STARDOM UNIVERSITY

STUDENT RECORDS RETENTION AND MANAGEMENT POLICY

1. Purpose

This Policy establishes controls for creating, maintaining, protecting, retrieving, retaining, and securely disposing of student academic and administrative records held by Stardom University. It is intended to support accurate academic records, reliable verification of enrollment and awards, student privacy, and compliance with applicable legal and regulatory requirements.

2. Scope

This Policy applies to student records in paper, electronic, audiovisual, and other formats, including records held in the University's student information system, learning management system, electronic archive, email repositories, and authorized third-party systems. It applies to Admissions and Registration, Academic Affairs, Student Affairs, Finance, IT, faculty members, and any other authorized personnel who create, access, process, or maintain student records.

3. Governing principles

- Accuracy and integrity: records must be complete, attributable, legible, and protected against unauthorized alteration.
- Need-to-know access: access is limited to authorized personnel for legitimate institutional duties.
- Confidentiality and security: records must be protected using appropriate physical, technical, and organizational safeguards.
- Traceability: material changes, disclosures, corrections, and disposal actions must be logged where technically and operationally feasible.
- Retention by record category: records are retained according to the schedule in this Policy, applicable law, contractual duties, and any legal hold.
- Secure disposal: records are not destroyed while subject to a legal hold, audit, complaint, investigation, or other preservation obligation.

4. Student record categories

Record category	Examples	Primary custodian

Admissions and identity	Application, identity verification, admission decision, prior qualifications, enrollment agreement and supporting documents	Admissions and Registration
Academic history	Registration, course enrollment, grades, assessment results, academic standing, progression, withdrawals and transfer-credit decisions	Registrar / Academic Affairs
Awards and graduation	Approved graduate list, degree conferral, diploma/certificate number, diploma copy, transcript, replacement and verification logs	Registrar / Admissions and Registration
Financial	Tuition invoices, payments, refunds, outstanding balances and related correspondence	Finance
Student support and conduct	Advising, complaints, appeals, disciplinary records and accommodations, subject to restricted access	Student Affairs / designated office
Learning and assessment evidence	Course submissions, examination records, project evaluations, academic-integrity case records	Academic Affairs / faculty
System and security logs	Access logs, change history, backup logs, verification activity and incident records	IT / designated information security role
Communications	Official notices and material correspondence affecting admission, progression, grades, graduation or student rights	Relevant department; official record copied to student file

5. Retention schedule

The periods below are proposed internal retention periods for review, not a representation that every period is prescribed by BPPE. Before adoption, the University must confirm

applicable California requirements, any other jurisdictional obligations, contractual requirements, and the actual systems and records maintained.

Record category	Proposed retention period	Start point	Notes
Permanent academic transcript and official academic history	Permanent	Creation / award	Preserve an authoritative record of courses, grades, credits, degree and conferral date.
Degree/certificate award record and diploma register	Permanent	Conferral / issuance	Retain the award decision, unique credential number and correction/replacement history.
Approved graduate lists and conferral approvals	Permanent	Approval / conferral	Retain the final approved list and evidence of authorized approval.
Admissions/enrollment file and signed enrollment agreement	At least 5 years after the student's last attendance or separation, or longer if required	Last attendance / separation	Confirm applicable law and contractual requirements before adoption.
Coursework, examinations, project assessments and grade-change evidence	At least 5 years after course completion, or longer if required	Course completion	Retain longer for unresolved appeals, misconduct matters, audits or legal holds.
Financial and refund records	At least 5 years after the transaction or student separation, whichever is later, or longer if required	Transaction / separation	Finance must verify tax, accounting, refund and regulatory requirements.
Complaints, appeals and disciplinary records	At least 5 years after final resolution, or longer if required	Final resolution	Restrict access; retain longer where legal hold, safety, litigation or regulatory matter applies.

Identity verification and admission supporting documents	At least 5 years after separation, or longer if required	Separation	Apply data minimization and secure storage; do not retain unnecessary copies.
Student support records	At least 5 years after separation, or longer if required	Separation	Apply additional access restrictions to sensitive records.
System access, security and change logs	At least 2 years as a proposed baseline, subject to security risk and applicable law	Log creation	IT should set actual log periods based on system capabilities and risk.
Backups	According to an approved backup and recovery schedule; expired backups securely overwritten	Backup creation	Backups do not replace permanent official academic records.
Routine correspondence	At least 3 years, unless it documents a material academic, financial, legal or student-rights decision	Closure / last action	Material correspondence must be copied into the relevant official student record.

6. Permanent award records and verification

- The Registrar or designated records custodian maintains an authoritative record of each awarded degree or certificate, including the student's legal name, program/degree title, conferral date, official credential number, and the approval supporting the award.
- Corrections to an academic record must not erase the audit trail. The original entry, correction reason, date, and authorizing person should remain traceable.
- Replacement diplomas and transcripts must be recorded in a register showing the request, identity verification, authorization, issue date, replacement status, and credential reference.

- Any QR code or online credential-verification service may be used only if the service is actually implemented, access-controlled, tested, and linked to accurate official records. This Policy does not claim that a QR service is currently operational.
- Access to official records for verification must be limited to information that the University is authorized to disclose.

7. Access, disclosure and student requests

Requests to inspect, obtain, correct, or verify student records must be handled by the responsible custodian under the University's approved privacy, student-rights, complaints, and records procedures. The University must verify the requester's identity and authority, document material disclosures where required, and disclose only information permitted by applicable law. No employee may release a student's record to an unauthorized person.

8. Security and backups

- Electronic records must be protected through role-based access, strong authentication where available, secure transmission, and timely removal of access when personnel leave or change roles.
- Paper records must be stored in access-controlled areas and protected from loss, damage, or unauthorized viewing.
- Backups and recovery arrangements must be documented and tested periodically. Backup copies must be protected to the same standard as the source records.
- Suspected loss, unauthorized access, alteration, or disclosure must be reported promptly through the University's incident-response process and assessed for any legally required notification.

9. Legal holds, audits and investigations

When the University receives notice of litigation, a regulator inquiry, an audit, a complaint, an investigation, or another preservation obligation, routine destruction of relevant records must be suspended. The responsible compliance/legal representative must notify affected custodians and document release of the hold.

10. Secure destruction

At the end of an approved retention period, and only after confirming that no legal hold or other preservation requirement applies, records may be securely destroyed. Paper records must be cross-cut shredded or handled by a vetted secure-destruction provider. Electronic records must be securely erased or rendered inaccessible using methods appropriate to the

medium and system. Destruction should be logged with record category, date, method, authorizing person, and service provider where applicable.

11. Responsibilities

Role	Responsibility
Registrar / Admissions and Registration	Maintain official student files, academic history, award register, approved graduate lists and transcript/diploma records; coordinate record requests and corrections.
Academic Affairs	Validate academic records, grade changes, program completion and academic approvals; maintain approved curricula and academic regulations.
Finance	Maintain financial and refund records and confirm applicable financial retention requirements.
IT / information security	Maintain system access controls, backups, audit logs, recovery procedures and secure deletion controls.
Student Affairs	Maintain assigned support, complaint, appeal and conduct records with appropriate restricted access.
Compliance / legal adviser, if appointed	Review legal requirements, retention periods, disclosures, legal holds, and regulatory requests.
All personnel	Use records only for authorized purposes, preserve confidentiality, report incidents, and follow this Policy.

12. Training, monitoring and review

Personnel with access to student records must receive role-appropriate instructions on confidentiality, secure handling, record correction, disclosure, and incident reporting. The policy owner should review compliance at least annually, document exceptions and corrective actions, and update the retention schedule when applicable requirements or systems change.

13. Exceptions and policy approval

Exceptions require written justification and approval by the designated authority, after consultation with the compliance/legal adviser where applicable. No exception may authorize destruction or disclosure contrary to law or a legal hold.