# Best Practices for Safely Sharing Google Docs

These guidelines help you use Google Drive strategically, balancing collaboration needs with data protection and security awareness. Adapt these practices based on your organization's risk level, document sensitivity, and compliance requirements.

# Before You Share: Document Classification

**Ask yourself first:**

- Who needs access to this document?
- What's the worst case if this document becomes public?
- Does it contain sensitive information (donor data, strategy, personal details)?
- How long will external parties need access?

**Document Sensitivity Levels:**

- **Public:** Annual reports, press releases, published research (share freely)
- **Internal:** Staff communications, draft materials (organization-only)
- **Confidential:** Strategy documents, donor lists, financial data (restricted sharing)
- **Highly Sensitive:** Legal materials, info that compromises sources (use Tresorit, not Google)

# Sharing Permission Levels: Choose Wisely

Google Docs offers three permission levels: viewer, commenter, and editor. Use the most restrictive option that still allows necessary work:

**Viewer (Read-only)**

- Best for: Sharing final documents, board reports, public materials
- Recipients can: View and download (but not edit)
- Use when: You want to share information without risk of changes

**Commenter**

- Best for: Review processes, feedback gathering
- Recipients can: View, download, and add comments
- Use when: You need input but want to control actual edits

**Editor (Full Access)**

- Best for: Active collaboration with trusted colleagues
- Recipients can: View, download, edit, and share with others
- **Warning:** Editors can also re-share your document with anyone

# The "Anyone with the Link" Trap

**Never use "Anyone with the link" for sensitive documents.** This setting makes your document accessible to anyone who obtains the URL—through forwarded emails, shared screenshots, or accidental posting.

**Instead:**

- Use **"Restricted"** access (specific people only)
- Manually add each person's email address
- Review the access list before sharing

**Exception:** Public documents like published reports can use "Anyone with the link" with "Viewer" permissions.

# Access Audits: Regular Maintenance

Set a recurring calendar reminder to review document access:

**Quarterly Reviews:**

1. Open important documents
2. Click "Share" button
3. Review the list of people with access
4. Remove anyone who no longer needs access (former staff, completed projects, external consultants)

**Immediate Removal When:**

- Staff members leave the organization
- External consultants complete their work

- Board members rotate off
- Partnership agreements end

# Advanced Security Settings (for owners of documents)

**Enable "Prevent viewers from downloading":**

- Click Share → Settings (gear icon)
- Under "People who can download, copy, and print," uncheck "Editors" and "Commenters and Viewers"
- Note: This deters but doesn't fully prevent determined users from capturing content

**Restrict sharing abilities:**

- Click Share → Settings (gear icon)
- Uncheck "Allow editors to change permissions and share"
- This prevents editors from adding new people

**Link expiration (for Google Workspace users):**

- Share → Advanced → Set expiration date
- Useful for time-limited external collaboration

# Secure Sharing Workflow

**For External Partners:**

1. Create a "clean" version with sensitive details removed
2. Share with "Commenter" access initially
3. Set calendar reminder to revoke access when project ends
4. If extensive collaboration needed, consider other platforms (see "Alternatives" below)

**For Internal Teams:**

1. Create shared folders with appropriate team permissions
2. Store sensitive documents in restricted folders
3. Use clear naming conventions indicating sensitivity level
4. Document your organization's folder structure

# Communication Security

**Don't share sensitive documents via:**

- Unsecured email with "Anyone with the link" settings
- Public Slack channels
- Social media messages

**Instead:**

- Send direct emails to specific individuals
- Use "Restricted" sharing with email addresses
- For highly sensitive materials, switch to Signal and use Tresorit links

# What Google Can Access

**Important Reality Check:**

Google can access the content of your documents. While Google Drive offers encryption "at rest" and "in transit," it is not end-to-end encrypted. This means:

- Google can read your documents (for business purposes and legal compliance)
- Documents can be subject to legal requests and subpoenas
- Google scans content for security threats and policy violations
- Documents are vulnerable if Google's systems are compromised

**For truly sensitive materials** (legal strategy, whistleblower information, highly confidential donor data), use end-to-end encrypted platforms like Tresorit instead of Google Docs.

# When NOT to Use Google Docs

**Switch to more secure alternatives when:**

- Documents contain personally identifiable information (PII) at scale
- Legal or financial information that could be subpoenaed
- Information about vulnerable individuals
- Strategic plans you cannot afford to have leaked
- Partnership with organizations requiring higher security standards

**Secure Alternatives:**

- **Tresorit:** End-to-end encrypted storage (Swiss-based, zero-knowledge)

- **Cryptpad:** Encrypted collaborative documents (less user-friendly)

# Red Flags: Signs of Compromised Documents

**Watch for:**

- Unexpected editors added to documents
- Unfamiliar names in version history
- Documents you don't recognize in your "Shared with me" folder
- Notifications of sharing activity you didn't initiate

**If you suspect compromise:**

1. Immediately revoke all sharing
2. Change your Google account password
3. Enable 2-factor authentication if not already active
4. Review recent account activity (myaccount.google.com/security)
5. Contact K'lal or your IT support for incident response guidance

---

Revision #1
Created 6 November 2025 16:20:24 by Josh
Updated 6 November 2025 16:21:05 by Josh