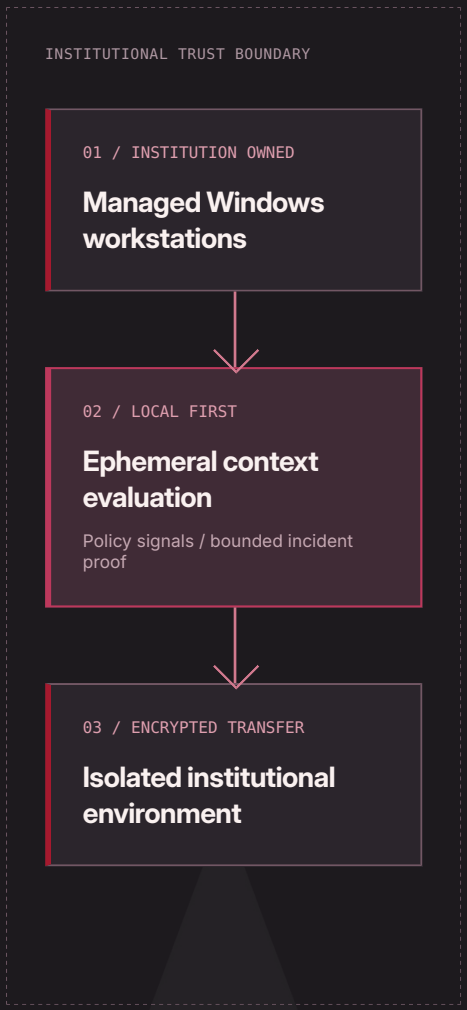
Obylon | BY UMBRAXIS

INSTITUTIONAL PUBLICATION / 2026

Obylon —
Privacy Policy
& Institutional Data Governance Framework



12	22.11.26	Umbraxis
POLICY CHAPTERS	EFFECTIVE DATE	PUBLISHER

SECURITY IS A SYSTEM.
TRUST IS AN OBLIGATION.

DOCUMENT REGISTER

The terms.
The scope.
The accountability.

Official policy record for institutional administrators, legal reviewers, and technical teams.

Product:

Obylon (Institutional Endpoint Governance & Computer Laboratory Security Platform)

Publisher:

Umbraxis

Applies To:

Obylon Endpoint Governance Suite, Obylon Optics Managed Browser Extension, and Umbraxis Institutional Management Console

Regulatory Alignment:

Digital Personal Data Protection (DPDP) Act, 2023 & DPDP Rules, 2025 (India)

Effective Date:

November 22, 2026

Official Domain:

https://umbraxis.tclservice.in

Privacy & Grievance Contact:

privacy@umbraxis.tclservice.in

DOCUMENT / CONTENTS

Twelve chapters of accountability.

12

Obylon — Privacy Policy & Institutional Data Governance Framework

01	1. About Obylon & Institutional Purpose	4
02	2. Legal Framework & Statutory Role Allocation	5
03	3. Architectural Design & End-to-End Data Lifecycle	6
04	4. Categories of Data Processed & Justified Purposes	8
05	5. Architectural Processing Boundaries & Prohibitions	11
06	6. Technical & Organizational Security Safeguards	12
07	7. Subprocessors & Cross-Border Processing Transparency	14
08	8. Data Retention, Automated Pruning & Verified Erasure	15
09	9. Security Incident & Personal Data Breach Protocol	16
10	10. Rights of Parents, Students & Institutional Staff (Data Principals)	17
11	11. Institutional Verification Reference (FAQ)	18
12	12. Grievance Desk, Security Disclosures & Policy Governance	20

Effective date: November 22, 2026

UMB / OBL / PRIVACY

01

INSTITUTIONAL PURPOSE

1. About Obylon & Institutional Purpose

Obylon is a B2B institutional endpoint security and computer-laboratory governance platform developed and operated by **Umbraxis**. Obylon is engineered exclusively for accredited schools, colleges, and educational institutions to secure institution-owned laboratory computers, enforce campus digital safety policies, prevent unauthorized removable-media execution, and maintain examination integrity.

Obylon operates strictly within managed institutional infrastructure under a written commercial agreement and **Data Processing Agreement (DPA)** executed with the subscribing educational institution. The platform is built on the principles of **purpose limitation, local-first evaluation, data minimization, cryptographic integrity, and verifiable institutional accountability**.

02

LEGAL FRAMEWORK

2. Legal Framework & Statutory Role Allocation

Umbraxis structures its data governance practices to align with the **Digital Personal Data Protection (DPDP) Act, 2023**, the **DPDP Rules, 2025**, and applicable Indian information technology standards.

2.1 Educational Institution as Data Fiduciary; Umbraxis as Data Processor

- **The Educational Institution (Data Fiduciary):** For all laboratory telemetry, policy enforcement records, incident artifacts, and administrative case dossiers processed through Obylon, the subscribing school or educational institution acts as the **Data Fiduciary**. The institution independently determines its acceptable-use policies, examination allowlists, staff role assignments, retention preferences, and notices to parents, guardians, and students.
- **Umbraxis (Data Processor):** Umbraxis acts strictly as a **Data Processor** with respect to institutional laboratory data, processing such data solely on the documented instructions of the Data Fiduciary and solely to deliver security, governance, and technical support services.
- **Independent B2B Administration:** Umbraxis acts as an independent Data Fiduciary exclusively for business-to-business relationship records—specifically institutional licensing, invoicing, authorized staff onboarding communications, and direct inquiries submitted through our official website.

2.2 Protection of Children's Personal Data

In alignment with **Section 9 of the DPDP Act, 2023** and the **Fourth Schedule of the DPDP Rules, 2025**, Obylon is purpose-built to support institutional safety and core educational operations:

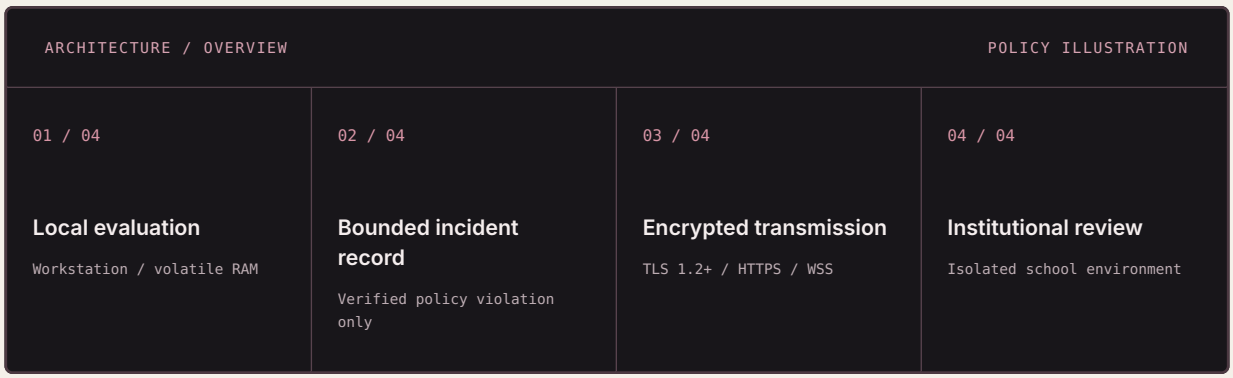
- **Conditional Educational Safety Scope:** Statutory exemptions available to educational institutions under the Fourth Schedule apply strictly within their legal conditions—namely child safety, digital protection, and core educational governance inside school laboratories. Obylon's technical enforcement is restricted exclusively to those boundaries (preventing unsafe web exposure, unauthorized software execution, academic misconduct during managed sessions, and workstation tampering).
- **Institutional Notice & Consent Responsibility:** The subscribing school, as Data Fiduciary, remains responsible for issuing clear acceptable-use and privacy notices to parents, guardians, and students, and for obtaining any verifiable parental consent required under applicable law for features or processing that extend beyond statutory educational exemptions.

- **Strict Prohibition on Commercial Use:** Obylon never engages in commercial tracking, cross-context behavioral profiling, targeted advertising, data brokerage, or third-party monetization of student or institutional records. Institutional data is never used to train artificial intelligence or machine learning models.

03

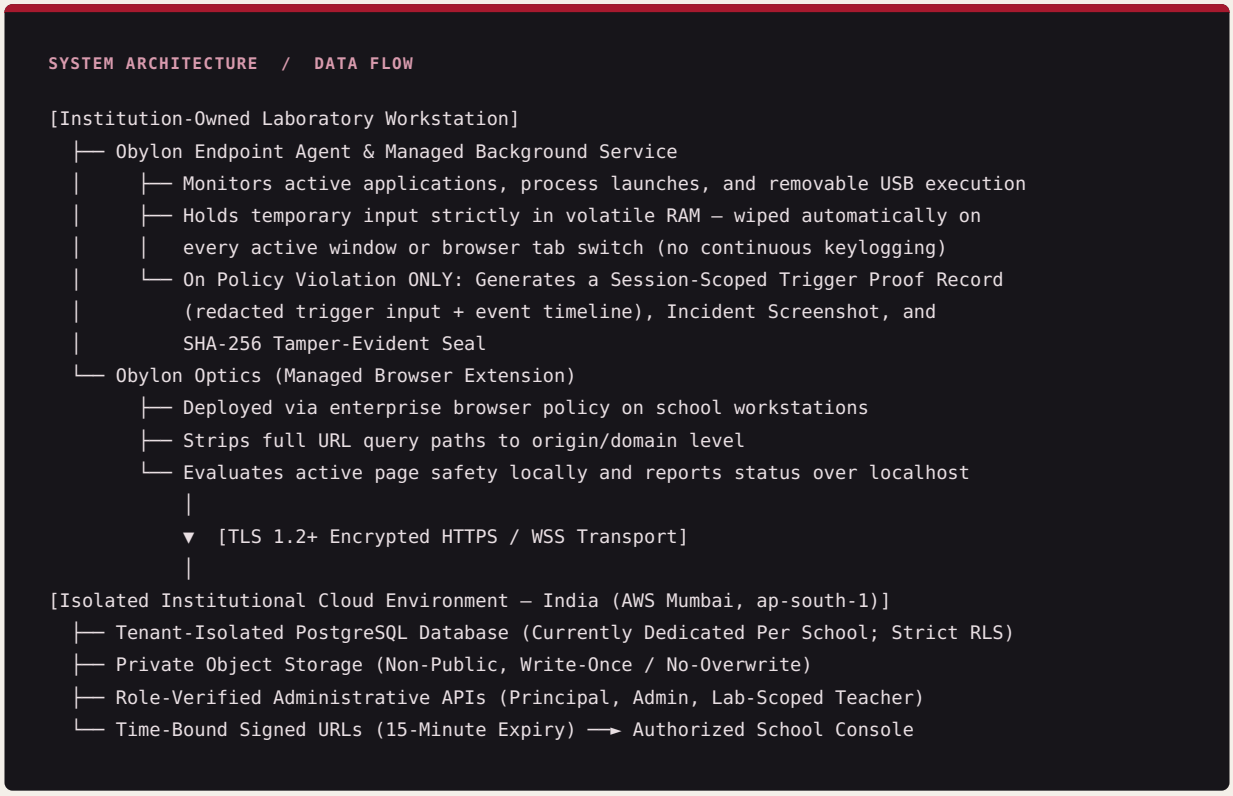
DATA ARCHITECTURE

3. Architectural Design & End-to-End Data Lifecycle



Obylon employs a **Local-First Evaluation, Minimal Cloud Reporting** architecture. Routine safety classification occurs ephemerally in volatile workstation memory (RAM) and is automatically cleared on every active window or browser tab switch unless a configured institutional policy violation occurs.

3.1 Data Flow Architecture



3.2 Transparent System Privileges & Technical Scope

To support thorough IT security reviews by school administrators and external auditors, Obylon transparently discloses its operational footprint:

- **Managed Endpoint Deployment:** Installation requires institutional Administrator authorization and deploys a managed background system service to maintain operational continuity, enforce school policies, and apply cryptographically verified software updates with automatic rollback protection.
- **Managed Browser Governance (`Obylon Optics`):** Deployed exclusively through institutional enterprise browser policies on managed laboratory workstations. `Obylon Optics` requests active-tab and page-context inspection permissions solely to evaluate websites against the school's safety and examination rules in real time. Full URL paths are stripped to origin/hostname, and page content is evaluated locally rather than bulk-archived to cloud servers.
- **Non-Intrusive Technical Boundaries:** Obylon operates in standard user and system service contexts without installing proprietary kernel-mode drivers and without performing covert HTTPS man-in-the-middle TLS decryption.

04

DATA CATEGORIES

4. Categories of Data Processed & Justified Purposes

Obylon collects only the minimum data required to deliver reliable laboratory security and verifiable governance.

4.1 Workstation Identity, Health & Licensing Telemetry

- **Data Processed:** Unique workstation identifier, assigned laboratory group (e.g., `Lab-1`, `Lab-2`), device hostname, hardware activation fingerprint, operating system version, CPU/memory utilization metrics, online heartbeat timestamps, software version, and crash/recovery diagnostics.
- **Purpose:** Maintain endpoint reliability, authenticate active institutional licenses, manage software updates, and provide technical diagnostics.

4.2 Application, Process & Removable Media Governance

- **Data Processed:** Active foreground application name, window title, executable path and digital publisher signature (for allowlist verification), removable USB drive detection events, and records of blocked or unauthorized executable launches.
- **Purpose:** Enforce examination-mode application allowlists, block unapproved tools, and prevent unauthorized software or malware execution from external USB drives.

4.3 Browser Safety Signals (`Obylon Optics`)

- **Data Processed:** Active tab origin/hostname (with URL paths stripped), page title, and locally computed safety and redirect-anomaly scores.
- **Purpose:** Enforce institutional web safety rules and distinguish intentional user navigation from automated advertising or pop-up redirects. Routine browsing text is processed locally in RAM and is not uploaded to cloud storage.

4.4 Session-Scoped Trigger Proof & Incident Screenshots (No Continuous Keylogging)

Shared school computers are used across periods by both students and staff (such as teachers logging into school ERPs, exam portals, or email). At the same time, when a genuine policy incident occurs, school leadership needs clear, objective records to evaluate whether the event resulted from deliberate user input or an accidental pop-up redirect.

Obylon addresses both requirements through **Session-Scoped Trigger Proof**:

- **How Ephemeral Window-Scoped Evaluation Works:**
  - Input context is evaluated strictly in volatile local memory (RAM) on the workstation—never written to disk during routine use and never streamed continuously to the cloud.
  - **Automatic Context Wipe:** The moment the active desktop window or browser tab changes, the temporary RAM buffer is cleared immediately. Previous sessions, closed tabs, classroom assignments, coding work, and staff login credentials entered in other windows or portals are discarded and cannot carry over into a later alert.

- **What Is Recorded Upon a Verified Policy Violation ONLY:** When—and **only** when—a workstation triggers a configured institutional policy violation (such as accessing restricted content, launching a prohibited executable, or bypassing examination controls), Obylon captures and uploads a bounded incident package consisting of:
  - **Incident Screenshot:** A single full-screen still image captured at the moment of the policy trigger and uploaded directly to the school's private, non-overwritable cloud storage bucket.
  - **Redacted Session-Scoped Trigger Input:** Exclusively the bounded search query or command entered inside the active violating window/tab that triggered the rule—automatically passed through redaction filters to mask email addresses, phone numbers, and long numeric/OTP sequences (`[REDACTED]`). Unrelated typing from earlier windows, tabs, or sessions is never recorded.
  - **Timestamped Event Timeline & Context Signals:** A chronological record of the triggering sequence (active application/browser transition, trigger input timestamp, and enforcement action) alongside `matched_rule_category` and browser-level pop-up/redirect indicators (`redirect_signals`) to help administrators distinguish deliberate user navigation from an automated redirect.
  - **Cryptographic Integrity Seal (`evidence_sha256`):** A SHA-256 digest computed across the incident image, trigger record, timestamp, and workstation identifier at capture time. This seal establishes **tamper-evidence**—verifying that the stored record has not been altered after capture—rather than acting by itself as proof of user intent.

- **Advisory Indicators & Mandatory Human Review:** Automated alerts, classification scores, and trigger records are technical indicators designed to assist school leadership; they are not infallible disciplinary determinations. Authorized school staff must review incident context before taking disciplinary action, and any false-positive or misattributed record may be dismissed, corrected, or deleted inside the institutional console.

4.5 Ephemeral Local Clipboard Risk Flagging

- **Data Processed:** Local clipboard monitoring runs at throttled intervals strictly inside volatile RAM to flag high-risk bulk sensitive-data copy patterns via boolean status indicators.
- **Strict Minimization:** Plaintext clipboard history is never uploaded to cloud servers or attached to incident records.

4.6 Optional Camera Still Capture (Disabled by Default)

- **Default State:** Camera capture capability is **disabled by default** across all standard institutional deployments.
- **Strict Governance Gate:** Camera capture cannot be enabled by teaching staff or assistants. Activation is restricted strictly to an authorized `Principal` or `Admin` role and requires execution of a formal **School Fiduciary Declaration** confirming parental disclosure and institutional necessity for physical security or anti-tampering governance. Even where explicitly activated by a school, capture is limited to a single still frame upon critical alerts; Obylon never records continuous video or audio.

4.7 Institutional Staff Accounts & Administrative Accountability Logs

- **Data Processed:** Staff display name, assigned role (`Principal`, `Admin`, `Teacher`), institutional email address, phone number (if OTP authentication is enabled), MFA/TOTP status, authentication session metadata (IP address, browser/device metadata, timestamps), and an immutable log of every administrative action executed (such as activating Focus Mode, freezing a terminal, or initiating a laboratory shutdown).
- **Purpose:** Enforce role-based access control, secure administrative access, and maintain a complete accountability trail of every staff intervention.

4.8 Optional Institutional Case Dossiers

- **Data Processed:** Authorized school staff may optionally associate an incident record with a student's name, class, section, and administrative remarks inside the institution's private console for internal disciplinary documentation.

- **Minimal Identity Requirement:** Obylon endpoints do not require Aadhaar numbers, residential addresses, personal mobile numbers, financial records, or biometric templates to operate.

05

PROCESSING BOUNDARIES

5. Architectural Processing Boundaries & Prohibitions

By technical design and binding institutional contract, Obylon strictly excludes the following practices:

1. **No Personal Device Deployment:** Obylon operates solely on institution-owned laboratory computers and is never installed on personal student, parent, or staff mobile phones or home devices.
2. **No Continuous Keylogging or Cross-Session Typing Archives:** Obylon never performs continuous keystroke logging, never archives general typing, essays, or passwords across windows or user sessions, and never uploads plaintext clipboard histories to cloud databases or third-party artificial intelligence services.
3. **No Audio or Video Surveillance:** Obylon contains no microphone capture, audio recording, or continuous webcam video streaming capabilities.
4. **No Personal Credential or File Harvesting:** Obylon does not collect browser cookies, saved browser passwords, personal file directories, or full browser history databases.
5. **No Cross-Institution Data Commingling:** Institutional records are strictly isolated per subscribing school and are never shared, queried, or aggregated across separate institutions.
6. **No Commercial Monetization or AI Training:** Institutional and student records are never sold, licensed for advertising, or used to train external or internal AI models.

06

SECURITY SAFEGUARDS

6. Technical & Organizational Security Safeguards

SECURITY / CONTROLS

Defense built into the architecture.

01
Transport
TLS 1.2+

02
Access
Role verified

03
Integrity
SHA-256

04
Updates
Signed releases

In alignment with **Rule 6 of the DPDP Rules, 2025**, Umbraxis maintains layered technical and organizational controls across endpoint, transport, and cloud layers:

Security Domain	Implemented Technical & Operational Safeguard
Indian Data Residency & Tenant Isolation	Primary databases, authentication services, and private media storage are hosted in **India (AWS Mumbai region, `ap-south-1`)**. Each school operates within a strictly isolated database environment—currently provisioned as a **dedicated database instance per school**, with strict tenant isolation and database-level Row-Level Security enforced across any future multi-tenant scaling.
Encryption in Transit	All communications between laboratory endpoints, administrative consoles, and cloud infrastructure are encrypted via **TLS 1.2+ (HTTPS and WSS)**.
Private, Immutable Incident Storage	Incident screenshots are stored exclusively in **private, non-public object storage buckets** with write-once (`no-overwrite`) controls. Authorized staff view media solely through **short-lived, 15-minute cryptographically signed URLs**.
Cryptographic Evidence Integrity	Incident records are sealed at capture time with a **SHA-256 cryptographic digest** to verify authenticity and detect any post-capture alteration.
Hardware-Bound Endpoint Secrets	Workstation authentication tokens and licensing credentials are encrypted at rest using **Windows OS-native machine-scope DPAPI** tied to the specific device. Diagnostic logs redact sensitive credential values.

Security Domain	Implemented Technical & Operational Safeguard
Granular Role-Based Access Control (RBAC)	Enforced simultaneously at the database layer (Row-Level Security) and server-side API layer. `Teacher` roles are scoped strictly to classroom controls (`Focus Mode`, `Freeze`, `Lock`, and `30-second countdown shutdown` providing students time to save open work) within assigned laboratory groups. Institutional policy changes and campus-wide actions are restricted to `Principal` and `Admin` roles. Unprivileged accounts are denied administrative API access (`HTTP 403`).
Authentication & Session Hygiene	Enforces compromised-password screening, short-lived OTP windows (5–10 minutes), TOTP multi-factor authentication support for administrators, restricted origin policies (CORS), and scoped API key architecture.
Signed Supply Chain & Update Integrity	Over-the-air software updates (operator-controlled) are verified locally prior to execution using **ECDSA-P256 cryptographic manifest signatures**, **SHA-256 binary integrity checks**, **Windows Authenticode verification**, and automated atomic rollback upon verification or health failure.

07

SUBPROCESSORS

7. Subprocessors & Cross-Border Processing Transparency

Umbraxis relies on vetted enterprise infrastructure providers to operate Obylon. While primary institutional storage resides in India (`ap-south-1`), certain optional administrative integrations may process limited payloads outside India when enabled by the institution:

Subprocessor	Function & Exact Data Processed	Residency & Contractual Safeguards
Supabase (AWS Infrastructure)	Primary isolated PostgreSQL database, staff authentication, private incident object storage, and serverless administrative APIs.	**India — AWS Mumbai (`ap-south-1`)**. Dedicated per-school isolation today; strict Row-Level Security enforced for any future multi-tenant architecture.
Google Gemini API *(Optional Admin Feature)*	Generates structured incident summaries *only* when manually invoked by an authorized school administrator. Receives **exclusively** minimized incident summary metadata (policy category, redacted session-scoped trigger input, event timeline context, and staff remarks). Never receives continuous keystroke logs, cross-session typing history, or plaintext clipboard contents.	Optional integration operated strictly under commercial API terms that prohibit model training on API payloads; subject to Google Cloud/API processing regions. Schools may disable AI summarization entirely at contract or console level.
Resend	Transmits institutional staff onboarding invitations and essential administrative account emails. Not used for routine student violation blasts.	Processes staff business email addresses and account notification templates only.
Telegram / Firebase Cloud Messaging *(Optional Admin Alerts)*	Delivers real-time administrative notifications or staff OTP messages *only* when explicitly enabled and configured by the school administrator.	Opt-in notification channel; subject to provider global messaging infrastructure.
Software Distribution Infrastructure (GitHub Releases / Microsoft)	Hosts cryptographically signed update bundles and install-time OS runtime prerequisites.	Receives standard connection IP metadata during software updates only; **never receives student, laboratory, or telemetry data**.

Umbraxis maintains written data protection obligations with subprocessors and notifies institutional administrators prior to onboarding any new core subprocessor.

08

DATA RETENTION

8. Data Retention, Automated Pruning & Verified Erasure

RETENTION / TIME-BOUND CONTROLS

30 DAYS	01 YEAR	30 DAYS
Incident media	**Security audit logs**	**Contract termination**
Rolling purge	Statutory retention	Institutional erasure*

*Subject to records legally mandated for statutory retention; see the full policy text below.

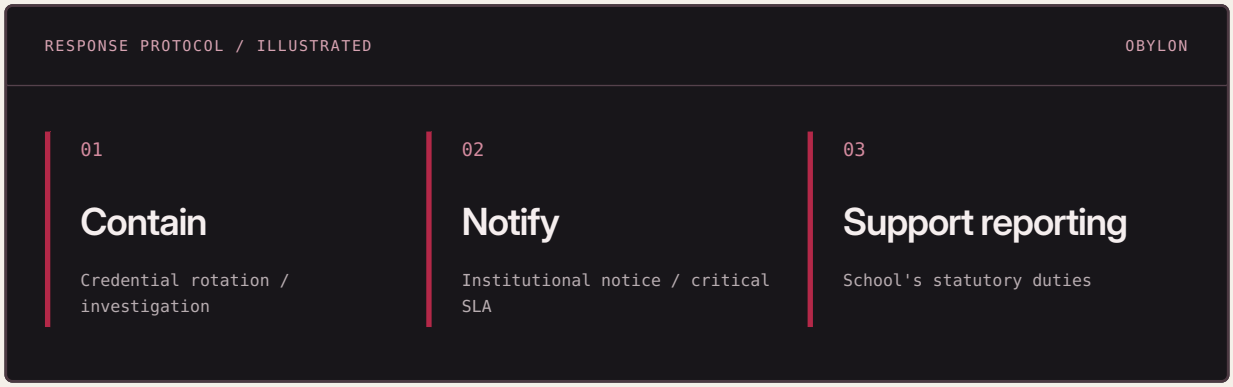
Obylon implements a tiered retention policy that balances **student data minimization** with statutory security-logging mandates under **Rule 6(1)(e) and Rule 8(3) of the DPDP Rules, 2025**:

1. **Incident Screenshots & Disciplinary Dossiers (Default 30 Days):** Incident media and associated case records are retained on a default **30-day rolling schedule** (or a shorter duration configured by the school), unless a longer retention period is required by applicable Indian law or an authorized Principal places a documented disciplinary or legal hold on a specific record. Automated, authenticated pruning routines purge expired database rows and physical storage objects alike.
2. **Minimal Security & Access Audit Logs (1 Year):** Non-intrusive authentication records, administrative command histories, and security access logs—stripped of incident media and student personal content—are retained for **one (1) year** to satisfy statutory DPDP security audit and breach-investigation requirements, after which they are purged automatically.
3. **Offline Endpoint Buffers & Decommissioning:** Temporary offline synchronization queues (used strictly when a laboratory experiences internet interruption) flush automatically upon reconnection. Uninstalling Obylon from a decommissioned workstation removes active services, browser policies, and local operational artifacts.
4. **Contract Termination & Institutional Erasure:** Upon termination of an institutional agreement or verified written instruction from the School Data Fiduciary, Umbraxis permanently deletes the institution's database records and private object storage within **30 days** (excluding records legally mandated for statutory retention) and issues a written **Certificate of Erasure**.

09

BREACH RESPONSE

9. Security Incident & Personal Data Breach Protocol



Umbraxis maintains an active incident response procedure aligned with **Section 8(6) of the DPDP Act, 2023**, the **DPDP Rules, 2025**, and the **CERT-In Cybersecurity Directions, 2022**:

- **Immediate Containment:** Upon identifying any confirmed unauthorized access, integrity anomaly, or security incident impacting institutional personal data, Umbraxis initiates immediate containment, credential rotation, and forensic root-cause analysis.
- **Rapid Institutional Notification (6-Hour Critical SLA):** Umbraxis notifies the affected Educational Institution (Data Fiduciary) **without undue delay upon confirmation—and within 6 hours for critical cybersecurity incidents**—supplying known incident scope, affected data categories, containment actions, and technical remediation evidence. This rapid processor notification enables the institution to meet its own statutory timelines, including **CERT-In 6-hour incident reporting** where applicable, as well as **initial breach intimation and 72-hour detailed reporting** to the **Data Protection Board of India** and affected Data Principals.

10

DATA PRINCIPAL RIGHTS

10. Rights of Parents, Students & Institutional Staff (Data Principals)

Under the **DPDP Act, 2023**, Data Principals—and parents or lawful guardians exercising rights on behalf of minors—are entitled to:

- **Right to Access:** Obtain a clear summary of personal data processed in relation to an identifiable institutional record.
- **Right to Correction & Updating:** Request prompt correction of inaccurate, incomplete, or misattributed case dossier details (including resolution of false-positive alerts).
- **Right to Erasure:** Request deletion of personal records that are no longer necessary for institutional safety, disciplinary review, or statutory retention.
- **Right to Grievance Redressal:** Raise any privacy, fairness, or data-governance concern and receive a timely, documented response.
- **Right to Nominate:** Exercise nomination rights as applicable under the DPDP Act.

How to Submit a Request: Because your school or college is the **Data Fiduciary** that owns institutional records and determines campus policies, parents, students, and school personnel should direct privacy requests to their **School Principal or Institutional Data Officer**. Umbraxis provides rapid technical execution and verification support to every institution to fulfill valid Data Principal requests within statutory timelines.

11

VERIFICATION FAQ

11. Institutional Verification Reference (FAQ)

What is Obylon and who develops it?

Obylon is an institutional computer-laboratory security and endpoint governance platform developed by **Umbraxis**. It is licensed exclusively to schools and educational institutions to maintain safe computing environments, manage classroom focus and examination sessions, and protect institutional workstations.

Where is Obylon's data stored and how is it separated between schools?

All primary institutional databases and incident media are hosted in **India (AWS Mumbai, `ap-south-1`)**. Each subscribing school operates within a strictly isolated database environment—currently provisioned as a dedicated database instance per school, with strict tenant isolation and Row-Level Security enforced for any future multi-tenant deployments—ensuring records are never commingled across schools.

How does Obylon secure data in transit and at rest?

All network traffic is encrypted using **TLS 1.2+ (HTTPS/WSS)**. Incident screenshots reside in private, non-public storage buckets protected against overwriting and accessed solely through **15-minute signed URLs** available only to authenticated school personnel. Each incident artifact is sealed with a **SHA-256 hash** for tamper-evidence, workstation credentials are protected with OS-native machine-scope encryption, and software updates require **ECDSA-P256 cryptographic signatures** and **Windows Authenticode** verification.

Does Obylon run continuous keylogging, record staff passwords, or monitor personal devices?

No. Obylon is deployed strictly on school-owned laboratory workstations—never on personal phones or home computers—and never performs continuous keylogging or plaintext clipboard archiving. Temporary input context stays strictly in volatile local RAM and is automatically wiped every time the active desktop window or browser tab changes, ensuring teacher logins, staff credentials, and

routine classwork are never retained. Only when a real policy violation triggers does Obylon record the redacted trigger search or command from that active window alongside a timestamped event timeline and incident screenshot, which remain subject to human review by school staff.

How does Obylon comply with India's DPDP Act, 2023 and DPDP Rules, 2025?

Obylon operates with the educational institution as **Data Fiduciary** and Umbraxis as **Data Processor** under a binding DPA. Processing is strictly bounded to conditional educational safety and child-protection governance (Section 9 & Fourth Schedule), excludes commercial profiling or advertising, implements Rule 6 technical security safeguards, enforces a 30-day rolling purge on incident media alongside 1-year statutory security log retention, and provides rapid breach notification (within 6 hours for critical incidents) so schools can fulfill both CERT-In and DPDP reporting duties.

12

GOVERNANCE DESK

12. Grievance Desk, Security Disclosures & Policy Governance

For institutional Data Processing Agreements (DPAs), security architecture reviews, vulnerability disclosures, or Data Principal grievances:

- **Publisher / Operator:** Umbraxis
- **Designated Contact:** Privacy & Grievance Desk, Umbraxis
- **Privacy & DPA Inquiries:** `privacy@umbraxis.tclservice.in`
- **Security & Vulnerability Disclosures:** `security@umbraxis.tclservice.in`
- **Operating Jurisdiction:** India (full corporate and registered office particulars are provided directly in each institutional Data Processing Agreement)
- **Acknowledgment SLA:** Written acknowledgment within **48 hours**, with substantive resolution in accordance with DPDP Act, 2023 statutory timelines.

Policy Amendments

Umbraxis reviews this Privacy Policy and Data Governance Framework periodically to reflect architectural enhancements, regulatory updates, or subprocessor changes. Material revisions will be published on this page with a revised **Effective Date**, and institutional administrators will receive direct written notice at least **15 days** prior to material changes taking effect.