SMS / Text Message Governance Policy

Policy number: 800-IT-9
Policy owner: ITS

Date of initial publication: August 28, 2026
Date of latest revision: N/A

SECTION I. PURPOSE

This policy establishes enterprise governance standards for SMS/text messaging conducted for University of St. Thomas business. It is intended to support responsible, consistent, and compliant use of SMS while protecting recipient trust, privacy, and the university's messaging reputation.

A. Executive Summary - Key Points for Non-Technical Readers

- This policy applies to university business SMS activity conducted by St. Thomas employees and units, regardless of the SMS-capable tool or service used.
- SMS is treated as a shared enterprise communication channel. Use of SMS by one program can affect recipient trust, delivery, and opt-out risk for other university communications.
- Consent for one lifecycle stage, program, or use case does not automatically authorize SMS for another lifecycle stage, program, or unrelated use case.
- New recurring SMS programs, new categories of texting, and use of new SMS-capable tools require university review before launch.
- Detailed platform standards, operational procedures, technical controls, and implementation guidance are maintained in an authenticated internal companion resource referenced in Appendix A.

SECTION II. SCOPE AND APPLICABILITY

This policy governs SMS/text messaging activity conducted for university business, regardless of the SMS-capable tool, vendor, platform, or service used.

SMS messages for university business may be sent only through ITS-approved or university-sanctioned platforms and sender configurations. Existing or newly discovered SMS-capable tools that have not been reviewed by ITS are subject to review, remediation, transition, or restriction.

The expectations set forth in this policy apply to all St. Thomas employees (faculty, staff and student workers) and all schools, colleges, divisions, departments, programs, and other units conducting university business by SMS/text message.

This policy does not govern emergency notification programs operated by UART or Public Safety. Those programs remain under their existing protocols and operational ownership. Questions about the intersection of this policy and emergency notification operations should be directed to UART, Public Safety, and ITS jointly.

SECTION III. DEFINITIONS

When used in this policy, the following terms have the following meanings:

a. ***Program*** means an approved SMS use case, communication workflow, or sender activity conducted for university business.

b. ***SMS/text messaging*** means electronic text messaging sent to or received from a mobile telephone number for university business, including one-to-one, group, bulk, automated, or recurring messages.

c. ***Consent*** means documented permission or other approved authorization that supports a defined SMS program, audience, or use case, as required by university standards and applicable law.

SECTION IV. GOVERNING PRINCIPLES

- SMS is a shared enterprise channel and is not a general self-service marketing channel.
- Consent for one lifecycle stage, program, or use case does not automatically transfer to another.
- University units must use approved platforms, sender configurations, consent practices, and opt-out processes.
- No unit may use an SMS-capable tool or alternate sending method to bypass enterprise approval, consent, or suppression requirements.
- SMS programs must have an identifiable business purpose and an accountable university owner.

SECTION V. REGULATORY AND RISK FRAMEWORK

University SMS activity must comply with applicable legal, regulatory, carrier, privacy, records, and university requirements. These may include requirements related to consent, revocation of consent, sender registration, student records, privacy, and message delivery practices.

Except for emergency notifications, university business SMS may not be sent before 8:00 AM or after 9:00 PM in the recipient's local time zone unless a more restrictive university or emergency rule applies.

This policy is an operational risk-control document and is not a substitute for legal advice. Questions involving new consent language, unusual use cases, or legal interpretation must be reviewed with General Counsel.

SECTION VI. CONSENT STANDARDS

Consent requirements are governed by audience, lifecycle stage, program, and use case. Consent for one program, lifecycle stage, or use case does not authorize texting for a different program or unrelated use case, even when the recipient remains affiliated with the university.

A. Audience and Program Consent

- Prospective-student SMS must use an approved consent or authorization method appropriate to the admissions or recruitment use case.
- Enrolled-student SMS must use an approved consent or authorization method appropriate to the student-lifecycle program or use case.
- Alumni, donor, event, and Advancement SMS must use an approved consent or authorization method appropriate to the applicable engagement purpose.

B. Approved Consent Language

Only consent language that has been approved by General Counsel and implemented in the active collection method may be relied upon when such consent is required for an SMS program. Approval of language in principle does not establish operational readiness if the approved language is not yet in use.

C. Prohibited Consent Methods

- Pre-checked SMS consent boxes or default-Yes selections.
- Combined email and SMS consent in one checkbox.
- Implied consent based only on enrollment, employment, or another relationship with the university.
- Verbal consent without a retained written record.
- Third-party, purchased, or transferred SMS consent.

D. Consent Documentation

Approved SMS programs must be able to identify the basis for contacting the intended recipient population, including the applicable consent source or documented authorization and the intended program or use case.

SECTION VII. OPT-OUT AND RE-CONSENT

Recipients may revoke consent through STOP keywords or through another reasonable method recognized by the university. A valid revocation must be honored for the governed scope in accordance with university procedure.

Employees who receive an SMS opt-out request outside an automated keyword process must follow the approved internal procedure so the request can be recorded and honored promptly.

A recipient who previously opted out may be re-enabled only through an approved re-consent method appropriate to the program and sending platform. Employees may not manually override an opt-out or suppression outside an approved procedure.

SECTION VIII. PLATFORM, SENDER, AND ACCESS GOVERNANCE

University SMS programs may operate only through platforms, sender types, telephone numbers, short codes, gateways, or other sender configurations that have been reviewed and approved by ITS and registered or provisioned as required.

No university unit may independently procure, configure, or use an SMS-capable tool for university business without ITS review and approval.

Access to approved SMS platforms must be provisioned according to role and business need. Platform-specific use cases, sending models, access roles, operational thresholds, and technical requirements are maintained in authenticated internal standards and procedures.

SECTION IX. MESSAGE CONTENT AND OPERATING STANDARDS

Bulk SMS programs and first-contact messages must identify the university or program and provide opt-out instructions appropriate to the sending method. Messages should be concise, relevant to the approved use case, and sent only to the intended recipient population.

Sensitive content, including FERPA-protected student information, financial details, health information, disciplinary information, academic-standing details, or other high-risk personal information, must not be sent by text. SMS may direct a recipient to a secure university channel, but the text message itself must not include sensitive details unless an exception is explicitly approved under applicable university policy.

SECTION X. APPROVAL, REVIEW, AND ENFORCEMENT

New recurring SMS programs, new categories of texting, use of new SMS-capable tools, and exceptions to approved SMS use must be reviewed through Marketing Technology and ITS before launch. Additional review by General Counsel may be required where applicable.

Existing SMS programs and sender configurations may be reviewed for alignment with this policy and applicable internal standards. The university may require remediation, restriction, transition, or suspension when a program does not meet approved requirements.

Violations of this policy may result in suspension of SMS privileges, escalation to ITS and General Counsel, or other corrective action appropriate to the risk and severity.

SECTION XI. DATA GOVERNANCE AND RECORDS

University-designated systems and procedures must be used to document and govern SMS consent, opt-out status, and related preference information. Approved SMS platforms and business processes must honor the governing SMS suppression status and applicable program consent boundaries.

University units must follow approved procedures for maintaining recipient data quality, responding to reported wrong numbers or number changes, and retaining records needed to support SMS governance and compliance.

Detailed system-of-record design, cross-platform synchronization, technical controls, workflow ownership, and reconciliation procedures are maintained in authenticated internal standards and are not reproduced in this public-facing policy.

SECTION XII. INTERNAL STANDARDS AND PROCEDURES

Detailed implementation requirements for this policy are maintained in an authenticated internal companion document available to authorized St. Thomas users. The internal resource includes approved platform and channel guidance, role-based responsibilities, operational procedures, technical and data controls, opt-out workflows, platform-specific sending requirements, exception processes, and implementation guidance.

University employees and authorized users must comply with this policy and with the internal standards and procedures applicable to their role and SMS program. The internal companion document supports implementation of this policy and must remain consistent with the governance requirements established here.

See Appendix A for the authenticated internal resource location.

Appendix A to SMS / Text Message Governance Policy

Authenticated Internal Standards and Procedures

Date of initial publication: 800-IT-9
Date of latest revision: N/A

The detailed SMS governance standards, platform procedures, technical controls, implementation guidance, and operating requirements are maintained in an authenticated University of St. Thomas resource and are not reproduced in the public policy repository.

SECTION I. AUTHENTICATED INTERNAL RESOURCE

Resource title: Full SMS / Text Message Governance Policy (authenticated internal version)

Access: St. Thomas authentication required

Location: https://link.stthomas.edu/sms-policy

Questions regarding access, interpretation, or implementation should be directed to Marketing Technology, ITS.