# Best Practices for Secure Communications

1. **Use Encrypted Platforms**

- Use Signal for sensitive discussions. It offers end-to-end encryption, minimal metadata retention, and open-source transparency .
- Turn on disappearing messages, registration lock, and screen lock.

2. **Secure Accounts and Devices**

- Use strong, unique passwords and enable two-factor authentication (2FA) or passkeys on all communication apps.
- Store passwords in a manager such as 1Password or Bitwarden.
- Keep apps and operating systems updated to close security vulnerabilities.
- Use long log-in passwords on your devices and disable message previews on lock screens.

3. **Protect Shared Files and Metadata**

- Before sharing, strip metadata from Word and PDF files using the Document Inspector in Word or Remove Hidden Information in Adobe Acrobat .
- For highly sensitive material, share sanitized versions via encrypted services such as Tresorit, which provides end-to-end encryption.

4. **Establish Organizational Communication Protocols**

- Designate which platforms are approved for which types of communication (e.g., Signal for private, email or Slack for non-sensitive).
- Use separate channels for internal and external communication.
- Label sensitive topics and documents clearly.
- Include secure-comms guidance in your incident response plan (who to contact, when to switch to encrypted tools).

5. **Minimize Data Exposure**

- Collect and share only essential personal information. Avoid over-collection in communication platforms and forms.
- Train staff on privacy principles and proper use of encrypted tools.

6. **Maintain Privacy in Collaboration and AI Tools**

- Avoid uploading personal or confidential data to generative AI systems; use placeholder text in drafts.

- Keep advocacy or campaign plans off open systems unless sanitized.

---

Revision #2
Created 30 October 2025 20:11:20 by Josh
Updated 30 October 2025 22:06:17 by Josh