responsibilities

Responsibilities	Office / Role
Maintain student files, academic records, certificate register, graduate lists, and transcripts; coordinate requests and corrections.	Registrar / Admissions and Registration
Verify records, grades, graduation requirements, and academic changes; maintain approved curricula and regulations.	Academic Affairs
Maintain financial and refund records and verify relevant retention periods.	Finance
Manage system permissions, backups, audit logs, recovery, and secure erasure.	Information Technology / Information Security
Maintain support, complaints, appeals, and conduct records with appropriate access controls.	Student Affairs
Review legal requirements, retention periods, disclosures, legal holds, and regulatory requests.	Compliance / Legal Counsel, if appointed
Use records only for authorized purposes, protect confidentiality, and report incidents and comply with this policy.	All Personnel

12- Training, Monitoring, and Review

Personnel authorized to access student records must be trained on confidentiality, secure handling, record correction, disclosure, and incident reporting requirements. The policy owner must review compliance at least annually, document exceptions and corrective actions, and update the retention schedule when requirements or systems change.

13- Exceptions and Approval

Exceptions require written justification and approval by the authorized body, following consultation with the Compliance Officer or legal counsel where appropriate. No exception may authorize destruction or disclosure contrary to law or a legal hold.