Operating Standard

Title: Email Usage **Number:** A8000.30
Type: Administrative
Responsible: ED, Public Information & Marketing, Director, IT
Related Policies: A6200; A6300; A8000
Linked Operating Standards: A6000.15; A6200.25; A6200.35; A6300.00; A6300.10; A6300.15; A6300.30; A6300.35; A6300.45; A6400.15; A8000.00
Related Laws:
Related External Standards: AMA; EDUCAUSE/HEISC; ISO/IEC 27001; ISO/IEC 27002; NIST SP 800-53;
HLC Criterion: 2, 3D, 4A

1.0 Statement

Shawnee Community College (SCC) issues email accounts to employees as a primary means of official communication. Email is a vital tool for instruction, operations, and student and community engagement. This Operating Standard establishes expectations for email use that are professional, secure, accessible, and aligned with the College's mission, values, and brand identity. In doing so, it promotes consistency, civility, inclusivity, transparency, accountability, and security in all official communications.

2.0 Purpose and Scope

2.1 Purpose

This Operating Standard establishes clear expectations for the use of SCC email, including signature standards, access to large distribution lists, appropriate content use, and compliance with legal, accessibility, and branding requirements.

2.2 Scope

This Operating Standard applies to all SCC employees, including full-time, part-time, adjunct, and temporary employees, as well as consultants, contractors, and vendors issued SCC email accounts.

Student email use is governed separately by the Student Code of Conduct and related technology use policies.

This Operating Standard applies only to SCC-issued email accounts. Other forms of electronic communication, including text messaging, messaging applications, and social media, are governed by separate College policies where applicable.

3.0 Definitions

Official Communication: Email messages sent in the course of College business or on behalf of the institution.

Mass Email: A message distributed to more than fifty (50) recipients or any "All Employees," "All Students," or similarly broad distribution group.

Sensitive Data: Information protected under law or policy, including but not limited to student records, financial data, and personally identifiable information (PII).

College Business: Activities directly related to SCC instruction, operations, services, governance, or community engagement.

4.0 Assigned Email Addresses

Each employee is issued an official SCC email address by the Information Technology Department. All official College communication shall be directed to this address. Employees are expected to monitor and respond to SCC email regularly during business hours.

Personal email accounts shall not be used for College business except in rare, approved circumstances and in accordance with applicable College policy.

5.0 Email Signatures

To maintain a professional, consistent, and institutionally neutral appearance in official College communications, employee email signatures should include only business-related identification and contact information.

Approved signature elements may include:

- Employee name
- Job title
- Department or division
- Shawnee Community College
- Phone number(s)
- Official College website or approved links
- Professional credentials relevant to the employee's role
- Optional pronouns, if the employee chooses to include them

Email signatures may not include personal quotes, religious references, scripture, political statements, advocacy slogans, promotional language unrelated to College business, decorative graphics not approved by Public Information & Marketing, or other non-business content.

All email signatures shall follow approved College branding, formatting, and accessibility standards. Shawnee Community College reserves the right to require modifications to signatures that do not align with this Operating Standard.

6.0 Mass and All-College Email Communications

Access to large distribution lists such as “All Employees” or “All Students” is restricted to designated leadership and administrative offices.

Employees may not distribute mass or all-College email communications without prior coordination and approval from Public Information & Marketing.

Requests for mass email distribution must be submitted through Public Information & Marketing, which will review communications for relevance, appropriateness, accessibility, branding, and alignment with institutional priorities.

Mass email should be reserved for urgent or institution-wide communications such as policy changes, emergency notifications, or major College events. Routine department updates and reminders should not be sent using mass distribution lists.

Misuse of “reply all” to large distribution lists is prohibited.

7.0 Appropriate Use and Content

7.1 Permitted Uses

SCC email accounts may be used for:

- Academic and administrative communication
- Dissemination of information related to College programs, services, events, deadlines, and policies
- Professional collaboration and operational coordination
- Faculty-to-student instruction, advising, and support

All email communications must be accessible, including the use of readable text, adequate color contrast, descriptive links, and accessible attachments.

7.2 Prohibited Uses

SCC email accounts may not be used for:

- Harassment, discriminatory, defamatory, or offensive communication
- Political campaigning or partisan endorsements
- Religious proselytizing
- Commercial advertising or personal business
- Chain letters, spam, or mass forwards unrelated to College business
- Unauthorized transmission of sensitive or confidential information

8.0 Privacy, Security, and Records

SCC email accounts and communications are the property of the College. Use of SCC email constitutes acknowledgment that communications may be accessed by the College in messages sent or received through SCC systems.

The College does not routinely monitor individual email accounts but reserves the right to access accounts when required for operational continuity, security, legal compliance, investigations, or litigation.

Email communications may constitute public records and are subject to the College Records Retention Schedule and applicable state and federal laws, including FERPA, the Illinois Freedom of Information Act, and the Illinois State Records Act. Emails subject to litigation holds, audits, or investigations may be retained beyond standard retention periods.

Employees must follow all College security practices, including password standards, encryption requirements when transmitting sensitive data, and vigilance against phishing or unauthorized access.

8.1 Incident Response

If an employee suspects an email account compromise, the employee must:

1. Immediately change their password.
2. Disconnect affected devices from the network, if applicable.
3. Report the incident to the Information Technology Department and their supervisor without delay.
4. Follow Information Technology guidance for remediation and monitoring.

9.0 Roles & Responsibilities

9.1 Employees

Employees are responsible for using SCC email professionally; complying with signature standards; protecting credentials and sensitive information; ensuring accessibility; and adhering to approval requirements for mass email communications.

9.2 Supervisors and Department Heads

Supervisors and department heads are responsible for ensuring staff are aware of and comply with this Operating Standard and for addressing noncompliance.

9.3 Information Technology Department

The Information Technology Department is responsible for provisioning and managing SCC email accounts, maintaining security controls, providing technical support, and deactivating accounts upon separation of employment.

9.4 Public Information & Marketing
Public Information & Marketing is responsible for providing approved email signature templates; reviewing, coordinating, and approving mass or all-College email communications for branding, accessibility, and compliance; and ensuring messaging consistency with College standards.

9.5 Training
All employees must complete required onboarding and periodic training related to email use, data protection, and accessibility standards.

9.6 Non-Employee Email Accounts
Temporary SCC email accounts for consultants, contractors, and vendors must be approved by the sponsoring department and the Information Technology Department. Accounts will be time-limited, reviewed regularly, and deactivated immediately upon conclusion of the engagement.

10.0 Enforcement

Violations of this Operating Standard may result in corrective or disciplinary action consistent with College policy and applicable collective bargaining agreements, up to and including termination of employment.

Alleged violations involving security risks, harassment, or other serious misuse must be escalated immediately to the appropriate Vice President and the Information Technology Department.

Individuals who report inappropriate email use in good faith will be protected from retaliation in accordance with applicable laws and College policy.

11.0 Compliance with Laws

This Operating Standard shall be administered in accordance with applicable state and federal laws, including but not limited to FERPA, the Illinois Freedom of Information Act, the Illinois State Records Act, the ADA, and related employment and data protection laws. In the event of a conflict, applicable law supersedes this standard.

12.0 Review and Revision

This Operating Standard shall be reviewed at least every three (3) years, or as sooner due to legal, technological, or institutional changes, and shall follow SCC Shared Governance processes.

13.0 SCCES Connections

This Operating Standard supports the Infrastructure Effectiveness Key Performance Element, including:

- Strategic Communication
- Reliable System Performance
- Fiscal Stewardship (risk mitigation and control environment)

14.0 Monitoring Report Connections

This Operating Standard supports the College's Monitoring Report framework by generating evidence related to institutional communication practices, data security, and operational integrity. These elements contribute to the reliability, consistency, and effectiveness of College systems and services.

Evidence generated through this standard may include:

- Mass email usage and approval records
- Email-related policy violations or misuse incidents
- Email security incidents (e.g., phishing, account compromise)
- Compliance with signature and branding standards
- Accessibility compliance in electronic communications

These indicators provide insight into communication effectiveness, institutional risk management, and adherence to operational standards. Collectively, they support Monitoring Reports evaluating Infrastructure Effectiveness, including Strategic Communication, Reliable System Performance, and elements of Fiscal Stewardship related to risk mitigation.

Operational Area	**Evidence Generated**	**Monitoring Alignment**
Mass Email Governance	Approved vs. unauthorized communications	Strategic Communication Integrity
Email Usage Compliance	Misuse incidents, policy violations	Workplace Accountability & Operational Integrity
Email Security	Phishing attempts, compromised accounts	Reliable System Performance
Accessibility Compliance	Use of accessible formats and content	Equity in Access to Information
Signature & Branding Standards	Compliance with institutional templates	Institutional Consistency & Public Trust

Collectively, these indicators support the College's ability to maintain consistent, secure, and effective communication practices, while reinforcing institutional accountability and public trust.

15.0 Oversight & Review

- Reviewed at least every three (3) years or sooner as required
- Coordinated by Information Technology and Public Information & Marketing
- Supported by the Office of Institutional Effectiveness for data analysis and alignment with SCCES
- Aligned with applicable legal, regulatory, and accreditation requirements
- Revisions documented in the Change Log.

Change Log	Governance Unit: Executive Council
Date	**Description of Change**
04.23.26	Initial Adoption