

Acceptable Use Policy

Open Mind Ledger

Last Updated: January 20, 2026

1. Introduction

This Acceptable Use Policy ("AUP") governs your use of the Open Mind Ledger platform ("Service") operated by Uncle Sam Tax Rescue LLC dba Open Mind Archives, a Florida limited liability company ("Company," "we," "us," or "our"). This AUP is incorporated into and forms part of our [Terms of Service](#).

The purpose of this policy is to ensure the Service remains secure, reliable, and beneficial for all users. Violation of this AUP may result in suspension or termination of your account.

2. Intended Use

2.1 Permitted Uses

The Service is designed for:

- **Accounting Professionals:** Managing financial dashboards for multiple clients
- **Bookkeepers:** Tracking income, expenses, and generating reports
- **Business Owners:** Viewing their own financial data and analytics
- **Tax Professionals:** Using tax planning tools for client advisory

2.2 Authorized Users

You may only grant access to: - Employees of your accounting firm - Authorized contractors under appropriate confidentiality agreements - Your clients (for viewing their own financial data only)

3. Prohibited Activities

3.1 Illegal Activities

You shall not use the Service to:

- Violate any applicable local, state, national, or international law
- Commit fraud, embezzlement, or financial crimes
- Launder money or facilitate illegal financial transactions
- Evade taxes or assist others in tax evasion
- Process financial data for sanctioned individuals or entities
- Violate export control or trade sanction regulations

3.2 Unauthorized Access

You shall not:

- Access accounts, systems, or data without authorization
- Attempt to bypass authentication or security measures
- Use another user's credentials without permission
- Share your credentials with unauthorized individuals
- Access Teams or client data you are not authorized to view
- Exploit vulnerabilities in the Service

3.3 Data Misuse

You shall not:

- Collect, harvest, or scrape data from the Service without authorization
- Use data obtained from the Service for unsolicited marketing
- Sell, rent, or lease user data obtained through the Service
- Use client financial data for purposes not authorized by the client
- Retain client data after your engagement has ended (unless required by law)
- Transfer data in violation of data protection laws

3.4 Technical Abuse

You shall not:

- Interfere with or disrupt the Service or connected networks
- Introduce malware, viruses, or other malicious code
- Conduct denial-of-service attacks or attempt to overwhelm our systems
- Use automated tools to access the Service except via documented APIs
- Exceed reasonable API rate limits or usage thresholds
- Reverse engineer, decompile, or disassemble the Service
- Attempt to extract source code or trade secrets

3.5 Misrepresentation

You shall not:

- Provide false or misleading information during registration
- Impersonate any person or entity
- Misrepresent your affiliation with any organization
- Create fake accounts or Teams for fraudulent purposes
- Submit false or manipulated financial data
- Misrepresent the capabilities or accuracy of the Service to clients

3.6 Harmful Content

You shall not upload, transmit, or store:

- Content that infringes intellectual property rights
- Defamatory, libelous, or harassing content
- Content that violates privacy rights
- Obscene, offensive, or inappropriate content
- Content promoting hatred or discrimination

3.7 Competitive Activities

You shall not:

- Use the Service to develop competing products or services
- Benchmark the Service for competitive purposes without consent
- Resell, sublicense, or redistribute the Service without authorization
- White-label the Service without a written agreement

4. QuickBooks Online Integration Rules

4.1 Authorization Requirements

When connecting QuickBooks Online accounts:

- You must have explicit authorization from the account owner
- You may only connect accounts for legitimate accounting/advisory purposes
- You must disconnect accounts when your engagement ends
- You must not connect accounts solely to harvest data

4.2 Data Handling

When accessing QBO data:

- Use data only for purposes disclosed to the client
- Do not retain data beyond what is necessary for your engagement
- Ensure appropriate confidentiality measures are in place
- Report any unauthorized access immediately

4.3 Compliance with Intuit Terms

Your use of the QBO integration must comply with: - Intuit's Terms of Service - Intuit's API Terms of Use - Intuit's Data Privacy Guidelines

5. AI Features Usage

5.1 Appropriate Use

When using AI-powered features:

- Use AI outputs as supplementary information, not as sole decision basis
- Verify AI-generated insights before presenting to clients
- Do not misrepresent AI outputs as professional advice
- Do not input personally identifiable information unnecessarily

5.2 Prohibited AI Use

You shall not:

- Use AI features to generate fraudulent content
- Attempt to extract or replicate AI models
- Use AI features for purposes that violate AI provider terms
- Submit prompts designed to bypass safety measures
- Use AI to generate misleading financial information

6. Resource Usage

6.1 Fair Use

To ensure fair access for all users:

- Do not make excessive API calls that impact service performance
- Do not store excessive amounts of data beyond reasonable business needs
- Do not abuse trial periods or free tier limitations
- Report performance issues rather than attempting workarounds

6.2 Rate Limits

The Service implements rate limits to ensure stability:

Resource	Limit
QBO data refresh	1 per hour per Team
API requests	60 per minute
Report generation	10 per hour
File uploads	10 MB per file

Exceeding these limits may result in temporary throttling or account review.

7. Security Responsibilities

7.1 Account Security

You are responsible for:

- Using strong, unique passwords
- Enabling multi-factor authentication (recommended)
- Protecting your credentials from unauthorized access
- Promptly reporting suspected security breaches
- Logging out from shared or public devices
- Regenerating Dashboard Access Codes if compromised

7.2 Reporting Vulnerabilities

If you discover a security vulnerability:

1. **Do not exploit** the vulnerability
2. **Report promptly** to security@openmindledger.com
3. **Provide details** to help us understand and fix the issue
4. **Do not disclose** publicly until we have addressed it

We appreciate responsible disclosure and will acknowledge security researchers who help us improve our security.

8. Professional Conduct

8.1 For Accounting Professionals

If you are using the Service as an accounting professional:

- Maintain appropriate professional licenses and certifications
- Adhere to applicable professional standards (AICPA, state boards)
- Do not provide services beyond your qualifications
- Maintain appropriate professional liability insurance
- Follow client confidentiality requirements

8.2 Client Relationships

When inviting clients to the Platform:

- Clearly communicate what data will be accessed
- Explain how their information will be used
- Provide clear terms for your professional engagement
- Respond to client inquiries promptly
- Remove client access when the engagement ends

9. Compliance Monitoring

9.1 Our Rights

We reserve the right to:

- Monitor Service usage to ensure compliance with this AUP

- Investigate suspected violations

- Remove content that violates this AUP

- Suspend or terminate accounts for violations

- Report illegal activities to law enforcement

9.2 User Cooperation

If we investigate a potential violation, you agree to:

- Cooperate with our investigation
- Provide requested information
- Preserve relevant records

10. Enforcement

10.1 Violation Consequences

Violations of this AUP may result in:

Severity	Examples	Consequences
Minor	Exceeding rate limits, minor misuse	Warning, temporary throttling
Moderate	Sharing credentials, data misuse	Account suspension, required remediation
Severe	Unauthorized access, fraud	Immediate termination, legal action
Criminal	Illegal activities	Termination, law enforcement referral

10.2 Appeals

If you believe enforcement action was taken in error:

1. Contact support@openmindledger.com within 30 days
2. Provide detailed explanation and relevant evidence
3. We will review and respond within 10 business days

10.3 Repeat Violations

Repeated violations, even if minor, may result in escalated enforcement action including permanent account termination.

11. Reporting Violations

11.1 How to Report

To report a violation of this AUP:

- **Email:** abuse@openmindledger.com
- **Subject:** "AUP Violation Report"

11.2 What to Include

- Your contact information
- Description of the violation
- Any evidence (screenshots, logs)
- Affected accounts or Teams (if known)

11.3 Confidentiality

We will keep your report confidential to the extent possible while investigating.

12. Changes to This Policy

We may update this AUP from time to time. Changes will be:

- Posted on this page with an updated date
- Communicated via email for material changes
- Effective 30 days after posting (or immediately for urgent security matters)

Continued use after changes constitutes acceptance of the updated AUP.

13. Contact Information

For questions about this Acceptable Use Policy:

Uncle Sam Tax Rescue LLC dba Open Mind Archives 8198 South Jog Road, Suite 104 Boynton Beach, FL 33472

General Inquiries: support@openmindledger.com **Security Issues:** security@openmindledger.com
Abuse Reports: abuse@openmindledger.com

Governing Law: This Acceptable Use Policy shall be governed by the laws of the State of Florida, United States, without regard to conflict of law principles. Any disputes shall be resolved in the state or federal courts located in Palm Beach County, Florida.

Effective Date: January 20, 2026

Version: 1.0

This document is provided for informational purposes only and does not constitute legal advice. It should be reviewed and customized by a licensed attorney familiar with your specific business, jurisdiction, and circumstances before use.