POLAR CLOUD

Security & Data Privacy

Enterprise-Grade Protection for Global Education and Manufacturing

CONFIDENTIAL

Issued: Jan 2026
Polar3D, Inc. · polar3d.com
Version 1.0

Executive Summary

Polar Cloud is a secure, cloud-based ecosystem designed to streamline 3D printing and digital manufacturing across education and industry. As a platform serving more than 7,000 institutions in 170+ countries, we understand that our customers entrust us with assets of critical importance: the intellectual property (IP) of enterprise clients and the protected personal information of students and educators.

This document describes the technical controls, compliance frameworks, and architectural safeguards that Polar Cloud maintains to protect the confidentiality, integrity, and availability of customer data. It is intended for CISOs, IT administrators, data protection officers, and procurement teams evaluating Polar Cloud for deployment within security-conscious organizations.

1. Data Encryption & Transport Security

Polar Cloud employs a Defense-in-Depth strategy, applying multiple layers of cryptographic protection so that proprietary design files (STL, OBJ) and machine instructions (G-code) remain protected at every point in their lifecycle — from browser to API to printer.

1.1 Data in Transit

All communication between end-user clients, the Polar Cloud API, and connected 3D printers is encrypted using TLS 1.2 or higher. Legacy protocol versions (TLS 1.0, 1.1, SSL 3.0) are explicitly disabled. Certificate management follows industry best practices, including automated renewal and HSTS enforcement.

1.2 Data at Rest

Design files, user profiles, print histories, and all associated metadata are encrypted at rest using AES-256 — the same standard mandated for US federal government data under FIPS 140-2. Encryption keys are managed through a dedicated key management service and rotated on a defined schedule.

1.3 End-to-End Command Integrity

Printer commands are transmitted exclusively via authenticated, encrypted WebSocket channels. Each command is bound to a scoped API token that limits the action to explicitly authorized users within a given organization. This prevents both unauthorized command injection and lateral access between tenants.

2. Regulatory Compliance & Certifications

Polar Cloud is engineered to exceed the stringent privacy standards required by global enterprises and educational institutions. Our framework aligns with US federal mandates, state-specific student data privacy statutes, and international regulations like GDPR, all verified through rigorous internal controls and independent third-party audits.

Framework	Scope & Applicability
FERPA	Protects the privacy of student education records across all US-based institutional users. Polar Cloud stores, transmits, and processes student data in strict accordance with FERPA's access and disclosure requirements.
COPPA	Ensures verifiable parental consent and robust data protection for users under the age of 13. Polar Cloud enforces age-appropriate data handling controls and limits data collection for younger learners.
GDPR	Provides comprehensive data rights for EU citizens and residents, including the right to access, rectification, and erasure. Upon a deletion request, Polar Cloud permanently removes all design files and sensitive PII from active production environments. Consistent with security best practices and the “legitimate interest” provisions of GDPR, we maintain a limited, immutable audit log (consisting of name, email, and timestamp) solely to document the account’s history and closure. This ensures platform integrity and provides an audit trail for user-initiated account actions, while all other personal data is strictly purged within statutory timeframes.
iKeepSafe	Independent third-party certification verifying Polar Cloud's commitment to digital safety, responsible data practices, and age-appropriate privacy standards in educational environments.

Compliance documentation, audit reports, and certification records are available to qualified enterprise and institutional customers under a signed Non-Disclosure Agreement. Please contact your account representative to initiate a security review.

3. Data Privacy & Sovereignty

Polar Cloud is built on the principle of Data Minimization: we collect only what is strictly necessary to deliver the service, and nothing more. The following policies govern how customer data is handled.

3.1 No Data Commercialization

Polar Cloud does not sell, rent, license, or otherwise trade user data to third parties under any circumstances. Our business model is built entirely on platform value, not data monetization. User data is used solely to provide, maintain, and improve the Polar Cloud service.

3.2 Intellectual Property Ownership

Customers retain 100% ownership of all intellectual property uploaded to or generated within Polar Cloud. Polar3D, Inc. asserts no rights, licenses, or claims — express or implied — over any design files, models, or manufacturing instructions stored on the platform.

3.3 Data Portability & Deletion

Administrative users may export all organization data at any time through the platform's self-service tools. Upon receiving a Full Purge request, Polar Cloud will permanently and irreversibly delete all associated PII, design files, and derivative data from active systems within 30 days, consistent with applicable Data Privacy Agreement (DPA) obligations. Backups containing purged data are overwritten on the next scheduled rotation cycle.

4. Infrastructure & Operational Security

Polar Cloud is hosted on Tier-1 cloud infrastructure — specifically AWS and Google Cloud Platform — inheriting the physical security, redundant power systems, and environmental controls of their SOC 2 Type II and ISO 27001-certified data centers.

4.1 Multi-Tenant Architecture & Isolation

The platform uses strict logical tenant isolation: data, configurations, and print queues belonging to one organization are cryptographically and architecturally separated from all other tenants. Cross-tenant data access is architecturally impossible by design.

4.2 Authentication & Identity Management

Polar Cloud supports Single Sign-On (SSO) through Google, Microsoft, and Clever, enabling districts and enterprises to manage access control through their existing identity providers. This integration ensures that access revocation — upon employee termination or student departure — is propagated to Polar Cloud automatically, eliminating orphaned account risk.

Key authentication capabilities include:

- Federated SSO via SAML 2.0 and OAuth 2.0
- Role-based access control (RBAC) at the organization, school, and user level
- Multi-factor authentication (MFA) support for administrative accounts
- Session token expiry and automatic re-authentication enforcement

4.3 Audit Logging & Forensic Readiness

Polar Cloud maintains immutable, timestamped audit logs covering all print job submissions, file uploads and deletions, administrative configuration changes, and authentication events. Logs are retained for a minimum of 12 months and are available for export to support institutional compliance reporting, security incident investigations, and forensic analysis.

4.4 Vulnerability Management & Incident Response

Polar Cloud conducts regular vulnerability assessments and maintains a formal incident response plan with defined SLAs for identification, containment, and customer notification. Security patches are evaluated on a risk-prioritized basis and applied on an accelerated schedule for critical vulnerabilities.

5. Summary for the Security & Compliance Team

Polar Cloud is engineered to be invisible to your risk profile.

By combining enterprise-grade encryption, adherence to global privacy statutes, and strict data sovereignty controls, we provide an environment where institutional and commercial innovation can scale without compromising the security of your users or the confidentiality of your intellectual property.

In summary:

- AES-256 encryption at rest, TLS 1.2+ in transit, authenticated WebSocket channels for printer commands
- Compliance with FERPA, COPPA, GDPR, and independent iKeepSafe certification; US state-level Data Privacy Agreements (DPAs) in place across multiple states, with scalable opt-in frameworks for additional districts
- Zero data commercialization — your data is your data
- Full IP ownership retained by the customer at all times
- Self-service data export and irreversible Full Purge on request
- SSO integration with Google, Microsoft, and Clever for frictionless access management
- Immutable audit logs with 12-month minimum retention
- Hosted on AWS/GCP Tier-1 infrastructure with SOC 2 Type II and ISO 27001 foundations

For security questionnaires, penetration test reports, or a dedicated architecture review session, please contact: security@polar3d.com