

NORTHWEST ARKANSAS COMMUNITY COLLEGE

SMS (Text Messaging) and Telephone Communications Privacy Statement

The procedures in this statement establish the operational requirements for the collection, use, disclosure, retention, and protection of personal information obtained through SMS (text messaging) and telephone communications. These procedures support the NWACC Privacy Policy and ensure compliance with applicable federal and state laws, including the Telephone Consumer Protection Act (TCPA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), applicable FCC regulations, and other privacy requirements governing electronic communications.

SCOPE

These procedures apply to all College departments, employees, contractors, student employees, and approved third-party service providers who send or receive SMS messages or place telephone calls on behalf of NWACC.

These procedures apply to communications with:

- Prospective students
- Current students
- Parents or guardians (when permitted by law)
- Employees
- Applicants
- Alumni
- Donors
- Vendors
- Community members
- Other individuals interacting with the College

Collection of Telephone Numbers

College departments may collect mobile or telephone numbers through approved College processes, including:

- Admissions applications
- Employment applications

- Event registrations
- Online inquiry forms
- Student information systems
- Direct communications
- Other College-approved business processes

Only information reasonably necessary for College operations shall be collected.

Consent for SMS Communications

Before sending text messages, departments must obtain the individual's affirmative consent whenever required by law.

Consent may be obtained through:

- Website forms containing an SMS consent checkbox
- Electronic registration forms
- Admissions or employment applications
- Event registration systems
- Other approved electronic or written consent processes

Consent shall not be a condition of admission, employment, enrollment, receipt of services, or purchase.

Departments shall maintain documentation of consent consistent with College record retention requirements.

Telephone Communications

Telephone calls may be made for legitimate College purposes including:

- Admissions
- Enrollment
- Academic advising
- Student services
- Financial aid
- Campus events

- Safety notifications
- Employee communications
- Other official College business

Where permitted by law, calls may utilize:

- Automated dialing systems
- AI-assisted technologies
- Prerecorded messages
- Artificial voice technology

Individuals shall be informed when required by applicable law.

Appropriate Use of SMS Messaging

Departments may use text messaging for:

- Appointment reminders
- Registration reminders
- Application status updates
- Event notifications
- Enrollment communications
- Emergency notifications
- Student support communications
- Limited promotional information where consent has been obtained

Employees shall not use SMS messaging to transmit confidential information unless the communication method has been approved by Information Technology and complies with applicable security requirements.

Examples of information that shall not be transmitted through standard SMS include:

- Social Security Numbers
- Payment card information
- Protected educational records unless authorized under FERPA
- Sensitive medical information

- Passwords or authentication credentials

Call Recording

Where calls are recorded for quality assurance, training, compliance, or documentation purposes:

- Individuals shall receive any legally required recording notification.
- Recordings shall be stored securely.
- Access shall be limited to authorized personnel.
- Recordings shall be retained according to College record retention schedules.

Protection of Personal Information

Employees shall:

- Verify identity before discussing protected information.
- Access only information necessary to perform assigned duties.
- Use College-approved communication platforms.
- Follow FERPA, GLBA, and other applicable privacy requirements.
- Report suspected privacy incidents immediately according to College incident reporting procedures.

Third-Party Service Providers

Departments utilizing third-party SMS or telephone communication platforms shall ensure vendors:

- Maintain appropriate security safeguards.
- Use information solely for contracted services.
- Do not sell or disclose telephone numbers for marketing purposes.
- Comply with applicable privacy laws.
- Execute required College data protection agreements.

Opt-Out Procedures

SMS Messages

- Individuals may revoke consent by replying STOP, QUIT, END, REVOKE, OPT OUT, CANCEL, UNSUBSCRIBE, or any other reasonable statement that clearly communicates they no longer wish to receive text messages.
- Opt-out and revocation requests must be honored as soon as practicable and no later than 10 business days after receipt, unless a shorter period is required by law, contract, or platform rules.
- Individuals may also contact the College directly to request removal from SMS communications.

Telephone Calls

Individuals may opt out by:

- Informing the College representative during a call
- Contacting the appropriate College office
- Using any approved opt-out process provided by the College

Departments shall document and honor opt-out requests in accordance with applicable law.

Records Retention

SMS communications, call logs, consent records, and recorded telephone calls shall be retained according to:

- NWACC Records Retention Schedule
- Applicable FERPA requirements
- GLBA requirements
- State records retention requirements
- Litigation hold requirements when applicable

When records are no longer required, they shall be securely destroyed.

Data Security

Departments shall implement reasonable administrative, technical, and physical safeguards to protect information collected through SMS and telephone communications.

Safeguards include:

- Role-based access controls
- Secure vendor platforms
- Encryption where available
- Multi-factor authentication
- Employee privacy training
- Incident response procedures

Employee Responsibilities

Employees using SMS or telephone communications shall:

- Follow these procedures.
- Use only approved College communication systems.
- Protect confidential information.
- Verify recipient identity before discussing protected information.
- Report suspected privacy or security incidents immediately.
- Complete required privacy and information security training.

Questions

Questions regarding these procedures should be directed to:

Privacy Officer / Chief Information Officer

NorthWest Arkansas Community College

479-986-4000

helpdesk@nwacc.edu

Related Documents

- NWACC Privacy Policy
- FERPA Policy
- Gramm-Leach-Bliley Act Notification
- Acceptable Use Policy