

# Data Privacy Policy

What data we collect, how we protect it, and the additional care minors are owed.

---

|                |                 |
|----------------|-----------------|
| DELIVERABLE    | E-02            |
| EFFECTIVE DATE | January 1, 2025 |
| STATUS         | Adopted         |

## 1 Introduction

---

LinkScape is committed to protecting the privacy and security of personal data in accordance with applicable laws and our core values of Responsible Innovation, Transparency, Accessibility, Impact, and Safety.

This Data Privacy Policy ("Policy") outlines how LinkScape collects, uses, stores, protects, and deletes personal information from members, participants, volunteers, and other stakeholders. Because LinkScape primarily works with youth members, we prioritize heightened data protection measures and parental/guardian consent requirements.

## 2 Data Collection Principles

---

LinkScape adheres to the following data collection principles:

- Purpose Limitation: Data is collected only for clearly defined, explicit, and legitimate purposes related to our mission of technology research and education.
- Data Minimization: We collect only the minimum personal data necessary to fulfill stated purposes.
- Transparency: We clearly inform individuals what data we collect and how we use it before collection.
- Accuracy & Integrity: We maintain accurate records and allow individuals to verify and correct their information.
- Security by Design: Data protection is embedded into all systems and processes from inception.

### 2.1 Categories of Data Collected

LinkScape collects the following categories of personal data:

1. Identification Data: Name, email address, phone number, username, and unique member ID
2. Demographic Data: Age, date of birth (for age verification), school/university, geographic location
3. Account & Activity Data: Login history, project participation, course enrollment, assessment results

4. Parental/Guardian Data: For members under 18, parent/guardian name, email, phone, and consent records
5. Device & Technical Data: IP address, browser type, operating system, device identifiers (for security purposes only)
6. Communication Data: Messages, forum posts, feedback, and support communications

### 3 Consent Requirements

---

Explicit, informed consent is required for all data collection activities. LinkScape does not use pre-checked consent boxes or coercive practices.

#### 3.1 Consent for Members Under 18

For members under 18 years of age:

- Both the youth member AND their parent/legal guardian must provide written consent to data collection
- Consent must be obtained before any data is collected
- Parents/guardians receive a separate, plain-language explanation of data practices
- Consent can be withdrawn at any time by the youth member or parent/guardian

#### 3.2 Consent for Adult Members & Participants

For individuals 18 years or older:

- Individual must provide explicit written consent for data collection
- Consent documents are provided in plain language
- Consent may be withdrawn at any time

### 4 Data Handling Procedures

---

#### 4.1 Secure Storage

LinkScape stores personal data securely using industry-standard protections:

- Encryption in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent)
- Access controls and multi-factor authentication for systems storing personal data
- Secure firewalls and intrusion detection systems
- Regular security audits and vulnerability assessments

#### 4.2 Access Control & Limiting

Personal data is accessible only to authorized personnel with a legitimate need:

- Access is based on role and minimum necessary principle

- Staff undergo privacy training before accessing personal data
- All data access is logged and regularly reviewed

### 4.3 Data Sharing & Third Parties

LinkScope shares personal data with third parties only under these conditions:

- Explicit user consent is obtained
- Necessary to provide services (e.g., platform hosting, email services)
- Required by law or court order
- To protect the safety and security of our community
- All third-party service providers execute Data Processing Agreements (DPA) committing to equivalent privacy standards

LinkScope does not sell, trade, or monetize personal data under any circumstances.

### 4.4 Cookies and Web Tracking

LinkScope uses minimal tracking technologies:

- Essential cookies only (session management, security)
- No tracking pixels, beacons, or behavioral analytics
- Users can disable cookies at any time; essential functionality may be limited

## 5 Data Retention and Deletion Policies

---

### 5.1 Data Retention Schedule

LinkScope retains personal data according to the following schedule:

| Data Type                | Retention Period                | Purpose                        |
|--------------------------|---------------------------------|--------------------------------|
| Active Member Data       | Duration of membership + 1 year | Service delivery, support      |
| Inactive Member Data     | 18 months after last activity   | Account reactivation, archival |
| Transaction/Payment Data | 7 years (per tax/legal)         | Compliance, auditing           |
| Log & Audit Data         | 90 days                         | Security, intrusion detection  |

### 5.2 Data Deletion & Anonymization

When retention periods expire or deletion is requested:

- Personal data is securely deleted or anonymized
- Deletion is performed using certified data wiping tools (NIST-compliant standards)
- Backup copies are deleted within 90 days

- Deletion is confirmed in writing to the data subject

### 5.3 Right to Deletion & Account Closure

Individuals may request deletion of their personal data at any time, subject to legal obligations:

- Deletion requests must be submitted in writing to [privacy@linkscope.app](mailto:privacy@linkscope.app)
- We will respond within 30 days
- Exceptions apply for data required by law, active disputes, or security holds
- Account closure triggers deletion of associated personal data within 90 days

## 6 Data Breach Notification Procedures

---

LinkScape is committed to transparently managing data security incidents and breaches in accordance with applicable laws.

### 6.1 Breach Definition

A Data Breach is an unauthorized access, disclosure, or loss of personal data resulting from:

- Unauthorized access to systems or data
- Loss of encrypted or unencrypted devices
- Transmission errors (misdirected emails, etc.)
- Insider threats or malicious intent
- Third-party compromise

### 6.2 Breach Detection & Assessment

Upon discovering a potential breach:

1. Immediate Response: The security team isolates affected systems within 1 hour of detection
2. Investigation: A formal forensic investigation begins within 24 hours
3. Assessment: Determine scope (affected individuals, data types, cause)
4. Risk Analysis: Evaluate risk to affected individuals based on data sensitivity and breach type

### 6.3 Notification Timeline

Notification is sent as soon as reasonably possible, following this timeline:

- Within 24 hours: Internal notification to leadership and legal team
- Within 72 hours: Notification to affected individuals (if high risk)
- Within 30 days: Public disclosure (if legally required)
- Within 90 days: Full post-incident report to stakeholders

## 6.4 Breach Notification Content

Breach notifications include:

- What happened (nature and scope of breach)
- What data was affected
- What LinkScape has done in response
- Steps affected individuals should take
- Contact information for questions
- Free credit monitoring (for financial data breaches)

## 6.5 Post-Incident Procedures

Following any data breach:

- Root cause analysis to identify how breach occurred
- Remediation of vulnerabilities and implementation of corrective measures
- Updated security training for all staff
- Documentation of incident for regulatory review
- Communication with relevant regulatory authorities

## 7 Individual Rights

---

LinkScape respects the following individual rights regarding personal data:

- Right of Access: Request a copy of personal data we hold
- Right to Correction: Request correction of inaccurate data
- Right to Deletion: Request deletion of personal data
- Right to Opt-Out: Withdraw consent for data processing
- Right to Portability: Receive data in machine-readable format
- Right to Withdraw Consent: Withdraw consent at any time for minors and their guardians

## 8 Third-Party Service Providers

---

LinkScape uses third-party service providers for hosting, email, and analytics. All third parties:

- Sign Data Processing Agreements (DPAs) committing to equivalent privacy standards
- Are prohibited from using data for their own purposes
- Are audited annually for compliance
- Must notify LinkScape immediately of any breaches

## 9 International Data Transfers

---

LinkScape operates primarily in the United States. If personal data is transferred internationally:

- Recipients must provide an equivalent level of data protection
- Standard contractual clauses (SCCs) or binding corporate rules are used
- Consent is obtained before transferring data to jurisdictions with lower privacy standards

## 10 Policy Governance & Contact

---

### 10.1 Data Protection Leadership

LinkScape designates the following leadership for data protection matters:

- Chief Privacy Officer: Responsible for overall data protection strategy
- Security Officer: Implements technical and operational safeguards

### 10.2 Policy Updates

This policy is reviewed and updated annually or when:

- Laws or regulations change
- Significant data practices change
- A security breach or incident occurs

### 10.3 Contact Information

For privacy inquiries, requests, or concerns:

Privacy Email: [privacy@linkscape.app](mailto:privacy@linkscape.app)

Organization: LinkScape

Fiscal Sponsor: The Hack Foundation dba Hack Club, 501(c)(3)

Response Timeframe: All inquiries will be responded to within 30 days

## End of Document

---

LinkScape operates as a fiscally sponsored project of The Hack Foundation dba Hack Club, a 501(c)(3) nonprofit. Hack Club holds the charitable status and every dollar moves through Hack Club Bank.

E-02 · version · effective January 1, 2025 · [linkscape.app/governance/e-02](https://linkscape.app/governance/e-02)