Cookie Policy

Last Updated: October 14, 2025
Effective Date: October 11, 2025

📋 Table of Contents

🍪 What Are Cookies?

Cookies are small text files that websites store on your device (computer, tablet, or mobile phone) to remember information about your visit. They help websites provide a better user experience by remembering your preferences and actions.

In our application, **our cookies** serve **one primary purpose**: to allow you to safely close your browser without losing your progress on forms and data entry. Additionally, third-party cookies from the QuillJS library CDN are used for library usage analytics.

🎯 How We Use Cookies

Our cookie usage is 100% user-controlled and privacy-focused:

- ✅ **User-Initiated Only**: Our cookies are created ONLY when you explicitly click the "Save for Later" button then enter the encryption phrase.
- ✅ **Client-Side Encryption**: All data is encrypted on your device before being stored
- ✅ **No Server Transmission**: Your data never leaves your device or gets sent to our servers
- ✅ **User-Controlled Access**: Only you have the encryption key (your chosen phrase)
- ✅ **Temporary Storage**: Our cookies automatically expire after 30 days
- ❌ **No Tracking**: We do not track your behavior, analytics, or personal information
- ❌ **No Marketing**: We do not use cookies for advertising or marketing purposes
- ❌ **No Third-Party Sharing**: Your data is never shared with third parties (QuillJS analytics track library usage only, not your data)

Third-Party CDN Cookies

Note: This application loads the QuillJS rich text editor library from a CDN (`cdn.quilljs.com`). The QuillJS CDN sets Google Analytics cookies to track library usage statistics. These cookies:

- Are set by QuillJS/Google Analytics (not by us)
- Track QuillJS library usage across websites (not your personal form data)
- Are used by QuillJS developers to understand library adoption
- Do **NOT** have access to your encrypted form data
- Expire after approximately 2 years
- Are subject to Google's Privacy Policy and QuillJS's practices

📊 Cookie Categories

Strictly Necessary Cookies ⚠️

These cookies are essential for the basic functionality you've requested:

Purpose	User Control	Can Opt Out?
Form data preservation	User-initiated only	✅ Yes - don't use "Save for Later"
Session state management	Automatic when saving	✅ Yes - clear saved data anytime

Functional Cookies 🔧

Purpose	User Control	Can Opt Out?
Remember if you have saved data	Automatic when saving	✅ Yes - clear saved data
Track data expiration dates	Automatic when saving	✅ Yes - clear saved data

⚠️ Third-Party Analytics (QuillJS Library)

Purpose	Source	Can Opt Out?
QuillJS library usage tracking	Google Analytics via QuillJS CDN	✅ Yes - block third-party cookies

Note: These analytics track how many websites use QuillJS, not your personal data or form content.

❌ We Do NOT Use

- **First-Party Analytics Cookies**: We do not track your behavior or usage
- **Marketing Cookies**: No advertising or personalization
- **Social Media Cookies**: No social media tracking or sharing buttons

🔍 Detailed Cookie Information

First-Party Cookies (This Website)

Cookie Name	Provider	Purpose	Duration	Security
`userFormData`	This Website	Stores your encrypted form data	30 days	AES-GCM 256-bit encryption
`hasStoredData`	This Website	Indicates if you have saved data (for UI)	30 days	Boolean flag only
`dataExpiration`	This Website	Tracks when your saved data expires	30 days	Timestamp only

Third-Party Cookies (QuillJS CDN)

Cookie Name	Provider	Purpose	Duration	Domain
`_ga`	Google Analytics (via QuillJS)	Track QuillJS library usage statistics	~2 years	`.quilljs.com`
`_ga_B37E2WMSPW`	Google Analytics (via QuillJS)	Enhanced analytics for QuillJS usage	~2 years	`.quilljs.com`

Important: These cookies are set by the QuillJS CDN to track how many websites use their library. They track library usage patterns, **NOT your personal form data or information**. Your encrypted form data remains completely separate and inaccessible to these analytics cookies.

🔒 Encryption Details

- **Algorithm**: AES-GCM with 256-bit keys
- **Key Derivation**: PBKDF2 with 100,000 iterations and SHA-256
- **Salt**: Randomly generated 16-byte salt per save operation
- **IV**: Randomly generated 12-byte initialization vector per save operation

🛡️ Security & Encryption

How Your Data Is Protected

1. **Client-Side Encryption**: Your data is encrypted on your device using industry-standard AES-GCM encryption
2. **User-Controlled Keys**: Only you know the encryption phrase - we cannot access your data
3. **No Server Storage**: Encrypted data stays in your browser's cookies only
4. **Secure Transmission**: Cookies use `Secure` and `SameSite=Strict` flags when possible

What This Means

- ✅ **Privacy**: Your actual form data is unreadable without your phrase
- ✅ **Control**: You have complete control over your data
- ✅ **Transparency**: All encryption happens in your browser (client-side)

⚠️ User Risks & Responsibilities

🚨 IMPORTANT: You Accept Full Responsibility

By using the "Save for Later" feature, you acknowledge and accept that:

Security Risks You Assume:

1. **Phrase Security**: If you choose a weak phrase, your data may be vulnerable
2. **Device Security**: If your device is compromised, your saved data may be at risk
3. **Browser Security**: If your browser is compromised, cookies may be accessible
4. **Shared Devices**: Anyone with access to your device/browser may attempt to access your data
5. **Data Loss**: We cannot recover your data if you forget your phrase
6. **No Backup**: There is no way to recover lost or corrupted cookie data

Your Responsibilities:

- ✅ Choose a strong, memorable encryption phrase (minimum 4 characters recommended)
- ✅ Keep your encryption phrase secure and private
- ✅ Use this feature only on trusted devices
- ✅ Clear saved data when using shared or public computers
- ✅ Understand that our saved data expires after 30 days
- ✅ Accept that data recovery is impossible without your phrase

Limitations of Our Security:

- 🔒 We cannot access your data (even to help recover it)
- 🔒 We cannot reset or recover forgotten phrases
- 🔒 We cannot guarantee protection against all attack vectors
- 🔒 We cannot protect against device-level compromises

⚖️ Legal Disclaimer

THE RISK IS 100% ON YOU. By using the save functionality, you agree that:

- You use this feature at your own risk
- We are not liable for any data loss, theft, or compromise
- You will not hold us responsible for security breaches on your device
- You understand the technical limitations and accept them

🎛️ Managing Your Cookie Preferences

How to Control Cookies

Option 1: Use Our Built-In Controls

- **Save Data**: Click "Save for Later" button (creates our first-party cookies)
- **Load Data**: Click "Load Saved Data" and enter your phrase
- **Clear Data**: Click "Clear Saved Data" (removes our first-party cookies only, not QuillJS cookies)

Option 2: Browser Settings

You can also manage cookies through your browser (manages both our cookies and QuillJS cookies):

- **Chrome**: Settings → Privacy and Security → Cookies and other site data
- **Firefox**: Settings → Privacy & Security → Cookies and Site Data
- **Safari**: Preferences → Privacy → Manage Website Data
- **Edge**: Settings → Cookies and site permissions → Cookies and site data

Option 3: Automatic Expiration

Our first-party cookies automatically expire after **30 days** - no action needed.

Third-party QuillJS cookies expire after approximately **2 years**.

Option 4: Managing Third-Party Analytics Cookies

QuillJS sets Google Analytics cookies that expire after approximately 2 years. To manage these:

- **Block Third-Party Cookies**: Use browser settings to block third-party cookies
  - Chrome: Settings → Privacy and Security → Third-party cookies → Block third-party cookies
  - Firefox: Settings → Privacy & Security → Enhanced Tracking Protection → Strict
  - Safari: Preferences → Privacy → Prevent cross-site tracking (enabled by default)
- **Clear Existing Cookies**: Manually delete `.quilljs.com` cookies from your browser
- **Privacy Mode**: Use incognito/private browsing mode for automatic cookie deletion
- **Ad Blockers**: Many ad blockers automatically block Google Analytics cookies

Important: Blocking these analytics cookies will **NOT** affect the rich text editor functionality. The QuillJS library will still work normally; only the usage tracking will be blocked.

📅 Data Expiration Tracking

When you save data, you'll see messages like:

> "Saved data will expire in 30 days"

You can check remaining time by attempting to load your data.

📞 Contact Information

If you have questions about this Cookie Policy or our data practices:

Developer: Austin Steil
Project: Document Generator
Policy Version: 1.1.0

📋 Policy Updates

This policy may be updated to reflect changes in our cookie usage. When updates occur:

- The "Last Updated" date at the top will change
- Significant changes will be highlighted in the application
- Continued use after updates constitutes acceptance of new terms

🔗 Related Information

- **Privacy by Design**: This application is built with privacy as the primary concern
- **Open Source**: The encryption implementation is transparent and auditable
- **Minimal External Dependencies**: Only CDN-hosted libraries (QuillJS) for rich text editing functionality
- **No User Tracking**: We do not track users; QuillJS CDN tracks library usage only (not user behavior)

This cookie policy is designed to be comprehensive and transparent about our minimal cookie usage. Your privacy and control over your data are our top priorities.