API USAGE POLICY

Effective Year: 2026

1. Introduction

This API Usage Policy governs access to and use of the MDOI Foundation's Application Programming Interfaces (APIs). The APIs are provided to support secure integration, identifier registration, metadata retrieval, identifier resolution, dashboard automation, reporting, interoperability, and connection with approved external systems.

2. Purpose of the Policy

The purpose of this policy is to ensure that all API access is used responsibly, securely, lawfully, and in a manner that protects the stability, integrity, performance, and trustworthiness of the MDOI infrastructure.

3. Scope

This policy applies to all individual users, organisations, developers, repositories, publishers, institutions, technical partners, API clients, and third-party systems that access or integrate with MDOI APIs.

4. API Access Eligibility

API access may be granted to approved users, organisations, repositories, publishers, or partners with legitimate technical, research, institutional, or operational needs. MDOI reserves the right to approve, restrict, suspend, or revoke API access where necessary.

5. API Key Management

Users and organisations must protect API keys, tokens, credentials, and integration secrets. API credentials must not be shared publicly, embedded in insecure code, exposed in repositories, transferred to unauthorised persons, or used outside the approved purpose.

6. Authentication and Authorisation

All API requests must use approved authentication methods. API users may only access records, functions, and services permitted under their assigned role, organisation, subscription, access level, or integration agreement.

7. Permitted API Uses

The MDOI API may be used for approved purposes such as creating identifiers, updating metadata, resolving identifiers, retrieving public metadata, synchronising repository records, validating landing pages, generating reports, and supporting interoperability with scholarly and institutional systems.

8. Prohibited API Uses

Users must not use the API to overload the system, scrape restricted data, bypass dashboard permissions, harvest private records, reverse-engineer the platform, upload malicious content, conduct spam activity, perform unauthorised surveillance, violate intellectual property rights, or compromise system security.

9. Rate Limits and Fair Use

MDOI may apply rate limits, request quotas, usage thresholds, and fair-use rules to protect system stability and ensure equitable access for all users. Excessive or abusive API usage may be throttled, blocked, restricted, or suspended.

10. Data Protection and Privacy

API users must comply with applicable data protection and privacy requirements. Personal data, organisational information, private metadata, hidden records, and restricted content must not be accessed, processed, shared, or stored without proper authority and lawful purpose.

11. Metadata Integrity

API users are responsible for ensuring that metadata submitted, updated, or synchronised through the API is accurate, complete, authorised, lawful, and consistent with MDOI metadata standards. Automated metadata updates must not introduce false, misleading, duplicate, or corrupted records.

12. Identifier Registration Through API

Where identifier registration is permitted through API access, each submitted object must meet MDOI registration and metadata requirements. Users must ensure that automated registration workflows do not create duplicate, incomplete, fraudulent, or unauthorised identifiers.

13. API-Based Resolution

The API may support identifier resolution, metadata lookup, and public record discovery. Users must not use API-based resolution to evade visibility controls, extract hidden metadata, misrepresent identifier records, or redirect users to unrelated or harmful content.

14. Integration Requirements

Systems integrated with MDOI APIs must be secure, properly configured, and maintained. Users are responsible for ensuring that their applications handle credentials safely, validate inputs, secure outputs, manage errors responsibly, and respect MDOI access rules.

15. Logging and Monitoring

MDOI may log and monitor API activity, including request volume, endpoints used, authentication events, errors, failed requests, suspicious behaviour, and system impact. Logs may be used for security, troubleshooting, analytics, compliance, and enforcement.

16. Security Requirements

API users must implement reasonable technical safeguards, including secure storage of credentials, encrypted communication, access restriction, input validation, error handling, and monitoring of integration activity. API use must not introduce vulnerabilities into the MDOI platform.

17. Service Availability

MDOI shall take reasonable steps to maintain API availability, performance, and reliability. However, API access may be interrupted due to maintenance, technical failures, security incidents, infrastructure upgrades, rate limiting, or external service disruptions.

18. Changes to API Services

MDOI may modify, update, add, remove, or deprecate API endpoints, authentication methods, data structures, rate limits, or integration requirements. Where reasonable, users may be notified of major changes that affect active integrations.

19. Third-Party Applications

Users who build third-party applications using MDOI APIs are responsible for the security, legality, accuracy, and compliance of those applications. MDOI is not responsible for misuse, failures, or data handling practices of external applications.

20. Suspension or Revocation of API Access

MDOI may suspend or revoke API access where there is misuse, excessive traffic, security risk, policy violation, non-payment of required maintenance contribution, unlawful activity, or behaviour that threatens platform integrity.

21. Compliance

All API users must comply with MDOI policies, applicable laws, intellectual property requirements, data protection standards, security obligations, and any integration agreement issued by the Foundation.

22. Enforcement

Violation of this policy may result in warnings, throttling, temporary blocking, API key revocation, account suspension, termination of integration privileges, removal of non-compliant records, or legal action where necessary.

23. Policy Review and Updates

This policy may be reviewed and updated periodically to reflect technical improvements, API changes, security requirements, user feedback, legal obligations, and developments in digital research infrastructure.

24. Conclusion

This API Usage Policy supports responsible, secure, and interoperable use of MDOI APIs. By complying with this policy, users and organisations help protect the reliability, security, scalability, and trustworthiness of the MDOI digital knowledge infrastructure.