Archdiocese of Seattle

October 26, 2026

Advisory: Important Microsoft 365 Multi-Factor Authentication (MFA) Changes Coming in 2027

Audience: Parish and School Leadership, Business Managers, ParishStaq Administrators, Microsoft 365 Users
Action Required: Review and prepare for authentication changes before February 1, 2027

Microsoft Is Retiring SMS(Text Message) and Voice MFA

Microsoft has announced that it will retire its built-in SMS (text message) and voice-call multi-factor authentication (MFA) service for Microsoft 365 and Microsoft Entra ID users. Beginning **February 1, 2027**, users who rely on receiving authentication codes by text message or automated phone calls will no longer be able to use those methods unless an alternate telephony solution has been implemented. [learn.microsoft.com], [learn.microsoft.com]

As part of this transition, Microsoft is moving organizations toward **phishing-resistant authentication methods**, including passkeys, Microsoft Authenticator, Windows Hello for Business, and FIDO2 security keys. [learn.microsoft.com], [learn.microsoft.com]

Why Is Microsoft Making This Change?

Cybercriminals have become increasingly successful at bypassing traditional SMS-based authentication through phishing attacks, SIM-swapping, social engineering, and other techniques. Microsoft considers text-message and voice-call authentication among the least secure MFA methods available today. [learn.microsoft.com], [windowsreport.com]

Passkeys and other phishing-resistant authentication methods provide significantly stronger protection because they cannot be intercepted, forwarded, or stolen in the same way as one-time codes sent via text message or voice calls. [learn.microsoft.com], [windowsreport.com]

Important Dates

September 1, 2026

Microsoft will begin automatically encouraging users who currently use SMS or voice authentication to register a passkey and may present passkey registration prompts during sign-in. [learn.microsoft.com], [learn.microsoft.com]

February 1, 2027

Microsoft-provided SMS and voice authentication will be retired for most users. Users who only have SMS or voice configured for MFA may be unable to access their Microsoft 365 accounts until a supported authentication method is registered. [learn.microsoft.com], [learn.microsoft.com]

What Parishes and Schools Should Do Now

The Archdiocese recommends that parishes and schools begin preparing now by:

1. Contacting your Microsoft 365 Vendor

Many parish and school systems, including financial, student information, volunteer management, timekeeping, and cloud-based applications, may currently rely on SMS or voice-based authentication. Reach out to your vendors now to understand their plans for supporting passkeys, Microsoft Authenticator, security keys, or other phishing-resistant authentication methods. Early conversations can help identify potential compatibility issues, required software updates, user training needs, and implementation timelines well before Microsoft's February 2027 retirement date.

2. Review Current MFA Methods

Identify staff who currently receive MFA verification codes by:

- Text message (SMS)
- Automated voice call

These users will be most affected by the change. [learn.microsoft.com]

3. Consider Passkeys

Microsoft is strongly promoting passkeys as the future of secure authentication. Passkeys may be stored on:

- Mobile devices
- Windows computers
- Security keys

These provide superior protection against phishing and account compromise. [learn.microsoft.com], [windowsreport.com]

4. Update User Training

Staff should become familiar with new authentication methods before Microsoft begins prompting users for passkey registration.

5. Avoid Waiting Until 2027

Organizations that postpone preparation may face increased help desk requests, account access issues, and user confusion as the retirement date approaches.

What This Means for AOS Guardian and Cybersecurity

The Archdiocese has consistently encouraged the use of stronger authentication methods as one of the most effective cybersecurity controls available. This change aligns with current industry best practices and helps reduce exposure to:

- Credential theft
- Business email compromise
- Phishing attacks
- Account takeover
- Financial fraud

Strong authentication remains one of the most effective ways to protect parish, school, and chancery information systems.

The best time to prepare is before Microsoft forces the change. Migrating users to stronger authentication methods now will help ensure a smooth transition and better protect parish and school accounts from increasingly sophisticated cyber threats.