DATA RETENTION POLICY & SCHEDULE

Purpose

Carden Academy of Maui maintains student, staff, and operational records in compliance with applicable laws, accreditation standards, and best practices. This policy defines how long records are kept and how they are securely destroyed.

Retention Principles

Records will be retained only as long as necessary for educational, legal, or operational purposes.

Permanent records (such as student transcripts, birth certificates, and immunization records) will be kept indefinitely.

Confidential records will be securely destroyed once the retention period has expired.

Digital records are subject to the same retention timelines as paper records.

Record Type	Examples	Retention Period	Disposition Method
Student Records – Permanent	Transcripts, cumulative file summary, immunizations, birth certificate, standardized test scores, final report cards	Indefinite (permanent archive)	Secure storage (digital + hard copy)
Student Records – Temporary	Attendance, disciplinary records, health forms, SST notes, IEP/504 plans	5 years after student leaves/withdraws	Cross-cut shred (paper), secure delete (digital)
Special Education (IDEA)	Evaluations, service plans, progress reports	5 years after services end	Secure delete or shred
Administrative	Board minutes, accreditation reports, handbooks, policies	Permanent	Secure archive
Operational Records	General correspondence, schedules, supply orders, non-essential files	3 years	Secure delete/shred
Financial – Permanent	Annual audit reports, IRS Form 990, general ledgers	Permanent	Secure archive
Financial – Standard	Payroll records, invoices, A/P & A/R, expense reports, bank statements	7 years	Secure delete/shred
Donor & Grants	Donation records, pledge agreements, grant documents	7 years after last entry or fulfillment	Secure delete/shred
Employee Records	Personnel files (contracts, evaluations, discipline)	7 years after separation	Secure delete/shred
Employment Eligibility (I-9)	I-9 forms	3 years after hire OR 1 year after termination (whichever is later)	Secure delete/shred
Technology Records	User account credentials, access logs, incident reports	2 years unless tied to investigation	Secure delete