

# Privacy Policy & Terms of Service

**Last Updated:** August 2nd, 2025

## 1. Introduction

Welcome to Clearview ("we," "our," or "us"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our journaling application and related services (the "Service").

By using our Service, you agree to the collection and use of information in accordance with this policy and our terms of service.

## 2. Information We Collect

### 2.1 Account Information

- **Discord Authentication:** When you authenticate through Discord, we collect your Discord username, user ID, and associated email address
- **Profile Data:** Display name and any profile information you choose to provide

### 2.2 Journal Content

- **Journal Entries:** All text, images, and content you create within your journal
- **Entry Metadata:** Timestamps, categories, tags, and mood indicators
- **Usage Patterns:** How you interact with features and frequency of use

### 2.3 Technical Information

- **Device Data:** Device type, operating system, browser type and version, screen resolution
- **System Logs:** IP addresses, access times, error logs, performance metrics, and crash reports
- **Session Data:** Authentication tokens, session state, and temporary cache information
- **Analytics:** Page views, click patterns, feature usage statistics, and user flow data
- **Browser Storage:** Essential cookies for authentication, preference settings, and local storage for offline functionality

## 3. How We Use Your Information

### 3.1 Core Services

- **Service Delivery:** Provide, maintain, and improve our journaling platform
- **Account Management:** Manage your account authentication and access

- **Data Synchronization:** Sync your journal entries across devices
- **Customer Support:** Respond to inquiries and provide technical assistance

### 3.2 Service Improvement

- **Performance Optimization:** Monitor application performance and optimize user experience
- **Error Resolution:** Identify, diagnose, and resolve technical issues
- **Feature Development:** Understand feature usage to guide development priorities
- **Security Monitoring:** Detect and prevent unauthorized access or malicious activity

## 4. Medical Information Protection

**Critical Privacy Notice:** We recognize that journal entries may contain sensitive health and medical information.

### 4.1 Absolute Protection Guarantee

- We will **NEVER** share, sell, or disclose any medical or health information contained in your journal entries to third parties
- Your personal health insights, symptoms, medications, or medical experiences remain completely confidential
- We do not analyze journal content for medical purposes or share data with healthcare providers, insurance companies, or medical research organizations

### 4.2 Medical Disclaimer

- Our Service is not intended to provide medical advice, diagnosis, or treatment
- Always consult qualified healthcare professionals for medical concerns
- We are not responsible for any medical decisions based on journal entries or app usage

## 5. Data Storage and Security

### 5.1 Infrastructure

- **Primary Database:** MongoDB for core application data storage
- **Authentication Platform:** Supabase for user authentication and real-time features
- **Encryption Standards:** All data encrypted in transit and at rest using industry-standard protocols

### 5.2 Security Measures

- **Technical Safeguards:** TLS/SSL encryption, access controls, and role-based permissions

- **Monitoring:** 24/7 system monitoring with automated threat detection
- **Authentication:** Secure OAuth 2.0 integration with Discord
- **Regular Audits:** Periodic security assessments and vulnerability testing
- **Incident Response:** Established procedures for security breach detection and response

## 6. Data Sharing and Disclosure

### 6.1 We Do NOT Share Your Data Except:

- **With Your Consent:** Only when you explicitly authorize sharing
- **Legal Requirements:** When required by valid legal process or government request
- **Safety Purposes:** To prevent imminent harm when legally obligated

### 6.2 Service Providers

- Trusted third-party providers (MongoDB, Supabase, Discord) are bound by strict confidentiality agreements
- They may only access data necessary to provide their specific services
- All providers maintain equivalent security standards

## 7. Third-Party Services and Limitations

### 7.1 Technology Stack

Our web application utilizes modern web technologies, frameworks, and various open-source libraries that enable core functionality and user experience.

### 7.2 External Service Limitations

- **Discord:** Authentication provider; we are not responsible for Discord's data practices
- **MongoDB/Supabase:** Data storage providers; we are not liable for issues on their platforms
- **Third-Party Dependencies:** We are not responsible for vulnerabilities in open-source packages, libraries, or frameworks
- **Web Technologies:** Security issues inherent in underlying web technologies are beyond our direct control

### 7.3 Technology Risk Management

- We regularly update and monitor dependencies but cannot guarantee absolute security of third-party code
- Security patches are applied promptly, subject to upstream provider availability

- Zero-day vulnerabilities may exist before patches are available

## 7.4 Breach Notification

- Users will be notified within 72 hours of any confirmed data breach affecting their information
- We are not responsible for breaches at third-party providers or in open-source dependencies beyond our control

## 8. Your Rights and Controls

### 8.1 Data Rights

- **Access:** Request a complete copy of your journal data in portable format
- **Correction:** Update or correct any inaccurate information
- **Deletion:** Request permanent removal of your account and all associated data
- **Portability:** Export your data for use with other services

### 8.2 Account Deletion

- Delete your account anytime through app settings or by contacting support
- All personal data permanently removed from active systems within 30 days
- Some anonymized technical logs may be retained for security compliance
- Cached data may persist until natural expiration

## 9. Cookies and Browser Data

### 9.1 Cookie Types

- **Essential:** Required for authentication, security, and core functionality
- **Preference:** Store settings, themes, and language choices
- **Analytics:** Help understand user behavior for service improvement
- **Session:** Temporary cookies that expire when browser closes

### 9.2 Browser Storage

- **Local Storage:** Offline functionality, draft saving, and performance optimization
- **Session Storage:** Temporary data for current session
- **Cache Storage:** Static assets for faster loading
- **IndexedDB:** Offline journal storage and synchronization

## 9.3 Control Options

- Manage preferences through browser settings
- Essential cookies required for core functionality
- "Do Not Track" browser settings respected where feasible

## 10. Data Retention

- **Active Accounts:** Data retained while account remains active
- **Inactive Accounts:** Accounts inactive for 2+ years may be deleted after notification
- **Deleted Accounts:** All personal data permanently removed within 30 days
- **Backup Systems:** Data in backups retained up to 90 days for disaster recovery
- **Legal Requirements:** Data may be retained longer if legally required
- **Anonymous Analytics:** Aggregated, anonymized statistics may be retained indefinitely

## 11. International Data Processing

### 11.1 Cross-Border Transfers

- Data may be stored and processed in servers worldwide
- Appropriate safeguards ensure protection during international transfers
- Usage constitutes consent to this processing

### 11.2 Protection Standards

- Equivalent data protection maintained regardless of server location
- All transfers comply with applicable privacy regulations

## 12. Children's Privacy

Our Service is not intended for users under 13 years of age (16 in the EU). We do not knowingly collect information from children. Upon discovery of underage usage, accounts will be immediately terminated and data deleted.

## 13. Policy Updates

We may update this Privacy Policy and Terms of Service at any time at our sole discretion. Changes will be communicated through:

- Prominent in-app notifications
- Email notifications (when available)

- Updated documentation with revision dates
- Website banner notifications

**Material Changes:** Substantial changes affecting your rights will include 30 days advance notice.

**Immediate Updates:** We reserve the right to make immediate updates for legal compliance, security, or urgent operational needs.

Continued use after changes constitutes acceptance. If you disagree with updates, discontinue service use immediately.

## **14. Terms of Service**

### **14.1 Acceptable Use**

- Use Service solely for personal journaling and intended purposes
- Maintain confidentiality of account credentials
- Do not attempt security breaches, reverse engineering, or unauthorized access
- Prohibited: illegal activities, storing illegal content, system abuse, or service disruption
- Respect intellectual property rights

### **14.2 Service Availability**

- Target 99.9% uptime with no absolute guarantee
- Scheduled maintenance announced in advance when possible
- Emergency maintenance may occur without notice for security or stability
- Right to modify or discontinue features with reasonable notice

### **14.3 User Responsibilities**

- Maintain Discord account security for authentication
- Keep devices and browsers updated
- Report security vulnerabilities or suspicious activity promptly
- Back up important entries using export functionality

### **14.4 Limitation of Liability**

- Liability limited to maximum extent permitted by law
- Not responsible for data loss from user error, device failure, or browser issues
- Third-party service failures, breaches, or technical issues beyond our control

- No liability for third-party package vulnerabilities or framework issues
- Total liability capped at amounts paid in preceding 12 months
- Disclaimer of indirect, incidental, consequential, or punitive damages

## 15. Contact Information

**Privacy Inquiries:** [privacy@clearview.ca](mailto:privacy@clearview.ca)

**General Support:** [support@clearview.ca](mailto:support@clearview.ca)

**Response Commitment:** All inquiries answered within 48 hours during business days.

---

*This Privacy Policy ensures transparent data practices while maintaining the highest protection standards for your personal journaling content, including any sensitive health or medical information you choose to include. We are committed to safeguarding your privacy and providing a secure journaling experience.*