



Information Technology Network Accounts & Identity Policy

Date: June 2026

I. PREAMBLE & MISSION ALIGNMENT

The technology resources at Saint Joseph's College of Maine are provided as tools of stewardship to support our educational mission and Mercy values. We believe that Excellence and Integrity extend into our digital interactions. Protecting the privacy of our students, the security of our data, and the reputation of our institution is a core shared commitment. Access to College technology is a revocable privilege. Compliance with this policy by all members of the Saint Joseph's College of Maine community is strictly required.

II. IDENTITY LIFECYCLE & IDENTITY SUNSET

1. *The SJC Digital Identity (SSO)*

An @sjcme.edu account serves as a Single Sign-On (SSO) Identity, providing the essential institutional key to our integrated systems.

2. *Identity Sunset (Account Lifecycle)*

To maintain a secure perimeter and honor our data privacy obligations, account eligibility is strictly tied to active affiliation:

Faculty & Staff: Access is maintained through active employment status (ADP). Account access is retired immediately at the close of the final day of service or earlier as determined by SJC in its sole discretion.

Students: Access generally remains active for one year following the last date of attendance, after which the account is deleted.

Emeritus Status: Emeritus faculty utilize a dedicated identity within the @emeritus.sjcme.edu domain.

III. REGULATORY STEWARDSHIP & LEGAL PRESERVATION

Saint Joseph's College complies with the following institutional and legal standards:

All users must comply with these federal privacy and security mandates as outlined in Section III of the College's expanded compliance handbook: Family Educational Rights and Privacy Act ("FERPA"), Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach-Bliley Act ("GLBA"), & Higher Education Opportunity Act ("HEOA").

Maine Privacy Law: Compliance with applicable Maine State law regarding the protection of privacy to the extent applicable.

Institutional Preservation (Legal Hold): The College's obligation to preserve information for legal, regulatory, or audit purposes overrides all other deletion schedules. In the event of a "Legal Hold" or active litigation, the automated Identity Sunset and data deletion processes will be suspended for specific accounts as required by applicable law.

IV. DATA SOVEREIGNTY & INSTITUTIONAL CONTINUITY

1. Ownership of Data

All data created, stored, maintained, or transmitted using College-provided resources are the property of Saint Joseph's College unless otherwise expressly stated in an applicable policy or contract. The granting of access to College-provided resources does not transfer ownership of any data to any user.

2. Business Continuity & Access

The institution reserves the right to access any account's data for business-critical needs, including during a user's absence or following a separation of service.

3. Responsibility for Personal Data

College accounts are provided exclusively for institutional business. Users are expected to minimize any personal use of such accounts (such as banking or private commerce). The College is not responsible for the preservation or migration of personal data. Upon the Identity Sunset, access to all stored files is terminated.

V. SECURITY & NETWORK INTEGRITY

1. Credential Security & Monitoring

The College utilizes multi-factor authentication ("MFA") and proactive monitoring. Users should have no expectation of privacy with respect to their use of, or for the information contained in,

College-owned technology resources, including, without limitation, any infrequent personal use of such resources.

2. Remote Access & Security Incident Reporting

Users must ensure devices used for remote access meet SJC security standards. This Policy should be considered a subset of the College's various policies regarding information security, which include but are not limited to the policies contained in the Guidebook, including *Confidentiality*, the Technology Resources listed on the mySJC webpage, and the College's Student Handbook. Suspected breaches or phishing must be reported to the IT Helpdesk (iteam@sjcme.edu) immediately.

VI. APPROVALS AND ASSET STEWARDSHIP (IT HARDWARE)

The College prohibits users from using the following media without written approval from Information Technology: remote-access technologies, wireless technologies, removable electronic media, laptops, and mobile devices. All College-owned hardware must be returned to the IT Department on or before the final day of employment for secure decommissioning and reallocation.

VII. TRAINING, COMPLIANCE & ENFORCEMENT

Keeping sensitive information secure requires periodic training of users to keep security awareness levels high. Users are expected to complete periodic security training and cooperate with security audits. A user's failure to comply with the standards set forth in this Policy may result in a loss of technology privileges, and disciplinary action up to and including termination of employment or, for students, sanctions under the Student Code of Conduct.

VIII. CONCLUSION: THE INTEGRITY OF STEWARDSHIP

At Saint Joseph's College, our commitment to security is a direct reflection of our commitment to our people. We recognize that true stewardship requires the diligent protection of the information entrusted to us. This policy may be interpreted, amended, supplemented, or rescinded in the College's sole discretion and without notice to employees.