ADVANCED STUDY INSTITUTE OF ASIA
SGT UNIVERSITY

MARCH 2026

LEGAL FRAMEWORK · DATA PROTECTION · CHILD SAFETY · AI PLATFORMS · CONSENT MECHANISMS · PRIVACY RIGHTS

POLICY RESEARCH REPORT

DPDP *Compliance* in Respect to Children's Data

A Comprehensive Assessment of AI Tools Extensively Used by Minors in India

PREPARED BY

Shivani Singh
Program Coordinator for Law & Critical Emerging Technologies, ASIA

Sonal Lalwani
Research Associate - Innovation, Law, Governance, & Creative Economy, ASIA

COVER DESIGN BY

Raghav Sibal
Senior Communications Design Specialist, ASIA

REVIEWED BY

Nainika Sharma
Trust and Safety Compliance,
Electronic Arts (EA)

Neeti Goutam
Senior Research Communications Manager,
ASIA

Table of Contents

Glossary of Key Terms

Definitions of terms used throughout the Report

Term	Definition
AI Platform	Any digital system that uses artificial intelligence to process inputs, generate outputs, or facilitate user interaction, including general-purpose AI tools, social media platforms, and educational technology applications.
Age Verification Mechanism	Any technical or procedural method used by a Data Fiduciary to determine whether a user is a child under the DPDP Act, including self-declaration, document-based verification, or third-party authentication systems.
Behavioural Tracking	The monitoring, collection, or analysis of a child's activity, interaction patterns, or usage behaviour over time, including for personalization, analytics, or profiling, as restricted under the DPDP Act.
Breach Notification	The obligation of a Data Fiduciary to notify the Data Protection Board and affected Data Principals in the event of a personal data breach, in accordance with prescribed procedures and timelines.
Child	An individual who has not completed eighteen years of age, as defined under the Digital Personal Data Protection Act, 2023.
Consent Manager	A person registered with the Data Protection Board who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw consent through an accessible, transparent, and interoperable platform.
Cross-Border Data Transfer	The transfer of digital personal data outside India, subject to restrictions, conditions, or whitelisting mechanisms as may be notified by the Central Government.
Data Fiduciary	Any person who alone or in conjunction with other persons determines the purpose and means of processing personal data.
Data Minimisation	The principle that personal data collected must be limited to what is necessary for the specified purpose of processing.
Data Principal	The individual to whom the personal data relates. In the case of a child, this includes the child acting through their parent or lawful guardian.
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary.
Data Protection Board of India	The statutory authority established under the DPDP Act responsible for enforcement, adjudication of complaints, and ensuring compliance with the Act.
Data Retention and Erasure	The obligation to retain personal data only for as long as necessary for the specified purpose and to erase such data upon fulfillment of the purpose or withdrawal of consent.
Deemed Consent	A form of consent recognized under the DPDP Act under specific circumstances where processing is permitted without explicit consent, subject to statutory conditions.

Digital Personal Data	Personal data in digital form, including data collected online or offline and subsequently digitized.
DPDP Act, 2023	The Digital Personal Data Protection Act, 2023, which governs the processing of digital personal data in India and establishes rights, obligations, and enforcement mechanisms.
DPDP Rules, 2025	The Draft Digital Personal Data Protection Rules, 2025, which operationalize the provisions of the DPDP Act, including procedures for notice, consent, compliance, and enforcement.
Grievance Redressal	The mechanism established by a Data Fiduciary to receive, address, and resolve complaints or requests from Data Principals within prescribed timelines.
Harm (in relation to a child)	Any detrimental effect on the well-being of a child, including physical, mental, psychological, or developmental harm.
High-Risk Processing (Report Context)	Processing activities identified in this report as posing elevated risks to children's privacy or well-being, particularly where they involve tracking, profiling, or sensitive data use.
Multimodal Data	Data collected through multiple input formats such as text, voice, images, video, or sensor-based inputs, often processed simultaneously by AI systems.
Notice (Privacy Notice)	A clear and accessible communication provided by the Data Fiduciary specifying the nature, purpose, and scope of data processing prior to obtaining consent.
Parental Consent (Verifiable)	Consent provided by a parent or lawful guardian for the processing of a child's personal data, obtained through reliable and reasonable verification mechanisms.
Personal Data	Any data about an individual who is identifiable by or in relation to such data.
Processing	A wholly or partly automated operation performed on digital personal data, including collection, storage, use, disclosure, sharing, or erasure.
Profiling	Any form of automated processing used to evaluate, analyze, or predict aspects relating to an individual's behaviour, preferences, or characteristics.
Purpose Limitation	The requirement that personal data be collected and processed only for specific, clear, and lawful purposes, and not used beyond those purposes without fresh consent.
Significant Data Fiduciary (SDF)	A Data Fiduciary notified by the Central Government based on factors such as volume and sensitivity of data processed, risk to Data Principals, and impact on sovereignty or public order.
Third-Party Data Sharing	The disclosure or transfer of personal data by a Data Fiduciary to external entities, including service providers, affiliates, or processors.
User Profiling	The creation of structured representations of user behaviour and preferences based on collected data, typically used for personalization or targeted recommendations.

Verifiable Consent Mechanism	A consent framework that incorporates identity validation or authentication measures sufficient to ensure that consent is provided by an authorized individual.

List of Abbreviations

Abbreviation	Full Form
AI	Artificial Intelligence
COPPA	Children's Online Privacy Protection Act
DPDP	Digital Personal Data Protection
EU	European Union
GDPR	General Data Protection Regulation
GDPR-K	GDPR-Kindergarten, GDPR for children in the EU context
OTP	One-Time Password
ExIF	Exchangeable Image File Format
URL	Uniform Resource Locator
UK	United Kingdom
US	United States
X	X platform, formerly known as Twitter
UI	User Interface
API	Application Programming Interface

Executive Summary

This document examines widely used AI tools among minors in India and evaluates their compliance with the Digital Personal Data Protection Act, 2023 (DPDP Act). DPDP Act 2023 compliance in India follows a structured, phased implementation of the DPDP Rules 2025 over 18 months, concluding around May 2027. The immediate actions focus on governing bodies, followed by the initial 12-month goals for the implementation of Consent Managers, and a long-term 18-month goal for full operational compliance, including data auditing, consent mechanisms, and breach notifications. This report situates its analysis within this transition timeline, assessing platform preparedness as the statutory deadline approaches.

This report presents a structured, quantitative assessment of fourteen AI platforms extensively used by minors in India, evaluated against the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025. The assessment covers fourteen compliance criteria drawn directly from DPDP Act. Across 196 individual criterion-level assessments (14 platforms × 14 criteria), 71% were found to be outright non-compliant, 16% partially non-compliant, and only 13% relatively compliant. The findings reveal systemic structural misalignment between platform design and India's child data protection framework.

It finds that most platforms are structurally misaligned with India's child data protection standards, particularly on parental consent, behavioural tracking, and safeguards for child well-being. The rapid adoption of AI in education is outpacing regulatory compliance, exposing minors to systemic privacy and developmental risks.

About This Document

This is a policy-oriented analytical report prepared by the Centre for Law and Critical Emerging Technologies at the Advanced Study Institute of Asia. It assesses selected AI tools used by minors through a legal-compliance lens and is intended for policymakers, regulators, EdTech platforms, and researchers working at the intersection of data protection, AI governance, and education.

1. Methodology

Platform Selection

Fourteen platforms were selected on the basis of their documented prevalence among minor users in India, spanning general-purpose AI assistants, social media platforms, educational technology tools, and government-backed learning platforms. The selected platforms are: Gemini, Notebook LM, Khan Academy (Khanmigo), Photomath, SATHEE (IIT Kanpur), DIKSHA (Ministry of Education), Microsoft Math Solver in OneNote, WhatsApp, Instagram, ChatGPT, Perplexity, Claude (Anthropic), Canva, and xAI Grok.

Assessment Criteria

Each platform was assessed against fourteen criteria derived from the operative provisions of the DPDP Act and Rules:

- Parental consent for processing children's data
- Processing likely to harm child well-being
- Behavioural tracking and monitoring prohibition
- Data collection and purpose limitation
- Data retention and deletion obligations
- Cross-border data transfer safeguards
- Grievance redressal and accountability
- Prohibition on targeted advertising directed at children
- Notice and language accessibility
- Age threshold discrepancy
- Webcam/camera access consent
- Consent withdrawal mechanism
- Data shared with third parties and parental control
- Voice/audio recording consent

Scoring Framework

Each platform-criterion combination was assigned one of three ordinal ratings based on a close reading of the platform's publicly available privacy policies, terms of service, help centre documentation, and product disclosures as of early 2026:

- **Non-compliant (score 2):** The platform's documented practices or policies directly conflict with the relevant DPDP provision, or the platform offers no mechanism whatsoever to satisfy the requirement.
- **Partial / risk noted (score 1):** The platform has some relevant mechanism in place but it falls materially short of the DPDP standard, or the issue is noted as a potential risk.
- **Relatively compliant (score 0):** The platform's documented position is meaningfully closer to the DPDP standard than its peers, though full compliance cannot be confirmed.

The risk score for each platform is calculated as:

Risk Score (%) = (Sum of ratings across 14 criteria) / (14 × 2) × 100

A score of 100% indicates non-compliance on every criterion; 0% would indicate full compliance on every criterion. Platforms are grouped into four risk tiers: Very high (85–100%), High (70–84%), Medium (55–69%), and Low (below 55%).

Limitations

This assessment is based solely on publicly disclosed platform policies and documentation. It does not involve technical auditing, regulatory correspondence, or access to internal platform data. Compliance status may change as platforms update policies or as the DPDP Rules are notified and enforced by the Data Protection Board of India. The user reach index used in Figure 5 is a relative estimate based on publicly available usage statistics and should be treated as indicative rather than precise.

1.1 Risk Tier Classification

Table 1 summarises the risk tier assigned to each platform along with constituent platforms and aggregate risk scores.

Risk Tier	Count	Platforms	Avg Score
Very High Risk	6	Instagram, xAI Grok, WhatsApp, ChatGPT, Perplexity, Canva	89–100%
High Risk	4	Gemini, Notebook LM, MS Math Solver, Claude	79–86%
Medium Risk	3	Khan Academy, Photomath, SATHEE	64–75%
Low Risk	1	DIKSHA (Ministry of Education)	46%

Table 1. Platform Risk Tier Summary

Table 2. Individual Platform Risk Scores

Platform	Category	Risk Tier	Score
Instagram	Social	Very high	100%
xAI Grok	Social/AI	Very high	100%
Canva	Design	Very high	100%
ChatGPT	AI	Very high	96%
Perplexity	AI	Very high	96%
WhatsApp	Social	Very high	89%
Gemini	AI	High	86%
MS Math Solver	EdTech	High	86%
Notebook LM	AI	High	82%
Claude	AI	High	79%
Photomath	EdTech	Medium	75%
Khan Academy	EdTech	Medium	71%
SATHEE	EdTech	Medium	64%
DIKSHA	Govt EdTech	Low	46%

1.2 Data Visualizations

Figure 1 - Platform Risk Scores

Figure 1 presents all fourteen platforms ranked from highest to lowest risk score. The horizontal bars encode both the magnitude of non-compliance (bar length) and risk tier (bar colour). The dashed vertical line at 75% marks the boundary between the high and medium tiers.

Instagram, xAI Grok, and Canva achieve the maximum score of 100%, indicating non-compliance or partial compliance on every single assessed criterion. The government-run DIKSHA platform scores the lowest at 46%, consistent with its non-commercial mandate and national educational objectives.

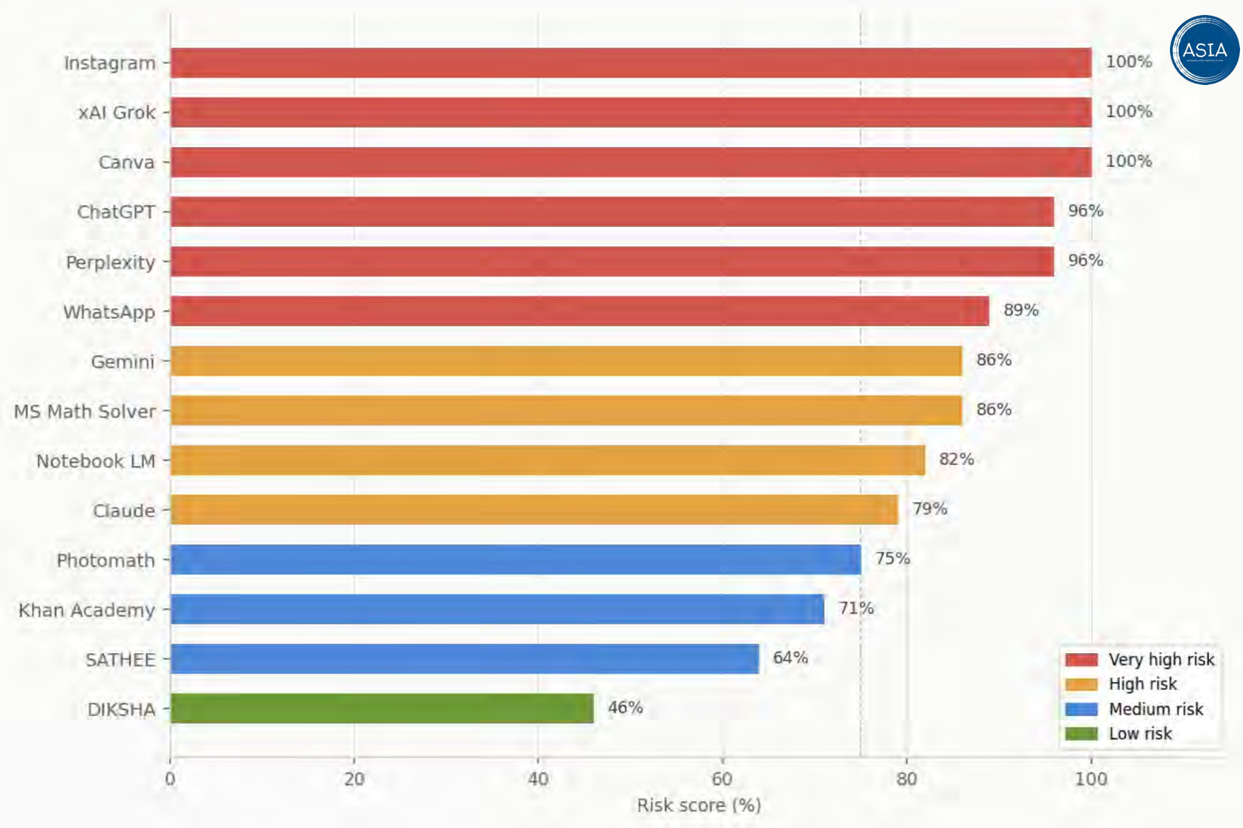

Figure 1. Platform DPDP risk scores (%). Higher = greater non-compliance. Colour denotes risk tier.

Figure 2 - Criteria Failure Rates by Risk Tier

Figure 2 is a radar chart plotting each risk tier's average failure rate across all fourteen DPDP criteria. Each spoke represents one criterion; the distance from the centre represents the percentage of platforms within that tier failing that criterion.

The very high risk tier (red) traces a near-complete circle, with only the advertising criterion showing any deviation. The radar also reveals that tracking and parental consent are universal failures: every tier scores at or near 100% on those spokes, confirming that these are structural industry-wide problems rather than tier-specific issues.

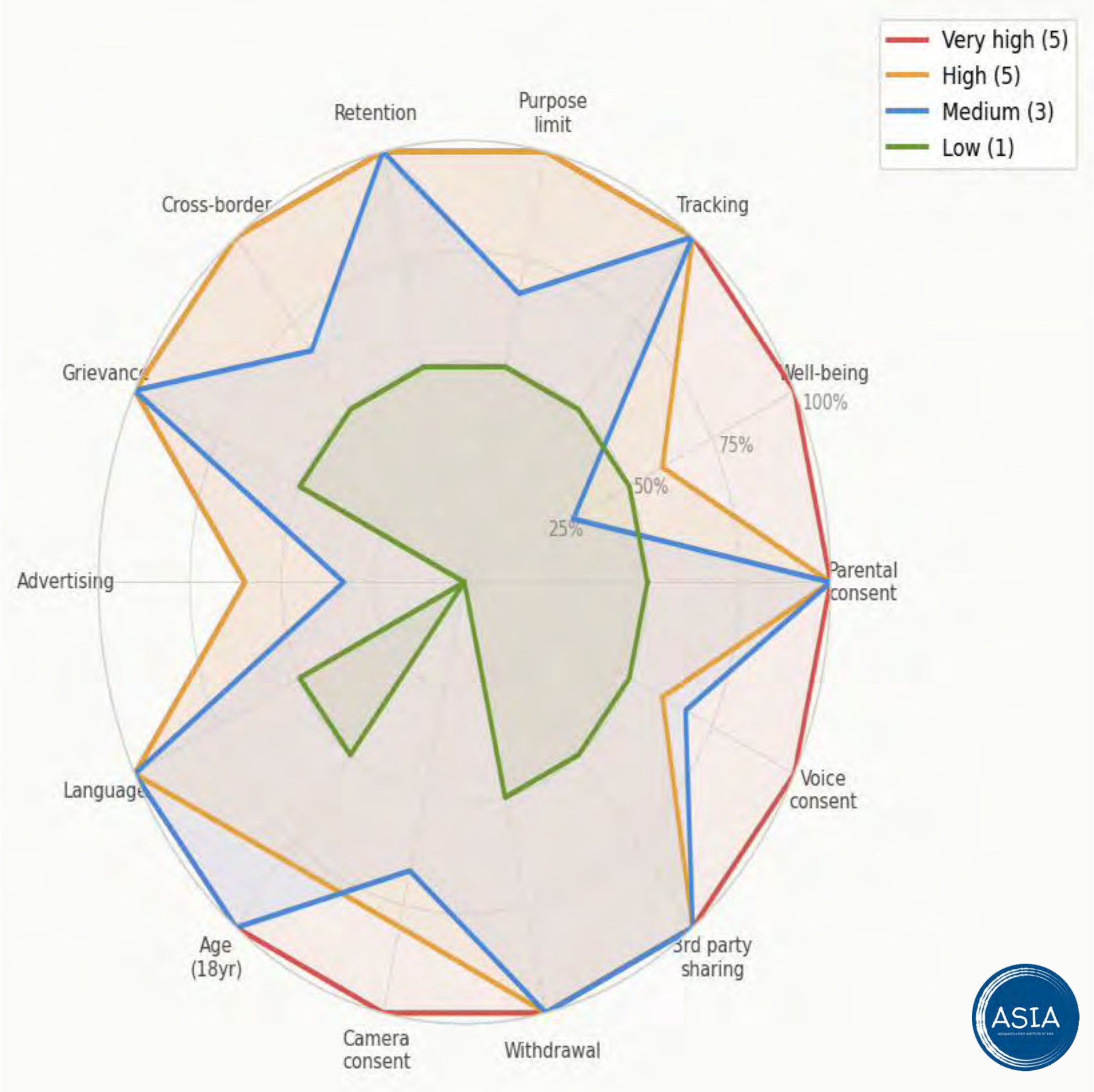

Figure 2. Radar chart of criterion failure rates by risk tier. Outer edge = 100% of platforms in that tier failing the criterion.

Figure 3- Criteria Failure Counts Across All Platforms

Figure 3 shows, for each of the fourteen DPDP criteria, how many of the fourteen platforms were assessed as non-compliant (red) or partially non-compliant (amber).

Five criteria, parental consent, consent withdrawal, grievance redressal, third-party data sharing, and age threshold alignment, are failed by thirteen of fourteen platforms. Well-being protection (Section 9(2)) shows a different profile: zero platforms are outright non-compliant but twelve are partially non-compliant. Targeted advertising presents the only criterion with meaningful variance.

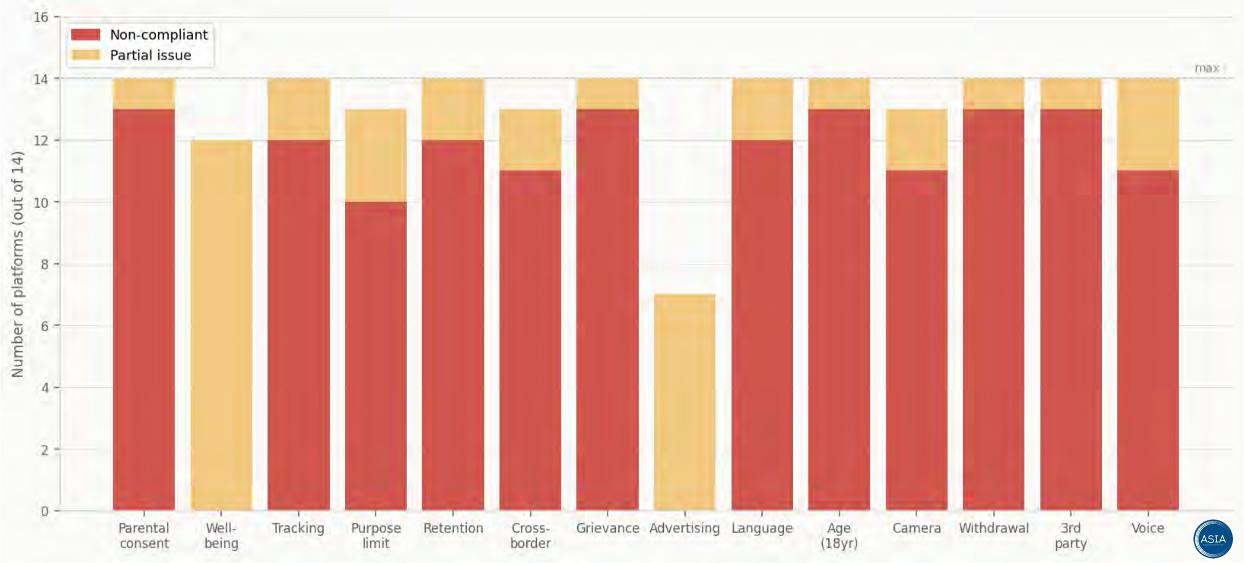

Figure 3. Stacked column chart showing non-compliant (red) and partial (amber) counts per criterion across 14 platforms.

Figure 4 - Overall Compliance Breakdown

Figure 4 presents two donut charts summarising compliance in aggregate. The left chart covers all 196 individual assessments. The right chart compares average risk scores by platform category.

The left donut is stark: 71% of all assessments are outright non-compliant, with only 13% achieving even relative compliance. The right donut reveals a clear gradient by platform type, social and general-purpose AI platforms average an 88% risk score, while EdTech platforms perform meaningfully better at 65%, and the government platform sits at 46%.

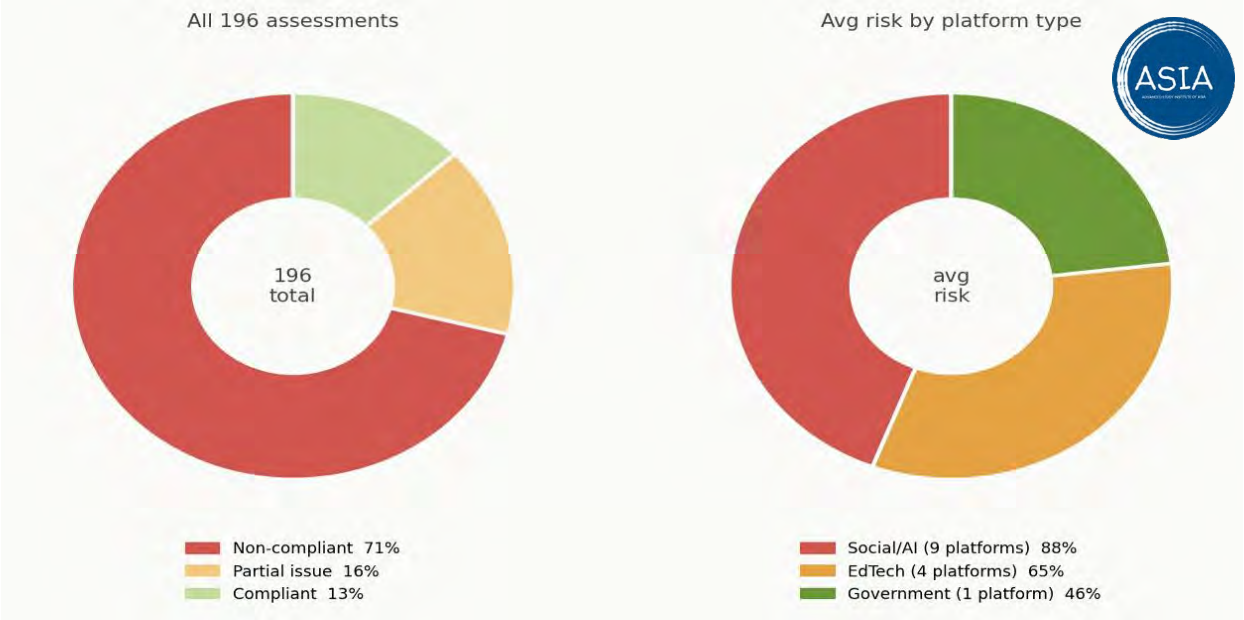

Figure 4. Left: all 196 assessments by compliance status. Right: average risk score by platform category.

Figure 5 - Risk Score vs Estimated Minor User Reach

Figure 5 maps each platform on two axes: risk score (y-axis, higher = worse) and estimated minor user reach in India (x-axis, higher = larger user base among children). Bubble size also encodes reach.

Instagram and WhatsApp occupy the most concerning position: near-maximum risk scores combined with the largest estimated minor user bases in India. DIKSHA is the only platform in the lower-right quadrant (high reach, lower risk), reflecting its government mandate and non-commercial design.

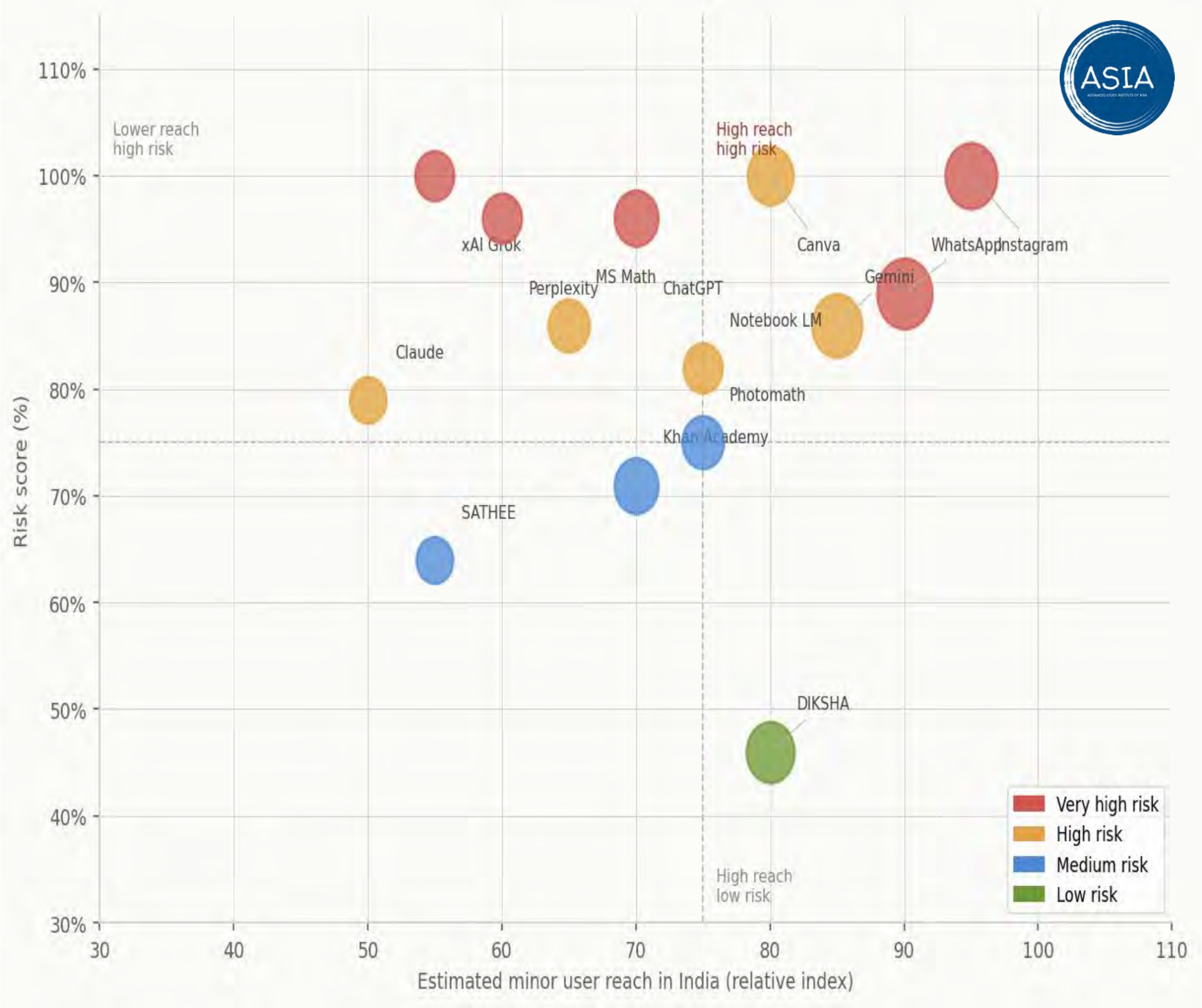

Figure 5. Bubble chart: risk score (y) vs estimated Indian minor user reach (x). Bubble size proportional to reach. Dashed lines at 75% risk and median reach.

Key Findings at a Glance

10 of 14 platforms fall in the very high or high risk tier

5 criteria are failed by 13 or more platforms: parental consent, consent withdrawal, grievance redressal, third-party data sharing, and age threshold alignment

The DPDP Act defines a child as any person under 18; all reviewed platforms use a 13-year minimum, a five-year regulatory gap affecting millions of Indian teenagers

Social media and general-purpose AI platforms average 88% risk versus 46% for the government-run DIKSHA platform

Claude (Anthropic) is the only platform whose stated minimum age of 18 nominally aligns with the DPDP threshold, though enforcement relies entirely on self-declaration

2. Legal Framework: DPDP Act 2023 and Children's Data

The Digital Personal Data Protection Act, 2023 establishes India's first comprehensive data protection regime. Section 9 of the Act contains specific and stringent obligations concerning the processing of children's personal data, operating as a near-absolute constraint on data fiduciaries handling data of users below the age of 18.

2.1 Key Provisions Governing Children's Data

The Digital Personal Data Protection Act, 2023 (DPDP Act), read with the Draft Digital Personal Data Protection Rules, 2025, establishes a structured regulatory framework for the processing of children's personal data in India. The framework imposes heightened obligations on Data Fiduciaries, while also incorporating conditional exemptions and regulatory flexibility through delegated legislation.

- **Definition of a Child**

  Under Section 2(1)(f) of the Act, a child is defined as any individual who has not completed eighteen years of age.

  This definition applies uniformly across all sectors and digital platforms, regardless of differing international standards such as COPPA or GDPR. However, the Act provides flexibility by empowering the Central Government under Section 9(5) to notify a lower age threshold for specific Data Fiduciaries, provided their data processing practices are demonstrably "verifiably safe."

- **Requirement of Verifiable Parental Consent**

Section 9(1) mandates that Data Fiduciaries obtain *verifiable consent* from the parent or lawful guardian prior to processing any personal data of a child.

While the Act does not define the term "verifiable consent," the Draft Rules provide operational clarity. Rule 10 requires Data Fiduciaries to adopt appropriate technical and organizational measures to verify:

- the identity of the parent or guardian; and
- that such individual is an adult.

Verification may be conducted using:

- reliable identity information already available with the Data Fiduciary;
- government-recognised identity credentials; or
- digital identity systems such as Digital Locker or equivalent token-based mechanisms.

➢ Prohibition of Processing Harmful to Children

Section 9(2) imposes a substantive restriction by prohibiting Data Fiduciaries from undertaking any processing of children's personal data that is likely to cause a *detrimental effect on the well-being of a child*.

This provision functions as a **core protective standard** within the framework. Unlike other obligations under Section 9, it is not subject to express exemptions or relaxations, indicating a strong legislative intent to prioritise the best interests and well-being of children.

➢ Restrictions on Tracking, Monitoring, and Targeted Advertising

Section 9(3) prohibits:

- tracking or behavioural monitoring of children; and
- targeted advertising directed at children.

However, this restriction is **not absolute**. Section 9(4) empowers the Central Government to exempt certain classes of Data Fiduciaries or specific purposes from these prohibitions, subject to prescribed conditions.

The Draft Rules further elaborate on such exemptions under Rule 11 read with the Fourth Schedule, thereby allowing limited flexibility for activities such as educational services, safety features, or other child-centric functionalities, provided adequate safeguards are in place.

➢ Recognition of "Verifiably Safe" Data Fiduciaries

Section 9(5) introduces an important regulatory mechanism by allowing the Central Government to designate certain Data Fiduciaries as "verifiably safe."

Such Data Fiduciaries may be exempted, wholly or partially, from the requirements of:

- obtaining verifiable parental consent (Section 9(1)); and
- complying with restrictions on tracking and targeted advertising (Section 9(3)).

➢ Withdrawal of Consent and Data Erasure

Sections 6(4) and 8(7) establish key rights relating to consent and data retention:

- consent must be withdrawable as easily as it is given; and
- personal data must be erased upon withdrawal of consent or when the specified purpose is no longer served, unless retention is required by law.

In the case of children, these rights are exercised by the parent or lawful guardian, who is recognised as the Data Principal for such purposes.

➢ Notice and Transparency Obligations

Section 5 requires Data Fiduciaries to provide a clear and accessible notice at or before seeking consent. Such notice must include:

- the personal data to be processed;
- the purpose of processing;

- the manner of exercising rights; and
- grievance redressal mechanisms.

The notice must be available in English or any of the languages listed in the Eighth Schedule to the Constitution.

The Draft Rules further strengthen this requirement by mandating that notices be:

- presented in clear and plain language;
- independently understandable; and
- sufficiently detailed to enable informed consent.

➢ Grievance Redressal and Accountability

Under Sections 8(10) and 13, Data Fiduciaries are required to:

- establish an effective grievance redressal mechanism; and
- ensure timely response to complaints raised by Data Principals.

Additionally, Data Fiduciaries must publish contact details of a responsible officer to address queries related to personal data processing. The Draft Rules further require disclosure of grievance timelines and mechanisms to ensure accessibility and effectiveness.

➢ Overall Regulatory Approach

The framework governing children’s data under the DPDP Act reflects a balanced and layered regulatory design, comprising:

- Non-negotiable safeguards, particularly the prohibition on harmful processing;
- Conditional obligations, such as parental consent and restrictions on tracking; and
- Regulatory flexibility, enabled through government notifications, exemptions, and rule-based implementation.

EDUCATIONAL EXEMPTIONS AND AI INTEGRATION

The DPDP Act, 2023, read with Rule 11 and the Fourth Schedule (Part A), provides 'carve-outs' for educational institutions. Under Rule 11, institutions are exempt from the Section 9(1) verifiable parental consent requirement and the Section 9(3) ban on tracking for activities strictly limited to educational activities or student safety (e.g., adaptive learning AI or proctoring AI). However, general purpose AI for non-curricular tasks remains subject to standard consent and anti-profiling rules. Critically, Section 9(2) remains an absolute boundary: no exemption permits AI processing that causes a detrimental effect on a child's well-being.

2.2 The Age-Threshold Gap: The Most Pervasive Compliance Failure

The most structurally significant compliance failure across all international platforms reviewed is the mismatch between platform-set minimum ages and India's DPDP threshold. All major international platforms, Google, Meta (Instagram, WhatsApp), OpenAI (ChatGPT), Canva, Perplexity, and xAI (Grok), set minimum ages at 13 years, aligned to the US Children's Online Privacy Protection Act (COPPA). The DPDP Act sets the threshold at 18 years, creating a five-year regulatory gap that affects millions of Indian teenagers who are legally 'children' under Indian law but processed as adults on these platforms.

Anthropic (Claude) and Microsoft (follows regional statutory age) are the only platform reviewed that formally sets its minimum age at 18, nominally aligning with the DPDP threshold. However, this alignment is substantively hollow as it relies entirely on self-declaration at sign-up with no technical enforcement mechanism.

Key Findings

- **Weak and non-verifiable parental consent mechanisms:** Most platforms rely on self-declaration or email-based consent, which falls short of the DPDP Act's requirement for verifiable parental authorization for all users under 18.
- **Inherent conflict between platform design and legal prohibition on tracking:** Core features such as learning analytics, personalization, and usage tracking directly conflict with the Act's prohibition on behavioural monitoring and profiling of children.
- **Emerging risks to child well-being from AI-driven outputs and interactions:** AI systems can generate inaccurate, misleading, or psychologically impactful content, creating risks extending beyond privacy into learning outcomes and mental well-being.
- **Systemic age-threshold discrepancy across all international platforms:** Platforms from Google, Meta, OpenAI, and others set minimum ages at 13 (per COPPA/GDPR-K)

while India's DPDP Act defines a 'child' as anyone below 18, creating a five-year regulatory gap affecting millions of Indian teenagers.

Policy Implications

- **Mandatory Alignment and Corrective Action:** The Data Protection Board of India should issue platform-specific compliance notices to all identified AI data fiduciaries, requiring the immediate initiation of corrective measures and time-bound alignment with the requirements of the DPDP Act and forthcoming Rules. Any deviation from statutory intent in the processing of children's data should be subject to regulatory scrutiny, and transitional status should not be treated as a justification for non-compliance.
- **Enforceable Child Data Safeguards:** All platforms, including international operators, should implement verifiable parental consent mechanisms, age-appropriate design standards, and proportionate age verification systems in a phased but enforceable manner. Technically enforced age-gating aligned with India's 18-year threshold should be adopted, and reliance on self-declaration mechanisms should not be treated as compliant. Deferral, dilution, or superficial compliance should not be permitted beyond the notified implementation framework.
- **Heightened Oversight of Government Platforms:** Government-affiliated platforms such as SATHEE and DIKSHA should function as benchmark compliance models and should be subject to enhanced oversight, including mandatory disclosures, periodic compliance reporting, and demonstrable progress benchmarks. Immediate corrective action should be undertaken to address gaps in age verification and parental consent, and any failure to meet expected standards should trigger review and appropriate intervention.
- **Transparency and User-Centric Compliance Requirements:** Platforms should ensure the availability of regional language interfaces and child-specific privacy disclosures as a baseline compliance requirement to enable informed and meaningful consent. The absence of such measures should be treated as a material compliance deficiency affecting the validity of user consent.
- **Regulatory Clarity, Public Accountability, and Awareness Measures:** The Data Protection Board of India should issue sector-specific guidance on AI platforms and the processing of minors' data, while international platforms should submit India-specific compliance roadmaps with clearly defined milestones. The Government should establish a centralized public compliance dashboard to track platform readiness and adherence to

child data protection norms, and undertake targeted awareness initiatives for parents—particularly young and first-time digital users. The educational exemption under the applicable Rules should be construed narrowly and strictly, and the prohibition under Section 9(2) should operate as an absolute boundary. No exemption should be interpreted to permit AI-driven processing that is detrimental to the well-being of children. A stringent, continuously monitored compliance approach should be maintained to ensure full alignment by May 2027.

- **Grievance Redressal for Child-Specific Complaints** : Platforms should also establish child-sensitive grievance redressal mechanisms and be subject to periodic independent audits to ensure verifiable compliance. Data collection and processing of children's data should be limited to what is strictly necessary for the specified purpose.

3. Platform-by-Platform DPDP Compliance Analysis

The following section provides a detailed compliance assessment of fourteen AI tools extensively used by minors in India. Each platform is evaluated across fourteen DPDP compliance dimensions covering parental consent, child well-being, behavioural monitoring, purpose limitation, data retention, cross-border transfers, grievance redressal, targeted advertising, notice and language accessibility, age threshold, webcam/camera consent, consent withdrawal, third-party data sharing, and voice/audio recording consent.

GEMINI				
SL. NO.	ISSUE (PROVISION)	RULE	RISK ANALYSIS	RISK MITIGATION
1	**Consent of Parents/Lawful Guardian for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Gemini is accessible through Google accounts, including those managed via Family Link. While parental permission is obtained at account creation, there is no clear high-assurance verification mechanism (e.g., ID-based verification) ensuring that consent is truly "verifiable" under DPDP standards.	Introduce robust parental verification mechanisms such as gmail based or mobile-based verification or verified payment authentication before enabling Gemini access for minors.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	Google Gemini generates AI-driven responses that may at times be inaccurate, biased, or not age-appropriate, and minors may rely on such outputs without adequate critical evaluation, creating potential risks to their well-being. However, under Digital Personal Data Protection Act, 2023, Section 9(2) is	Implement strict child-safe response filters, age-adaptive AI outputs, and default "safe mode" for minors that blocks sensitive or harmful content categories. Implement automatic session-end deletion or a 24-hour auto-purge for all minor

			not triggered merely by a child's use of an AI system; it becomes relevant where the processing of a child's personal data goes beyond immediate response generation to enable profiling, behavioural influence, or other outcomes that are reasonably likely to adversely affect the child's well-being.	
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Gemini logs user prompts, interactions, and usage patterns to improve models. This constitutes behavioural profiling, even if anonymized, and may violate the prohibition on tracking minors.	Disable prompt logging, personalization, and usage analytics for minor accounts in India, or process such data only in fully anonymized, non-identifiable form.
4	**Data Collection and Purpose Limitation**	Section 7 requires personal data to be processed only for a specified and lawful purpose.	Gemini may collect input prompts, device data, and interaction metadata for broad purposes like "service improvement" and AI training, which may exceed what is strictly necessary for providing the service to minors.	Limit data collection for minors to strictly necessary inputs for real-time response generation, excluding retention for training or secondary purposes.
5	**Data Retention and Deletion**	Section 8(7) requires erasure once purpose is fulfilled or consent is withdrawn.	Gemini interactions may be retained for training and quality purposes. There is no clear minor-specific retention policy, leading to prolonged storage of sensitive prompts.	Provide automatic deletion of uploaded documents after session completion, along with parent-controlled retention settings and instant deletion options unless the user explicitly opts to retain it for future use.

6	**Cross-Border Data Transfers**	Section 16 allows transfers but requires equivalent protection standards. Under Section 16, the Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such countries or territories outside India as may be specified. Further, under Section 16(2), this provision does not limit or override the applicability of any existing law in force in India that provides for a higher degree of protection or imposes stricter restrictions on the transfer of personal data outside India, whether in relation to specific categories of	Gemini operates on Google's global infrastructure, meaning minor data may be processed and stored across multiple jurisdictions, complicating enforcement of DPDP protections.	Ensure strict contractual safeguards and localization options, with explicit guarantees that minor data receives DPDP-equivalent protection globally.

		personal data, particular Data Fiduciaries, or any class thereof.		
7	**Grievance Redressal and Accountability**	Sections 10(2) and 13 require accessible grievance mechanisms.	Current grievance mechanisms are generic and not child-specific, making it difficult for parents to report AI-related harms affecting minors.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising / Profiling**	Section 9(3) prohibits targeted advertising directed at children.	While Gemini itself may not display ads, interaction data could indirectly feed into Google's broader advertising ecosystem, raising concerns about indirect profiling.	Create a strict data silo, ensuring that Gemini interactions of minors are never used for ad personalization or profiling across Google services.
9	**Notice and Language Accessibility**	Section 5 mandates clear notice in English or any of the 22 scheduled languages.	Privacy disclosures relating to Gemini are fragmented across multiple policies (Google Privacy Policy, AI-specific pages) and may not be easily understandable for parents or available in all required languages. This becomes particularly significant in the Indian context, where linguistic diversity is substantial and digital users often engage with platforms in regional languages; the absence of clear,	Provide a dedicated, simplified "Gemini for Minors" privacy notice, translated at least into any or all 22 scheduled Indian languages with visual explanations. Presently, it is available in 10 languages including English.

			accessible disclosures in multiple vernaculars can undermine informed consent and limit meaningful understanding of how children’s data is collected and processed.	
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Google's own age gate permits Gemini access from age 13 (or with Family Link supervision). India's DPDP Act sets the child threshold firmly at 18, meaning Indian users aged 13–17 can access Gemini without any India-mandated parental consent mechanism being triggered, a five-year regulatory gap that exposes millions of Indian teenagers to unverified AI processing.	Align the India-specific minimum age for Gemini access to 18 years. Mandate Family Link or equivalent parental-approval flow for all Indian users under 18 and implement technical controls that actively prevent 13–17 year-olds from accessing the platform without verified guardian authorisation.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; its collection requires informed, specific, verifiable parental consent for minors, with processing limited to the stated purpose.	Gemini's multimodal features allow real-time camera and image input on Android and the web. For minor accounts, camera access is granted via OS-level device permissions without any separate, Gemini-specific parental-consent prompt. Live visual data, potentially including a child's face and environment, is thus processed by Google's AI systems without DPDP-mandated guardian authorisation.	Implement a mandatory, in-app parental-consent prompt specific to Gemini's camera/image features for Indian minor accounts, over and above any OS permission. Camera data from minor sessions must be processed only for the immediate query, deleted immediately after response generation, and excluded from model training or profiling pipelines.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of	Withdrawing consent for a child's Gemini data processing requires navigating multiple	Create a dedicated, one-step 'Withdraw Consent for Gemini' option within Family

		consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	layers of Google Account settings, Family Link controls, and AI-specific activity dashboards. There is no single, child-account-specific 'Withdraw Gemini Consent' button. Even after withdrawal, prompt logs retained for model-improvement purposes may continue to be held, defeating the purpose of withdrawal under DPDP.	Link and the Google Account safety centre for minor accounts. Withdrawal must immediately cease all Gemini data processing, trigger deletion of retained prompt logs from active and backup systems, and generate a confirmation receipt for the parent, all within the DPDP-prescribed timeframe.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and provided control over such sharing.	Google shares Gemini interaction data with third-party sub-processors (cloud infrastructure, safety vendors, analytics partners) under contractual arrangements governed by Google's global DPA, which has not been specifically assessed for DPDP child-protection compliance. Parents receive no itemised notice of which third parties receive their child's Gemini prompts, nor any mechanism to restrict such sharing beyond full account deletion.	Publish a dedicated, India-specific 'Gemini Third-Party Data Register' for minor accounts listing all sub-processors, the categories of data shared, and applicable safeguards. Provide a parent-facing opt-out mechanism for non-essential third-party sharing. All sub-processor contracts involving minor data must incorporate DPDP-equivalent obligations and be auditable by Indian regulators.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings are personal data and potentially biometric-adjacent; parental consent is required before audio capture from minors;	Gemini's voice interaction mode on Android and Google Assistant captures spoken queries from users, including minors. Voice data is biometric-adjacent (encoding speaker-identification characteristics) and is processed by Google's speech-recognition infrastructure. For	Implement a dedicated, parent-verified in-app consent prompt before voice features are activated on any Indian minor account. Voice data from minor sessions must not be retained beyond the immediate query, excluded from speech-model training, and never used to

		processing must be purpose-limited and session-bound.	minor accounts, no separate DPDP-specific parental-consent step exists for voice feature activation beyond the device microphone permission granted at OS level.	generate voice profiles or biometric identifiers. A parent-accessible log of voice-feature activations must be maintained.

Notebook LM				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Notebook LM operates via Google accounts and allows users to upload personal documents. If accessed by minors, parental consent is assumed through account-level controls, but lacks a direct, verifiable consent mechanism specific to Notebook LM usage.	Implement feature-level parental consent, requiring explicit guardian approval before a minor can upload or process documents within Notebook LM such as gmail based or mobile- based verification or verified payment authentication.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	Notebook LM analyses user-uploaded documents and generates summaries/insights. If minors upload sensitive or harmful content, the AI may reinforce misleading interpretations or expose them to inappropriate material, affecting well-being.	Introduce parental control that they can exercise to ensure content sensitivity filters, contextual warnings, and child-safe summarization modes that avoid harmful or misleading outputs.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Notebook LM logs user queries, document interactions, and usage behaviour to improve performance. This constitutes behavioural monitoring, especially	Disable interaction tracking and analytics for minor accounts or ensure processing is strictly non-identifiable and non-persistent.

			given the depth of interaction with personal documents.	
4	**Data Collection and Purpose Limitation**	Section 7 requires personal data to be processed only for a specified and lawful purpose.	Notebook LM collects uploaded documents, prompts, and interaction metadata, which may include highly sensitive personal data. Use of such data for model improvement or secondary purposes may exceed the original purpose.	Restrict processing to document analysis strictly for user-requested outputs, and prohibit use of minor data for AI training or secondary analytics.
5	**Data Retention and Deletion**	Section 8(7) requires erasure once the purpose is fulfilled or consent is withdrawn.	Uploaded documents and generated insights may be stored for extended periods, with no clear minor-specific retention limits, increasing risks of long-term exposure.	Provide automatic deletion of uploaded documents after session completion or a 24-hour auto-purge, along with parent-controlled retention settings and instant deletion options unless the user explicitly opts to retain it for future use.
6	**Cross-Border Data Transfers**	Section 16 allows transfers but requires equivalent protection standards. Under Section 16, the Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for	Notebook LM relies on Google's cloud infrastructure, leading to cross-border storage and processing of potentially sensitive documents uploaded by minors, raising jurisdictional compliance concerns.	Ensure strict data transfer agreements and DPDP-equivalent safeguards, with an option for data localization for minor accounts in India.

		processing to such countries or territories outside India as may be specified. Further, under Section 16(2), this provision does not limit or override the applicability of any existing law in force in India that provides for a higher degree of protection or imposes stricter restrictions on the transfer of personal data outside India, whether in relation to specific categories of personal data, particular Data Fiduciaries, or any class thereof.		
7	**Grievance Redressal and Accountability**	Sections 10(2) and 13 require a grievance officer and effective redressal.	There is no dedicated grievance mechanism specific to Notebook LM or AI-document processing harms involving minors, making redressal indirect and complex.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour

				acknowledgment window.
8	**Targeted Advertising / Profiling**	Section 9(3) prohibits targeted advertising directed at children.	While Notebook LM itself does not display ads, uploaded document data and interaction patterns could indirectly inform broader profiling ecosystems, especially if integrated with other services.	Enforce a strict data silo, ensuring that no document content or interaction data from minors is used for advertising or profiling across services.
9	**Notice and Language Accessibility**	Section 5 mandates clear notice in English or any of the 22 scheduled languages.	Privacy disclosures for Notebook LM are embedded within broader Google policies, lacking a clear, standalone explanation for document-based AI processing, especially for minors. Privacy disclosures relating to Notebook LM are thus, fragmented across multiple policies (Google Privacy Policy, AI-specific pages) and may not be easily understandable for parents or available in all required languages. This becomes particularly significant in the Indian context, where linguistic diversity is substantial and digital users often engage with platforms in regional languages; the absence of clear, accessible disclosures in multiple vernaculars can undermine informed consent and limit meaningful understanding of how	Provide a dedicated “Notebook LM for Minors” privacy notice, simplified and translated into any or all 22 scheduled Indian languages, with clear explanations of document processing risks. Presently, it is available in 10 languages, including English.

			children’s data is collected and processed.	
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) verifiable parental consent is mandatory for all such users.	Notebook LM inherits Google's general account minimum age of 13, and in some school-managed deployments this is reduced further. The DPDP Act sets the threshold at 18, creating a five-year gap during which Indian students aged 13–17 can freely upload highly sensitive personal documents, study notes, family records, medical information, and have them processed by AI without any India-mandated parental authorisation.	Implement an India-specific age gate that blocks independent Notebook LM access for users declaring an age below 18. All document-upload and AI-processing features must require prior parent-verification for Indian minor accounts, irrespective of whether the account is school-managed or personal.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Notebook LM is primarily document-based, but browser-based access may trigger incidental camera permission requests. More critically, documents uploaded by minors, particularly scanned images, photos of textbooks, or worksheets may embed EXIF (Exchangeable Image Files Format) metadata containing GPS coordinates and device identifiers that constitute personal data collected without any DPDP-specific parental-consent notice targeting the camera/image-capture dimension of the service.	Automatically strip all EXIF (Exchangeable Image Files Format) and embedded metadata from images uploaded to Notebook LM by minor accounts before AI processing. Implement a specific parental-consent disclosure explaining that uploaded images may contain location or device metadata, and provide a one-click 'metadata-free upload' toggle for minor accounts.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as	Notebook LM does not offer a standalone consent-withdrawal flow. A parent wishing to withdraw consent for their child's Notebook	Build a dedicated 'Withdraw Notebook LM Consent' option accessible from the parent's Family Link or Google Account

		giving it; Section 8(7) requires data deletion upon withdrawal.	LM data must navigate Google Account data controls, and even then previously uploaded documents and AI-generated summaries stored in Google's infrastructure may persist in backup systems. There is no confirmation mechanism confirming that Notebook LM-specific document processing has fully ceased.	safety dashboard. Upon withdrawal, all uploaded documents and AI-generated insights associated with the minor's Notebook LM account must be immediately and verifiably purged from active storage and backup systems, with a deletion-confirmation receipt issued to the parent.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Documents uploaded to Notebook LM, which may include children's school assignments, health records, or family correspondence, are processed on Google Cloud infrastructure involving multiple third-party sub-processors (e.g., data-centre operators, security-auditing vendors). Parents and students receive no specific itemised notice of which third parties receive or process the contents of uploaded documents, and have no mechanism to restrict such sharing independently of closing the entire Google account.	Publish a Notebook LM-specific 'Document Sub-Processor Register' for minor accounts listing all entities that access uploaded content, the purpose of access, and applicable data-protection obligations. Provide parents with a granular opt-out for non-essential sub-processing and ensure all relevant contracts incorporate DPDP child-protection standards.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing	Notebook LM's 'Audio Overview' feature generates AI-narrated audio summaries from uploaded documents. While this is currently an output rather than an input-audio feature, it means audio content derived from a minor's uploaded documents is generated and may be	Require explicit parent consent before Audio Overview or any voice-output feature is activated for minor accounts. Audio content derived from a minor's documents must not be stored beyond the session and must not be used to build voice

		must be purpose-limited and session-bound.	played or stored without a specific parental-consent step for audio processing. Any future voice-query integration would further heighten this risk.	profiles or train speech models. Future voice-input features must include a dedicated parental-consent gate before launch.

KHAN ACADEMY (KHANMIGO)				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Khan Academy relies on email-based "acknowledgement" or school-authorized consent. Under the DPDP Act, simple email confirmation may not meet the "verifiable" standard, as it does not strictly confirm the identity of the legal guardian.	Implement stronger verification protocols, such as a small refundable transaction to ensure consent is truly provided by a verified guardian.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	AI-enabled features like Khanmigo analyse student queries. Though safer, it still does not completely eliminate the risk of AI providing inaccurate or discouraging feedback that could impact a child's psychological development or educational confidence.	Implement strict AI safety guardrails, safe-prompt filters, and real-time output monitoring specifically designed to maintain a supportive, age-appropriate educational environment.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Khan Academy tracks learning progress and "mastery" levels to personalize lessons. Under the Act, using these behaviours to algorithmically profile a child's learning habits	Ensure that all personalized learning algorithms are purely functional for curriculum progression and do not track non-educational behavioural traits or

			could be interpreted as behavioural monitoring.	create engagement-driven profiles.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The platform collects technical data and usage logs for "service improvement." If this data collection extends beyond what is strictly necessary for tutoring, it may exceed the "purpose limitation" requirement.	Implement a "Data Minimization" audit and transparency for which the data is used to ensure that for minor accounts, only the bare minimum of data (e.g., username and learning progress) is collected and stored.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Student data is often kept for years to track long-term progress. If an account becomes inactive, the prolonged retention of detailed learning histories poses a risk of data exposure.	Implement automatic archival/deletion policies for inactive accounts and provide parents with a "one-click" account and data purge option. There should also be a measure for routine deletion of student data. Implement an automatic session-end deletion or a 24-hour auto-purge for all minor student data at the end of each session ensuring no permanent digital footprint of the child's queries remains on Khan Academy servers unless the user explicitly opts to retain it for further practice or solving.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	As a US-based non-profit, Khan Academy processes data primarily on US servers. This requires ensuring that the data continues to receive	Adopt Standard Contractual Clauses that specifically mirror DPDP Act protections for Indian students, ensuring that

			DPDP-level protection once it leaves India.	overseas storage does not dilute the user's statutory rights.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Parents may find it difficult to navigate foreign support channels for specific legal requests under the Indian DPDP Act, leading to delays in exercising rights like data correction.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	While Khan Academy is a non-profit and does not show third-party ads, any "internal" marketing or suggestions for paid features (like Khanmigo) to a child could be flagged.	Ensure that no promotional content or upsells for paid products are directed at accounts identified as minors; such communications should be made exclusively to the verified parent account.
9	**Notice and Language Accessibility**	Section 5 requires notice in English or any of the 22 scheduled languages.	While the educational content is multilingual, the full legal Privacy Policy and DPDP disclosures may not be available in all or any of the 22 Indian languages, hindering "informed" consent.	Provide simplified, visual privacy summaries and ensure the specific Children's Privacy Notice is translated into any or all 22 scheduled Indian languages.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for	Khan Academy permits independent registration from age 13 and parent-manage accounts for under 13, aligned with the U.S. COPPA standard rather than India's DPDP threshold of 18.	Update the India onboarding flow to apply an 18-year threshold. All users aged 17 and under registering from India must be routed through a mandatory, DPDP-compliant parental-consent verification step (guardian OTP or

		all such users. irrespective of platform-set minimum age.		small refundable transaction) before any personal data is processed, including learning progress, quiz scores, and usage analytics.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Khan Academy does not currently use webcam input for its core learning or Khanmigo features. However, live-class and tutoring integrations that use third-party video-conferencing tools (e.g., Zoom integrations) may involve video capture of minor students without a specific Khan Academy-level parental-consent mechanism. Any future AI-proctoring or avatar features would amplify this risk significantly.	Publish a clear disclosure to Indian parents specifying that no Khan Academy feature captures video or camera data from minors without a separate, explicit consent step. For any third-party video integration, ensure a dedicated DPDP-compliant parental-consent mechanism is in place before the integration is made available to Indian minor accounts.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Khan Academy provides a general account-deletion mechanism, but consent withdrawal does not automatically trigger deletion of all derived learning data — mastery scores, Khanmigo AI conversation histories, and performance analytics are retained even after a deletion request is submitted. The process involves multiple steps across different settings screens and does not confirm complete data erasure to the parent, failing the DPDP standard of withdrawal being as easy as consent.	Build a dedicated, single-step 'Withdraw Parental Consent' portal for Indian minor accounts accessible from the parent dashboard. Withdrawal must: (a) immediately suspend all data processing, (b) trigger deletion of all student data including AI tutoring histories and learning analytics, (c) confirm completion within the statutory timeframe, and (d) if possible be accessible in all 22 scheduled Indian languages.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties	Khan Academy shares student data with service providers including cloud-hosting, analytics, and email delivery	Publish an India-specific third-party sub-processor list for minor accounts, updated at least

		must be limited to stated purposes; parents must be informed and provided control.	partners. For Indian minor users, these third-party disclosures are governed by Khan Academy's U.S.-centric privacy policy without a DPDP-compliant data-sharing framework. Parents receive no India-specific register of data recipients, and there is no mechanism to opt out of non-essential third-party sharing without closing the student's account entirely.	annually, covering all entities that receive student learning data. Provide a granular parent opt-out for analytics and non-educational third-party sharing. All sub-processor agreements must incorporate DPDP child-protection obligations enforceable under Indian law.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited.	Khanmigo currently operates as a text-based AI tutor; voice input is not a current feature. However, Khan Academy's video lecture library and live-class sessions involve audio streaming to and from minor students' devices. Microphone access granted for these sessions is governed only by device OS permissions, with no separate DPDP-specific parental-consent step for audio capture. Future voice-interactive Khanmigo features would significantly increase this exposure.	Implement a mandatory parent-consent prompt before microphone access is enabled for any Khan Academy feature involving minor accounts. Audio from live-class sessions involving minors must not be recorded or retained without explicit parental consent. For future voice-AI tutoring features, a dedicated DPDP-compliant audio-consent framework must be in place before launch in India.

PHOTOMATH				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before	Photomath collects device identifiers and usage data. For younger users, it often relies on app store age gates or self-declaration. The DPDP Act requires strict verification, and self-certification does not	Photomath should implement stronger parental verification, such as a small, verifiable transaction from a

		processing personal data of a child.	meet the "verifiable" standard in India.	parent's account, to ensure consent is genuinely provided by a parent or legal guardian.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	Automated math solving can lead to academic over-reliance, potentially hindering a child's cognitive development or learning outcomes if the AI provides answers without sufficient conceptual explanation.	Implement "Learning-First" guardrails that prioritize step-by-step explanations over instant answers for minor accounts, and include periodic prompts encouraging independent problem-solving.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Photomath tracks which math problems a user scans to "personalize the experience." Under the Act, monitoring a child’s specific learning gaps and habits to profile them is restricted.	Disable all behavioural profiling for users identified as minors in India. The app should function as a stateless tool for children, where past scans do not influence a persistent behavioural profile and ensure that any personalisation remains session-based, avoiding the creation of long-term learning bias.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and	The app collects precise device information, IP addresses, and scan history. Collecting extensive metadata for "product improvement" may be seen as exceeding	Implement a "Minimum Data" protocol for minors that restricts data collection to the image scanned and the resulting

		lawful purpose.	what is strictly necessary for a math-solving utility.	solution, automatically purging metadata after the session. This is necessary to eliminate long-term learning bias.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Scan histories are often saved to the user's account indefinitely. For a minor, long-term storage of their academic struggles or scan patterns increases the risk of data misuse over time.	Implement automatic archival/deletion policies for inactive accounts and provide parents with a "one-click" account and data purge option. There should also be a measure for routine deletion of student data. Implement an automatic session-end deletion or a 24-hour auto-purge for all minor student data at the end of each session ensuring no permanent digital footprint of the child's queries remains on Photomath servers unless the user explicitly opts to retain it for the next attempt.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Photomath (owned by Google/Meta affiliates) processes data globally. This requires ensuring that Indian minors' data remains protected under DPDP act or equitable	Ensure that all cross-border transfers of Indian minor data are governed by Standard

			standards regardless of where the server is located.	Contractual Clauses that explicitly mandate compliance with the Indian DPDP Act.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal mechanism.	Users are currently directed to a general "privacy@photomath.com" email. This lacks the localized, time-bound accountability required for Data Fiduciaries operating in India.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	Photomath Plus is a paid subscription. Directing "upsell" prompts or marketing "relevant offers" based on a child's scan history could be interpreted as targeted advertising or profiling.	Remove all promotional content and subscription "nudges" from the child’s interface. All monetization-related communications should be directed solely to the verified parent's email.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	While the app supports math in many languages, the formal Privacy Policy is primarily in English, which may prevent non-English speaking parents in India from providing "informed" consent.	Provide a "Privacy at a Glance" summary in any or all of the 22 scheduled Indian languages, using simple icons and plain language to explain what happens to a child's data.

10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Photomath's Terms of Service set a minimum age of 13, reflecting COPPA and GDPR-K norms rather than India's DPDP threshold of 18. Indian students aged 13–17 who use the app to math problems are legal 'children' under Indian law but are processed as adults on Photomath's platform — a systemic gap that affects a substantial portion of the app's Indian user base, many of whom are secondary school students.	Implement an India-specific age gate that treats all users below 18 as children. For Indian users declaring an age between 13 and 17, a mandatory guardian-linked consent step must be completed (parent OTP or verifiable transaction) before camera access and scan features are enabled. The app must not function in data-collection mode for Indian minor users without such verified consent on record.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Photomath's core functionality is entirely camera-dependent — users must scan printed or handwritten math problems using the device camera. For Indian minor users, this camera permission is requested by the app at first launch via an OS-level prompt, with no DPDP-specific parental-consent mechanism. The captured images of handwritten student work — which may include names, school identifiers, and personal annotations — are transmitted to Photomath's servers for AI processing without explicit guardian authorisation.	Implement a dedicated, India-specific in-app parental-consent screen for camera feature activation on minor accounts, separate from the OS permission prompt. This consent must be confirmed by a verified parent before the camera scan feature is first used. Images captured from minor sessions must be processed only for the immediate solution request, deleted from servers immediately after response generation, and

				never retained for training or product-improvement purposes.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Photomath's consent-withdrawal process requires the user to navigate to account settings and manually submit a data-deletion request via email. There is no parent-facing dashboard, no confirmation of which data categories have been deleted, and no timeline commitment for erasure of scan histories, server-side image caches, or learning profiles. This multi-step, opaque process fails the DPDP standard of withdrawal being as accessible as consent.	Introduce a parent-facing 'Revoke Consent and Delete All Data' button within Photomath's app settings for Indian minor accounts. Upon activation, the app must: (a) immediately cease all data processing, (b) delete scan histories and server-side image data within the statutory timeframe, (c) confirm deletion by category to the parent's verified contact, and (d) if possible be accessible in all 22 scheduled Indian languages.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Photomath (now part of the Google ecosystem) shares device and usage data with analytics providers and advertising networks. For Indian minor users, the current privacy policy does not provide a comprehensive India-specific list of third-party data recipients. Parents have no visibility into which entities receive their child's scan data, device identifiers, or learning-pattern analytics, and there is no opt-out mechanism for non-essential sharing short of uninstalling the app.	Publish an India-specific 'Minor Data Sharing Register' listing all third parties that receive data from Photomath's Indian minor users, the categories of data shared, and the contractual data-protection obligations in place. Provide a parent-accessible opt-out for analytics and advertising-related sharing and ensure all such third-party

				contracts incorporate DPDP child-protection standards.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited and session-bound.	Photomath's core interaction is visual (camera-scan), not voice-based. However, integration with voice-assistant ecosystems (e.g., 'Hey Google, solve this with Photomath') can result in incidental voice data capture during problem-initiation commands, and some device configurations may permit background microphone access when the app is open. There is no DPDP-specific parental-consent mechanism for any audio capture associated with Photomath on minor devices.	Publish an explicit disclosure to Indian parents confirming that Photomath does not capture voice or audio input from users and implement technical controls to block microphone access for Indian minor accounts entirely unless a future voice feature is introduced with dedicated DPDP-compliant parental consent. If voice features are added in future, a standalone parent-verified consent step must be mandatory before activation.

SATHEE (IIT KANPUR)

SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	SATHEE allows registration for competitive exam prep. While it records email addresses, it lacks a formal mechanism to verify that the person providing consent is the legal guardian, which is a mandatory requirement	SATHEE should integrate verifiable consent tools, such as small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian.

			for users under 18 in India.	
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	The platform provides high-stakes exam preparation (JEE/NEET). Incessant performance tracking without psychological safeguards could lead to academic stress or burnout, impacting the mental well-being of the minor.	Implement wellness-focused features, such as "forced breaks" after long study sessions and encouraging feedback loops that prioritize learning growth over just high-pressure scores.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	The website logs server addresses, browser types, and pages accessed for "statistical purposes." If this data is used to profile a student's study habits or engagement levels, it falls under restricted behavioural monitoring.	Ensure all logging is strictly anonymized and aggregate. For minor accounts, disable any feature that monitors individual browsing patterns to influence content delivery or profiling.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The policy states it collects IP addresses and server info for general statistics. Collecting granular device and browser data for simple access to educational videos may exceed the "minimum necessary" requirement for a student.	Implement a "Data Minimization" policy for minors, where only the essential login credentials and course progress are tracked, excluding non-essential technical telemetry.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Competitive exam prep is seasonal. If SATHEE retains student data (emails, logs, test scores) indefinitely after the exam cycle ends, it might violate the requirement to delete data once the purpose is fulfilled.	Implement an automatic session-end deletion or a 24-hour auto-purge for all minor student data at the end of each academic/exam cycle generated data in India, ensuring no permanent digital footprint of the child's queries

				remains on SATHEE servers unless the user explicitly opts to retain it for the next attempt.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Being an IIT Kanpur initiative, data is likely localized; however, if third-party cloud or analytics services are used, data might cross borders. This requires ensuring the destination provides equivalent DPDP protection.	Conduct a data localization audit to ensure all minor data remains on sovereign Indian servers or is only transferred to "trusted" jurisdictions with equivalent privacy safeguards.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	The policy provides a generic email (sathee@iitk.ac.in). For DPDP compliance, there must be a designated "Grievance Officer" with a clear, time-bound response mandate for parents and students.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	SATHEE is a government-backed free initiative, which lowers the risk of third-party ads. However, "internal" promotion of specific paid resources or affiliate programs could still be categorized as targeted marketing.	Maintain a zero-advertisement policy for all minor users. Ensure that no data is shared with third-party service providers for the purpose of marketing any external products or services.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	Currently, the privacy statement is provided in English. Given its goal of "democratizing" education across India, the lack of regional language notices prevents "informed" consent for non-English	Provide the Privacy Policy and Consent forms if possible in all 22 scheduled Indian languages, ensuring that students and parents from all regions can

			speaking parents. Few private corporations in India such as (Google and Meta) provide their Privacy and Policy in over 10 languages which is a good step towards democratization of information. The widespread prevalence and accessibility to translation applications make it even more important that information is available in as many languages, formats and modes as possible.	fully understand their data rights and make informed decisions.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	SATHEE applies no formal age gate and targets JEE/NEET aspirants who are typically 16–18 years old — meaning virtually its entire active user base qualifies as 'children' under the DPDP Act. Yet SATHEE's registration form collects only an email address with no age-verification or parental-consent mechanism whatsoever. This is a near-total compliance gap given the platform's demographic reality, and it is particularly acute because the platform is a Government of India initiative that should set the benchmark for DPDP compliance.	Introduce an age-declaration field at registration and route all users declaring an age below 18 through a mandatory DPDP-compliant parental-consent verification step before account activation and data processing commences. As a government platform, SATHEE should publicly commit to and publish its DPDP compliance roadmap.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes	SATHEE does not currently deploy webcam-dependent features.	Publish a clear, India-specific policy commitment that no camera or webcam features will be introduced for

		personal data; collection requires informed, specific, verifiable parental consent for minors.		SATHEE without prior DPDP-compliant parental-consent infrastructure being in place. Any future AI-proctored assessment features must require a standalone parent-verified consent step before camera access is enabled for minor accounts, with proctoring data deleted immediately after the assessment session.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	SATHEE does not publish any dedicated consent-withdrawal mechanism. The only recourse for a parent wishing to withdraw consent for their child's data processing is to send an email to the sathee@iitk.ac.in address, with no confirmed response timeline, no structured data-deletion workflow, and no confirmation receipt. For a government platform processing the academic data of JEE/NEET aspirants, this absence of a structured withdrawal mechanism is a significant DPDP compliance failure.	Implement a dedicated 'Parental Consent Withdrawal' portal on the SATHEE website, if possible accessible in all 22 scheduled Indian languages. The portal must allow parents to: (a) withdraw consent with a single authenticated action, (b) receive confirmation of data deletion within the statutory timeframe, and (c) track the status of their withdrawal request. The platform must appoint a named Data Protection Officer to oversee this process.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes;	SATHEE's privacy policy does not identify specific third-party data recipients or describe what data is shared with them. The platform likely uses third-party analytics tools (e.g., Google Analytics) and	Publish a transparent, India-specific data-sharing register identifying all third parties that receive data from SATHEE, the categories of data

		parents must be informed and given control.	cloud-hosting services that receive student usage data. As a government initiative, this opacity is particularly concerning — parents and students have no means of determining whether their academic data is flowing to commercial entities or being used for purposes beyond exam preparation.	shared, and the purpose. As a government platform, SATHEE should commit to sharing student data only with government-approved entities and should prohibit all commercial third-party sharing. An annual compliance audit by a government-designated body should be made publicly available.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors.	SATHEE's current interface is text and video-lecture based without active voice-input features. However, the platform's live doubt-clearance sessions and webinars involve microphone access from student participants. For a platform whose users are almost entirely minor students, microphone access for live sessions is granted via browser permissions without any DPDP-specific parental-consent mechanism, and it is unclear whether any audio from these sessions is recorded or retained.	Implement a mandatory parental-consent disclosure before any SATHEE feature requiring microphone access is activated for minor accounts, clearly stating whether sessions are recorded, how long recordings are retained, and who has access. Live-session audio must not be retained beyond the session without explicit parental consent. SATHEE should publish a clear audio-data policy if possible in all 22 scheduled Indian languages.

DIKSHA (MINISTRY OF EDUCATION)				
SL. NO.	ISSUE (PROVISION)	RULE	RISK ANALYSIS	RISK MITIGATION
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	DIKSHA allows students to register and provide personal details. While the policy mentions consent, it does not currently outline a "verifiable" mechanism (like Aadhaar OTP or parent-linked accounts) to ensure a parent or legal guardian is providing the authorization.	DIKSHA should integrate verifiable consent workflows, such as linking student profiles to a government-backed identity verification for guardians.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	As a national platform, DIKSHA processes vast amounts of student performance data. There is a risk that competitive ranking or public visibility of progress could lead to academic anxiety or social shaming among minors.	Implement privacy-by-default dashboards for minors where performance data is visible only to the student and verified teachers/parents, ensuring a supportive rather than high-pressure environment.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	DIKSHA logs "Usage Data" including content viewed and time spent. If this is used to build behavioural profiles of students' learning habits, it may violate the absolute ban on tracking children under the Act.	Ensure all usage analytics for minor accounts are strictly anonymized and aggregated. Disable any individual-level behavioural tracking used for "suggested content" or profiling.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The policy indicates collection of IP addresses, browser types, and device IDs. For a public educational resource, collecting granular technical telemetry from children may exceed the	Implement a "Data Minimization" standard for minor accounts, restricting collection to only essential credentials and educational progress, excluding

			"minimum necessary" requirement.	non-functional device metadata.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	DIKSHA retains data even after account termination if there is a "legitimate purpose." For minors, keeping learning data indefinitely creates a long-term risk of data breaches or profiling later in life.	Define clear expiration periods for student data and ensure that "Account Deletion" results in an immediate, total purge from all backups. Implement an automatic session-end deletion or a 24-hour auto-purge for all minor student data at the end of each academic/exam cycle generated data in India, ensuring no permanent digital footprint of the child's queries remains on DIKSHA servers unless the user explicitly opts to retain it for the next attempt.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	While DIKSHA is a national platform, the use of global cloud service providers or third-party CDNs could result in data being processed outside India, requiring strict adherence to DPDP transfer rules.	Conduct a sovereignty audit to ensure that all personal data of Indian minors is stored and processed exclusively on servers located within India, in line with "data stay" preferences for sensitive sectors.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance	Currently, users are directed to a general NCERT email address. The DPDP Act requires a designated "Grievance Officer" and a structured	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-

		redressal process.	process to resolve complaints within a specific timeframe.	related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	DIKSHA is non-commercial; however, "recommendations" for external educational apps or third-party content within the platform could be construed as a form of targeted promotion or marketing.	Maintain a strict "No-Promotion" zone for minor accounts. Any links to external resources must be strictly vetted to ensure they do not lead to commercial or ad-supported environments.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	The content on DIKSHA is available in all 22 scheduled languages. But, the current Privacy Policy is only available only in English. For a platform intended for "teachers and learners across India," the lack of notices in regional languages hinders the ability of many parents to provide informed consent. Further, the privacy policy is inaccessible as it's not available for print or as a pdf document.	Provide the Privacy Policy and Consent Forms if possible in all 22 scheduled Indian languages, using simplified, non-legalistic language to ensure accessibility for all citizens.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	DIKSHA serves students from Class 1 upward, encompassing children as young as 5-6 years old. Its registration framework does not articulate differentiated protections for under-13, 13-17, and 18+ cohorts.	As a Ministry of Education platform, DIKSHA should implement a tiered, Aadhaar-linked age-verification mechanism that identifies all under-18 users at registration and mandates government-backed guardian consent (e.g., parent Aadhaar-OTP or UDISE-linked school

				authorization). This would set a national benchmark for DPDP compliance in the EdTech sector.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	DIKSHA does not actively collect webcam data through its core content-delivery features. However, the platform's integration with live virtual classroom tools and the National Initiative for School Heads and Teachers Holistic Advancement (NISHTHA) programme may involve video-enabled sessions where minor students' faces are captured. No DPDP-specific parental-consent mechanism exists for such video capture, and the platform's privacy policy does not address the camera-access dimension of live sessions.	DIKSHA must publish a clear, parent-accessible disclosure specifying which features or integrated tools involve camera access, for how long any video data is retained, and who can access it. A standalone DPDP-compliant parental-consent step must be implemented before any camera-dependent feature is activated for minor accounts, with session recordings deleted immediately after the live class ends.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	DIKSHA's account-deletion process involves navigating to settings and submitting a request but does not clearly specify what data is deleted versus what is retained under 'legitimate purpose', a term used in the privacy policy without definition. For a government platform collecting data on crores of minor students, the absence of a transparent, structured, parent-accessible consent-withdrawal process with confirmed timelines is a serious governance failure under DPDP.	Implement a dedicated 'Parental Consent Withdrawal' feature on DIKSHA accessible to parents through the platform and via the NCERT helpline, available if possible in all 22 scheduled Indian languages. The mechanism must specify exactly what data is deleted, provide a government-issued deletion confirmation, and ensure that withdrawal triggers deletion from all NDEAR-linked

				systems within the statutory timeframe.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	DIKSHA, operating under the National Digital Education Architecture (NDEAR), may share student performance data with state education departments, partnered EdTech providers under the PM eVidya initiative, and third-party analytics vendors. The privacy policy does not clearly enumerate which third parties receive student data, under what authority, and with what data-protection obligations. Parents have no mechanism to review or restrict the flow of their children's academic data to private EdTech partners.	Publish a comprehensive, publicly accessible 'DIKSHA Data Sharing Register' listing all government departments, state agencies, and private entities that receive student data, the legal basis for sharing, and the applicable protection standards. Parents must be able to opt out of sharing with non-government entities. All private EdTech partners receiving DIKSHA data must sign DPDP-compliant Data Processing Agreements published in the public domain.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors.	DIKSHA's video lectures and live classes involve audio streaming to and from minor students. For primary-school age children (Class 1-5), microphone access during online classes, granted via browser permissions, constitutes audio data collection from some of the most vulnerable users on the platform. The privacy policy does not address whether live-class audio is recorded, retained, or shared with state education authorities, and no parental-consent mechanism exists specifically for audio capture.	Publish a clear, parent-accessible audio-data policy in all 22 scheduled Indian languages specifying: (a) whether live-class audio is recorded, (b) retention period, and (c) who has access. Implement a mandatory parental-consent step before microphone access is enabled for any DIKSHA feature involving minor accounts. Live-session audio must not be retained beyond the session without explicit written parental consent, and any

				retention must be secured in accordance with government data-protection standards.

Microsoft Math Solver in OneNote

SL. NO.	ISSUE (PROVISION)	RULE	RISK ANALYSIS	RISK MITIGATION
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Microsoft relies on the "Microsoft Family Safety" group or school-led "M365 Education" consent. However, the Act requires a "verifiable" standard in India. Simple digital approval by a minor claiming to be an adult or school-wide blanket consent may not meet the strict identity verification requirements for individual guardians.	Microsoft should implement India-specific verification, such as a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian. for parents or linking the minor's OneNote profile to a verified parent's primary Microsoft account with an active identity check.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	Math Solver uses AI to provide instant solutions. There is a risk of creating "educational dependency," where a child's cognitive development and problem-solving resilience are hampered by over-reliance on automated answers without conceptual understanding.	Implement "Learning Scaffolding" modes for minors, where the AI provides hints or conceptual "stepping stones" before revealing the final answer, ensuring the tool supports rather than replaces cognitive effort. This is essential for supporting cognitive development of children.

3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Microsoft collects "Diagnostic Data" and "Connected Experience" data to understand how features are used. Tracking a child's specific math errors or frequency of tool usage to "personalize" the solver's AI constitutes behavioural monitoring under the Act.	Disable all personalized behavioural tracking for minor accounts in India. Diagnostic data should be strictly anonymized and should not be used to build a persistent profile of a student's learning gaps. This is necessary to eliminate long-term learning bias and student profiling.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	OneNote collects ink data, text inputs, and device telemetry. For a math utility, collecting broad telemetry (like location or other app usage) may exceed the "purpose limitation" for an educational task.	Implement a "Limited Context" protocol for minors, ensuring that Math Solver only accesses the specific mathematical string or image being solved and does not ingest surrounding personal notes or metadata.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Math problems solved in OneNote are stored in the user’s "Recent" history and synced to the cloud indefinitely. For minors, this persistent record of their academic history increases the risk of long-term data exposure.	Implement automatic history-clearing cycles for minor accounts and ensure that deleting a math notebook results in the immediate purging of all associated AI-processed metadata from Microsoft's servers. Implement automatic archival/deletion policies for inactive accounts (e.g., after 2 years of non-use) and provide parents with a "one-click" account and data purge option.

				There should also be a measure for routine deletion of student data. Implement an automatic session-end deletion or a 24-hour auto-purge for all minor generated data in India, ensuring no permanent digital footprint of the child's queries remains on Microsoft servers.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Microsoft processes data in global data centres (often in the US). This requires ensuring that the data continues to receive the same level of protection as mandated by the DPDP Act after it leaves Indian territory.	Utilize Standard Contractual Clauses that specifically mirror DPDP Act obligations for Indian minor data, ensuring that regardless of server location, the user's statutory rights under Indian law remain enforceable.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Users are currently directed to global privacy web-forms. This lacks the localized, statutory accountability required for a Data Fiduciary in India, making it difficult for parents to escalate minor-specific privacy concerns.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	Microsoft's policy states it does not use "content in OneNote" for ads. However, usage of "Connected Experiences" data to suggest other M365 products to a minor could be construed as a	Implement a strict "Commercial Silence" policy for minor accounts, ensuring that no promotional "nudges" or upsells for premium Microsoft services are

			form of targeted internal marketing.	displayed within the Math Solver interface.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	While Microsoft provides a "Privacy for Young People" page, it is primarily in English. The lack of detailed regional language notices for parents in non-urban areas prevents truly "informed" consent under the DPDP Act.	Launch multilingual "Privacy Explainer" modules in all 22 scheduled Indian languages, using simple language and visuals to explain how a child's data is used within the Microsoft ecosystem.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Microsoft's follows different statutory age criteria for different regions. Any children under the statutory age must have a parent manage their account. They mention the different age barriers to create an independent account in their website for M365 accounts.	They should provide easy navigation to their minimum non-parental managed account age in their Privacy Policy so, that this information is easily accessible for everyone using their services.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Microsoft Lens (embedded in OneNote) and the Math Solver's camera-scan function require camera access to photograph mathematical problems from textbooks, worksheets, or whiteboards. For minor users in schools or at home, this permission is granted at the OS level without a separate, DPDP-specific parental-consent prompt. Images captured may contain handwriting, personal annotations, or other contextual data beyond the math problem itself, all processed by	Implement a dedicated, in-app parental-consent screen for the Microsoft Lens and Math Solver camera features on minor accounts registered in India. Camera images must be processed only for the specific math problem, with all metadata stripped, and deleted from Microsoft's servers within the session. Parents must receive a disclosure explaining exactly what visual data is captured and processed.

			Microsoft's AI pipeline without guardian-specific authorisation.	
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Microsoft provides a Privacy Dashboard for managing account data, but consent withdrawal for a minor's OneNote/Math Solver data involves navigating Microsoft's global Privacy Dashboard, a tool not designed for the Indian DPDP context. It lacks India-specific guidance, is not available in regional languages, and does not provide item-level confirmation of what has been deleted from Math Solver specifically versus other M365 services. Parents in India face a practically opaque withdrawal process.	Create an India-specific 'Parental Data Control' page within the Microsoft Family Safety app if possible in all 22 scheduled Indian languages, allowing parents to withdraw consent specifically for Math Solver data processing with a single authenticated action. Withdrawal must trigger deletion of Math Solver history, ink data, and associated AI-processed metadata from all active and backup Microsoft servers, with category-level confirmation issued to the parent.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Microsoft shares OneNote data with its affiliates, enterprise cloud service providers (e.g., Azure sub-processors), and, in limited cases, third-party app developers through the M365 integration ecosystem. For Indian minor users, the breadth of this sharing, including potential access by school IT administrators, third-party educational app integrations, and Microsoft's global sub-processors, is not communicated in a DPDP-specific or parent-friendly manner, leaving families unable	Publish an India-specific 'OneNote Minor Data Sub-Processor Register' listing all entities that may access a minor's Math Solver data, the legal basis for sharing, and the DPDP-equivalent protections applied. Provide a parent-facing opt-out for all non-essential third-party data sharing via a dedicated India-DPDP privacy portal if possible in all 22 scheduled Indian languages.

			to make informed consent decisions.	
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited.	OneNote supports voice dictation for note-taking, a feature commonly used by students to record spoken notes alongside written content. Microsoft's speech-recognition systems process this audio input, which for minor users constitutes biometric-adjacent data. Additionally, Microsoft Teams integrations with OneNote in school environments may involve class recordings accessible within the OneNote ecosystem. No DPDP-specific parental-consent mechanism exists for voice dictation or class-recording access on minor accounts.	Implement a dedicated, parent-verified in-app consent prompt before voice dictation or any audio recording feature is activated on Indian minor accounts. Voice data processed via OneNote's dictation feature must be deleted after transcription and must not be used for speech-model training. Class recordings accessible in OneNote must be subject to school-level parental consent compliant with DPDP standards, with clear retention and access policies disclosed.

WHATSAPP				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	WhatsApp provides parent-managed accounts for children under 13, but does not clearly specify a robust "verifiable consent" mechanism (e.g., Aadhaar/ID-based verification). Reliance on parental linkage via device/account may not meet DPDP's strict standard.	Implement verifiable parental consent mechanisms such as such as a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian.
2	**Processing Likely to Harm**	Section 9(2) prohibits	Features like group chats, unknown contact	Introduce child-safe default settings,

	the Well-being of a Child	processing that may cause detrimental effects on the well-being of a child.	requests, and business messaging expose children to risks such as harassment, spam, or inappropriate interactions despite parental controls.	restrict communication to approved contacts, and deploy AI-based harmful content detection systems.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	WhatsApp collects usage data (activity logs, duration, interaction patterns), which may indirectly enable behavioural profiling of minors even if not used for ads.	Ensure all minor-related analytics are anonymized and aggregated, and explicitly prohibit individual-level behavioural profiling.
4	**Data Collection and Purpose Limitation**	Section 7 mandates processing only for a specified and lawful purpose.	Collection of metadata such as device information, IP address, contact lists, and usage patterns may exceed what is necessary for providing messaging services to minors.	Adopt strict data minimization for minor accounts, limiting collection to essential data only and disabling non-essential telemetry.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	While messages are not stored long-term, other personal data is retained on a case-by-case basis without clear retention timelines, creating long-term risks.	Define fixed retention periods for minors' data and ensure complete deletion (including backups) upon account deletion. Implement an automatic a 24-hour auto-purge for all minor-generated chat logs in India, ensuring no permanent digital footprint of the child's queries remains on WhatsApp servers, and provide parents with a "Clear All History" dashboard for their teen's WhatsApp account.

6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Data sharing with Meta companies and third-party service providers may involve cross-border transfers without clear safeguards specific to minors' data.	Ensure localization or region-specific storage for minors' data and provide transparency regarding international data transfers.
7	**Grievance Redressal and Accountability**	Sections 10(2) and 13 require an effective grievance redressal mechanism.	No dedicated grievance mechanism specifically designed for minors or parents; lack of clarity on timelines and escalation processes.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) prohibits targeted advertising directed at children.	While WhatsApp does not show ads to parent-managed accounts, interactions with businesses may still include promotional or marketing messages.	Prohibit all forms of business-initiated marketing communication for minor accounts and implement strict filtering of promotional content.
9	**Notice and Language Accessibility**	Section 5 requires notice in clear language and accessible formats.	Privacy Policy is complex and primarily in English, limiting comprehension for minors and parents in India, affecting informed consent.	Provide simplified, visual privacy notices and ensure the specific Minor's Privacy Disclosure is available if possible in all 22 scheduled Indian languages. Presently, it is only available in 10 Indian languages.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires	WhatsApp's minimum age is 13 globally (16 in certain EU jurisdictions). India's DPDP Act fixes the child threshold at 18, creating a five-year	Implement India-specific controls that treat all users declaring an age below 18 as children under the DPDP Act, requiring a verifiable

		verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	window in which Indian teenage users aged 13–17 are processed as adults on WhatsApp but are legally 'children' requiring verifiable parental consent under Indian law.	parental-consent step verification before account activation. Teen Accounts functionality, already partially deployed, must be extended to cover all users under 18 in India, not only those under 13.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	WhatsApp requests broad camera access for photo sharing, video calls, and Status updates. For Indian minor users on parent-managed accounts, camera permissions are approved at the device level without a DPDP-specific parental-consent step. Given WhatsApp's function as a primary communication tool for Indian families, minors routinely share camera-captured photos and participate in video calls, visual data transmitted via Meta's servers, without any guardian-specific authorisation for this category of data processing.	Implement a separate, in-app parental-consent prompt for camera and video-call feature activation on Indian minor accounts, distinct from OS-level permissions. Camera-captured content transmitted by minor accounts must not be analysed, retained, or used by Meta's AI systems for content moderation training or product improvement without explicit parental consent specific to each use case.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Withdrawing consent for a child's WhatsApp data processing requires the parent to delete the child's account, an all-or-nothing action that provides no granular control. There is no mechanism for a parent to withdraw consent for specific processing activities (e.g., metadata collection, cross-service sharing with Meta) while retaining basic messaging functionality. This binary approach	Build a parent-facing 'Consent Management' dashboard if possible in all 22 schedule languages within the WhatsApp Family Controls feature for Indian minor accounts, providing granular withdrawal options for: metadata collection, cross-service data sharing with Meta, business messaging access, and AI content analysis.

			fails the DPDP standard of withdrawal being as accessible and granular as the original consent.	Each withdrawal action must be confirmed with a deletion receipt, and withdrawal must take effect immediately without requiring full account deletion.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	WhatsApp explicitly shares data with other Meta companies (Facebook, Instagram) and with business-messaging partners. For Indian minor accounts, contact lists, usage metadata, and interaction patterns are shared across Meta's ecosystem under a unified privacy policy without DPDP-specific parental consent for each category of intra-group and third-party sharing. Parents managing their child's account have no mechanism to opt out of cross-Meta data sharing while retaining WhatsApp access.	Publish a dedicated, India-specific 'Minor Data Sharing Disclosure' for WhatsApp, clearly itemising what data is shared with Meta group companies and third-party business partners. Provide parents a granular opt-out for all non-essential cross-Meta and third-party sharing via the Family Controls dashboard. Intra-Meta data sharing involving minor accounts must require separate DPDP-compliant parental consent.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited and session-bound.	WhatsApp's voice messaging, voice calls, and Status audio features involve extensive microphone access. For Indian minor accounts, voice notes stored on WhatsApp's servers constitute personal data whose retention and processing fall within the DPDP Act's protections. Voice notes from minor accounts may persist in chat histories indefinitely, and it is unclear whether Meta's AI systems process audio content for moderation or	Implement a dedicated parental-consent step for voice messaging and audio-recording features on Indian minor accounts. Voice notes sent by minor accounts must have a default auto-deletion timer (e.g., 24 hours) with parents able to adjust retention settings. Meta must publicly disclose whether AI systems process audio content from minor accounts, and any such processing must

			product-improvement purposes without guardian-specific authorisation.	require explicit parental consent separate from the general account terms.

INSTAGRAM				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children’s Data**	Section 9(1) of the DPDP Act	Instagram currently uses self-declared birthdays and optional "Supervision" tools for users aged 13-17. Under the DPDP Act, "verifiable parental consent" is mandatory for anyone under 18. Relying on a teen's declaration without a technical verification of the parent's identity poses a high legal risk.	Integrate verification in the form of a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian. guardian provides authorization. Make this mandatory for all Indian users under 18 before any data processing begins.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) of the DPDP Act	Instagram’s algorithmic "Explore" and "Reels" feeds may expose minors to content detrimental to their well-being. While "Nudges" exist to encourage switching topics, they may not meet the strict "no harm" standard required by the Act.	Strengthen "Sensitive Content Control" to the most restrictive setting by default for all minor accounts. Implement automated filters tuned specifically to prevent "detrimental effects" as defined by Indian regulatory standards.
3	**Tracking and Behavioural Monitoring**	Section 9(3) of the DPDP Act	Instagram logs "Usage Data," including content viewed and time spent, to build interest profiles for personalized experiences. The DPDP Act strictly forbids tracking or behavioural	Disable all behavioural tracking and individual-level profiling for accounts identified as minors. Re-engineer the feed for minors to be chronological or based only on accounts they

			monitoring of children for any purpose.	actively follow, ensuring analytics are strictly anonymized.
4	**Data Collection and Purpose Limitation**	Section 7 of the DPDP Act	Meta collects extensive telemetry, including device IDs, IP addresses, and browser types, to personalize products. Collecting this granular metadata from children may exceed the "minimum necessary" requirement for a social platform.	Implement a "Data Minimization" standard for minor accounts. Restrict data collection to essential credentials only, excluding non-functional technical telemetry and cross-product tracking.
5	**Data Retention and Deletion**	Section 8(7) of the DPDP Act	Meta may preserve information for "extended periods" even after a user stops using the products. Retaining a minor's social data indefinitely creates long-term risks of profiling or data breaches.	Define clear expiration periods for data belonging to minors. Ensure that "Account Deletion" results in an immediate, total purge from all active systems and backups within the timeframes specified by the Act. Implement an automatic session-end deletion or a 24-hour auto-purge for all minor data in India, ensuring no permanent digital footprint of the child's queries remains on Instagram’s servers.
6	**Cross-Border Data Transfers**	Section 16 of the DPDP Act	Meta processes data across global infrastructure, including servers in the US. This requires strict adherence to DPDP rules regarding countries to which data can be transferred.	Conduct a sovereignty audit to ensure that the personal data of Indian minors is stored and processed in compliance with the "data stay" or transfer restrictions notified by the Indian government.

7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13	Users are currently directed to a global "Privacy Operations" team in the US. The DPDP Act requires a "Significant Data Fiduciary" to have a designated "Grievance Officer" based in India.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) of the DPDP Act	Instagram's core model involves personalizing ads based on collected information. The Act explicitly prohibits "targeted advertising directed at children".	Maintain a strict "No-Targeted-Ad" zone for minor accounts. Ads shown to users under 18 must be purely contextual (based on the content currently being viewed) rather than behavioural.
9	**Notice and Language Accessibility**	Section 5 of the DPDP Act	Instagram's policy is primarily in English. Section 5 requires that every notice be available in English and any of the 22 scheduled languages of India.	Provide the Privacy Policy and consent forms if possible in all 22 scheduled Indian languages. Use simplified, child-friendly language and visual aids to ensure both parents and minors understand their rights. Presently, it is only available in 10 Indian languages.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of	Instagram allows self-declared sign-up from age 13 globally, with 'Teen Accounts' applying only to users who self-declare an age of 13–15. The DPDP Act's 18-year threshold is five years stricter than Instagram's global minimum age, meaning Indian teenagers aged 13–17, who constitute	Adjust the India-specific sign-up flow to apply an 18-year threshold as the default child-protection standard. All users declaring an age below 18 must complete a verified parental-consent step (guardian OTP or ID-linked verification) before any data

		platform-set minimum age.	one of Instagram's largest global demographics, are routinely onboarded, profiled, and targeted by Instagram's algorithmic recommendation systems without any India-mandated verifiable parental consent.	processing, including profile creation, commences. Teen Account restrictions currently applied only to under-15 users must be extended to all under-18 users in India.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Instagram relies extensively on camera access for Stories, Reels, and live filters, which are among the platform's most-used features by Indian teenagers. For minor accounts, camera permissions are granted via OS prompts without a dedicated parental-consent step. Instagram's AI-powered face filters and augmented-reality effects process real-time facial data from minors, data that is biometric-adjacent, without guardian-specific authorisation, and Meta's AI systems may use such imagery for model training and product improvement.	Implement a mandatory, parent-verified in-app consent prompt before camera access is activated for any Instagram feature on Indian minor accounts. Real-time facial and visual data processed by AI filters must not be retained beyond the session, must not be used to build biometric or facial-recognition profiles, and must be excluded from Meta's AI training pipelines unless explicit, separate parental consent is obtained for each such use.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Instagram's Supervision tool allows parents to monitor a teen's account but does not provide a clear 'Withdraw Consent and Delete Data' function. Account deletion, the only definitive withdrawal action, triggers Meta's standard 30-day deactivation period before data is deleted,	Build a dedicated 'Parental Consent Withdrawal' option within Instagram's Supervision feature for Indian minor accounts, enabling granular withdrawal by processing category. Account-deletion-based withdrawal must trigger immediate deactivation and

			with no guarantee of cross-service data being purged simultaneously. Parents have no granular mechanism to withdraw consent for specific Instagram processing activities (e.g., AI content analysis, cross-Meta profiling) while retaining account access.	complete data purge within the DPDP-prescribed timeframe. The withdrawal tool must be accessible if possible in all 22 scheduled Indian languages and must provide a category-level deletion confirmation receipt to the parent.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Instagram/Meta has one of the most extensive third-party data-sharing ecosystems of any consumer platform. Minor account data, including content interactions, facial data from filters, and usage metadata, flows to Meta's advertising partners, data brokers, analytics vendors, and intra-Meta services (Facebook, WhatsApp) under a unified privacy policy that does not differentiate DPDP-specific child-protection obligations for Indian users. Parents have no itemised view of these data flows and no opt-out mechanism beyond full account deletion.	Publish an India-specific 'Instagram Minor Data Sharing Register' itemising every category of data shared about minor accounts, all third-party and intra-Meta recipients, and the legal basis for each sharing arrangement. Provide parents a granular opt-out dashboard, accessible if possible in all 22 scheduled Indian languages, for all non-essential third-party and cross-Meta sharing. Prohibit the use of minor accounts' data in Meta's advertising auction system entirely.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must	Instagram Reels, Stories, and Live features involve active microphone access and audio recording as core product features. For Indian minor accounts, voice and background audio are captured routinely when using these features, not merely as a permission	Implement a parent-verified consent step before microphone access is enabled for any Instagram feature on Indian minor accounts. Audio recorded by minor accounts must not be retained beyond the specific Story, Reel, or Live session without

		be purpose-limited.	but as a functional requirement. Meta's AI systems process audio for automatic captioning, content moderation, and music recognition. All of this constitutes audio data processing from minors without any DPDP-specific guardian-authorisation mechanism.	explicit parental consent. Meta must disclose to Indian parents which AI systems process audio from minor accounts and for what purpose, with a dedicated opt-out for each use case accessible if possible in all 22 scheduled Indian languages.

CHAT GPT				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	OpenAI uses an "Invite a Parent" link-based system for teen accounts. This lacks a high-assurance identity check in the Indian context, as a minor could potentially link to a non-guardian adult account to bypass restrictions, failing the "verifiable" standard.	OpenAI should implement India-specific verification, such as OTP based verification for the parent or a small verifiable transaction, to ensure the linking process confirms a legitimate legal guardianship.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	AI can generate hallucinated or biased content. For a minor, relying on inaccurate AI advice for health, academic, or personal issues poses a risk to their psychological well-being and development.	Implement enhanced "Minor-Safety" filters by default for Indian users under 18, with proactive disclaimers and "human-in-the-loop" nudges when sensitive topics are detected in prompts. They should also include a protocol for Flagging of suicidal or harmful behaviour exhibited by the minor

				to the parent or concerned guardian authority to ensure child safety.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	OpenAI tracks conversation history to "improve the model" and "reference saved memories." Using a child's specific chat patterns to train or personalize AI models constitutes behavioural monitoring, which is prohibited.	Disable "Model Improvement" and "Memory" features by default for minor accounts in India. Training on data from Indian children should be strictly prohibited to ensure no behavioural profiling occurs.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	ChatGPT collects account information, conversation content, and technical metadata. Collecting deep conversational data for "research" purposes may exceed the "minimum necessary" requirement for providing a simple utility to a child.	Implement a "Purpose-Locked" data policy for minors where chat data is used only for immediate response generation and safety filtering, rather than broad organizational research or development.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Conversations are saved in the "Chat History" indefinitely unless manually deleted. For minors, this creates a persistent digital footprint of their private thoughts and queries, increasing long-term privacy risks.	Implement an automatic session-end deletion or a 24-hour auto-purge for all minor-generated chat logs in India, ensuring no permanent digital footprint of the child's queries remains on Chat GPT servers, and provide parents with a "Clear All History" dashboard for their teen's account.
6	**Cross-Border Data Transfers**	Section 16 governs the	OpenAI processes data primarily in the United	Establish Standard Contractual Clauses

		transfer of personal data outside India.	States. This necessitates ensuring that the data continues to receive DPDP-level protection regardless of the server's physical location.	that specifically mirror DPDP Act obligations, ensuring Indian minors' data processed in US data centers remains subject to Indian privacy standards and enforcement.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Currently, privacy queries are handled via global web-forms or emails. This lacks the localized, time-bound accountability required for a Data Fiduciary in India, making it hard for parents to escalate concerns.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	While ChatGPT is ad-free, the platform offers "Plus" subscriptions. Using a teen's usage data to "nudge" them toward a paid subscription could be construed as a form of targeted internal marketing or profiling.	Maintain a "Commercial Silence" interface for minors. All information regarding paid tiers or new commercial features should be communicated only to the verified parent, not the child.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	OpenAI's Privacy Policy available in many Indian and international languages apart from English but an effort should be made to make it available in all 22 scheduled languages considering the diversity and the breadth of the user population from India. This creates a barrier to "informed" consent	Provide illustrated Privacy Notices and FAQs in any or all 22 scheduled Indian languages, ensuring that parents in all regions can clearly understand the implications of their child using generative AI. The Privacy Policy is presently available in multiple Indian languages such as Gujrati, Bengali, Hindi among others.

			for millions of non-English speaking parents across India.	
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	OpenAI's global minimum age for ChatGPT is 13 (or higher where local law requires). OpenAI has begun introducing teen accounts with parental oversight for users aged 13–17, but this system relies on the minor voluntarily disclosing their age and the parent accepting an email link, neither of which constitutes 'verifiable' identity confirmation under the DPDP standard. Indian users aged 13-17 can create ChatGPT accounts and engage in detailed, open-ended AI conversations without any India-mandated verifiable parental authorisation.	Implement India-specific onboarding that enforces the 18-year DPDP threshold, routing all users who declare an age below 18 through a mandatory parent-OTP or government-ID verification step before account activation. Teen account access without verified parental consent must not be permitted for Indian users, regardless of OpenAI's global teen-account rollout architecture.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	ChatGPT's multimodal capabilities (GPT-4o) allow image input including live camera capture on mobile devices. Indian minor users who bypass the age gate can photograph documents, personal spaces, and people, submitting these images to OpenAI's AI processing pipeline, without any DPDP-specific parental-consent mechanism. This is particularly acute given the open-ended nature of	Implement a mandatory, parent-verified in-app consent prompt before image-upload or camera-capture features are enabled on Indian minor accounts. Camera-captured images submitted by minor users must not be retained after the session, must not be used in OpenAI's training datasets, and must not be analysed for purposes beyond the immediate query response. A clear parent-facing disclosure

			ChatGPT interactions, where camera-captured images of exam papers, home environments, or personal materials may be submitted as part of AI queries.	must explain exactly what happens to images submitted by minor accounts.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	OpenAI's current consent-withdrawal process for teen accounts requires the parent to navigate OpenAI's global privacy settings and submit a data-deletion request, a process not specifically designed for the DPDP framework. It lacks India-specific guidance, is not available in regional languages, and does not provide item-level confirmation that all conversational data (including training-pipeline contributions) has been deleted. Parents have no way to withdraw consent for specific processing activities such as model training while retaining ChatGPT access.	Build a dedicated 'Parental Consent Withdrawal' portal for Indian minor accounts if possible available in all 22 scheduled Indian languages. The portal must allow granular withdrawal (e.g., training exclusion, memory deactivation, session-history deletion) and provide a deletion-confirmation receipt within the DPDP-prescribed timeframe. OpenAI must confirm that withdrawal triggers removal from model training pipelines retroactively.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	OpenAI shares ChatGPT user data with cloud infrastructure providers (e.g., Microsoft Azure), safety-auditing partners, and, in some cases, API integration partners. For Indian minor users, conversational data, which may include deeply personal	Publish an India-specific 'Minor Data Sub-Processor Register' for ChatGPT listing all entities that receive or process minor users' conversational data, the purpose of sharing, and the applicable data-protection safeguards. Provide parents a granular opt-out for all non-essential third-party data flows. All

			queries about health, relationships, and academic struggles, flows to these third parties under OpenAI's global DPA without India-specific DPDP child-protection obligations. Parents receive no itemised disclosure of these data flows and have no mechanism to restrict them.	sub-processor contracts involving Indian minor data must incorporate DPDP-compliant child-protection obligations.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited and session-bound.	ChatGPT's Advanced Voice Mode (available on iOS and Android) enables continuous, real-time spoken conversation with the AI. For minor users who bypass the age gate, this means live voice conversations, including emotional tone, personal disclosures, and background audio, are processed by OpenAI's speech-recognition and large language model pipeline without DPDP-compliant parental authorisation. Voice Mode captures audio in a manner that is qualitatively different from text input, it is persistent, ambient, and potentially biometric.	Disable Voice Mode and all audio-input features by default for Indian minor accounts until a dedicated, parent-verified consent step (guardian OTP) has been completed for audio-feature activation. Voice data from minor sessions must not be retained beyond the conversation, must not be used for speech model training, and must never be used to derive voice profiles or speaker-identification markers. Parents must receive a clear disclosure of all Voice Mode processing if possible in all 22 scheduled Indian languages.

PERPLEXITY				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing**	Section 9(1) of the DPDP Act requires	Perplexity generally targets users above 13 (or 16 in some regions) and relies on	Perplexity should implement robust verification for

	Children’s Data	verifiable parental consent before processing personal data of a child.	self-declared age or third-party login (Google/Apple). In India, the DPDP Act requires a "verifiable" standard for anyone under 18, which self-declaration or standard social logins do not satisfy.	Indian minors, such as OTP verification for parents or a small, verifiable payment-based check to confirm legal guardianship.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	As an "Answer Engine," Perplexity provides real-time web-sourced info. There is a risk of providing age-inappropriate search results or "hallucinated" advice on sensitive topics (health/mental safety) that could negatively impact a minor's well-being.	Implement "Minor-Safety Mode" by default for Indian accounts under 18, which triggers stricter content filtering and prioritizes high-authority, child-safe educational sources for its answers.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Perplexity tracks search queries and "Threads" to build a context for future answers. For a minor, using this history to predict interests or "personalize" the AI experience constitutes prohibited behavioural monitoring.	Disable "Personalized AI" and history-based tracking for minor accounts in India. Each session should be treated as "Stateless," ensuring no persistent behavioural profile is developed from the child's queries.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The policy indicates collection of IP addresses, device identifiers, and detailed usage logs. Collecting deep technical telemetry from a minor seeking simple homework help may exceed the "minimum necessary" requirement for the service.	Implement a "Data Minimization" toggle for minor accounts that restricts collection to the specific query text and excludes non-essential metadata like precise location or device hardware specifics.
5	**Data Retention and Deletion**	Section 8(7) requires	Search "Threads" are saved indefinitely in the user's	Implement automatic "Thread Expiry" for

		erasure of personal data once the purpose is fulfilled or consent is withdrawn.	library. For a minor, this creates a permanent digital record of their inquiries, which increases the risk of long-term data exposure or profiling.	minor accounts and provide parents with a simplified dashboard to purge the child's entire search history instantly. This can be done by implementing automatic session-end deletion or a 24-hour auto-purge for all minor-generated chat logs in India, ensuring no permanent digital footprint of the child's queries remains on Perplexity servers.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Perplexity is based in the US and processes data globally. This requires ensuring that the data of Indian minors receives the same level of protection as mandated by the DPDP Act even when stored in foreign data centers.	Adopt Standard Contractual Clauses (SCCs) for Indian users that explicitly mandate DPDP-level protection and provide Indian authorities/parents the right to audit how minor data is handled abroad.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Currently, users must contact a global email (support@perplexity.ai). This lacks the localized, statutory accountability and the 72-hour/time-bound response requirements expected under the DPDP framework.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly	While Perplexity is currently focused on	Maintain a "Commercial

		prohibits advertising directed at children.	subscriptions, any use of search history to "recommend" Pro features or partner products to a minor could be seen as targeted marketing or profiling. Using a teen's usage data to "nudge" them toward a paid subscription could also be construed as a form of targeted internal marketing or profiling.	Silence" policy for minor accounts. All promotional offers for "Perplexity Pro" or third-party integrations should be hidden from the minor and only visible to a verified parent.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	The Privacy Policy is currently a complex legal document in English. To ensure "informed" parental consent for Indian users, the policy must be accessible in regional languages.	Provide simplified "Privacy-at-a-Glance" summaries if possible in all 22 scheduled Indian languages, using icons and plain language to explain exactly what data is collected from the child.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Perplexity's Terms of Service require users to be at least 13 (or 16 in some regions), relying on social login (Google/Apple) or email registration for age verification. In India, the DPDP Act requires the standard to be 18. Indian students aged 13–17 regularly use Perplexity for homework, essay writing, and research, detailed academic queries that reveal educational interests, knowledge gaps, and personal opinions — all processed without any India-mandated verifiable guardian authorisation.	Implement an India-specific age gate requiring all users who declare an age below 18 to complete a DPDP-compliant parental-consent verification before the platform's search and answer features are accessible. Social logins must not be accepted as proxy age verification for Indian minor accounts.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured	Perplexity's mobile app supports image-based search queries where users photograph documents,	Implement a dedicated, parent-verified in-app consent prompt

		imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	textbook pages, or real-world objects to receive AI-generated answers. For Indian minor users, this camera-based input feature is governed only by OS-level permissions with no DPDP-specific parental-consent mechanism. Images of textbook pages, handwritten notes, or classroom materials submitted by minor users are transmitted to Perplexity's servers and processed by its AI pipeline without guardian-specific authorisation.	before image-upload or camera-search features are enabled on Indian minor accounts. Images captured and submitted by minor users must be processed only for the immediate query, deleted from servers immediately after the answer is generated, and never used for AI training or product-improvement analytics. A parent-facing disclosure must clearly explain all image-processing activities if possible in all 22 scheduled Indian languages.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Perplexity does not currently offer a parent-facing consent-withdrawal portal. The only available recourse is account deletion via the app settings, which does not: (a) provide granular withdrawal by data-processing category, (b) confirm deletion of search threads from backup systems, (c) address withdrawal of model-training consent, or (d) offer any India-specific guidance in regional languages. This fails the DPDP standard of accessible and effective withdrawal.	Build a dedicated 'Parental Consent Withdrawal' portal for Indian minor Perplexity accounts if possible in all 22 scheduled Indian languages. The portal must support granular withdrawal (search-thread deletion, personalisation deactivation, model-training opt-out), provide confirmation receipts, and complete all deletion actions within the DPDP-prescribed timeframe. Withdrawal must immediately disable all processing beyond what is strictly required for the session.

13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Perplexity integrates with third-party AI providers (for web search grounding), web-search APIs, and infrastructure partners. For Indian minor users, search queries and associated metadata may be shared with these providers — including the content of academic and personal queries — without a distinct DPDP-specific notice to parents or any mechanism for parents to audit or restrict such third-party data flows. The platform's privacy policy does not itemise third-party recipients accessible to Indian parents.	Publish an India-specific 'Minor Data Third-Party Register' for Perplexity listing all API providers and sub-processors that receive query data from minor accounts, the categories of data shared, and the applicable protections. Provide a parent-facing opt-out for non-essential third-party sharing. All third-party API integrations involving Indian minor data must be governed by DPDP-compliant data-processing agreements.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited.	Perplexity's mobile application supports voice-input search, allowing users to speak queries aloud for transcription and AI processing. For Indian minor users, voice queries submitted to Perplexity constitute biometric-adjacent personal data (encoding speaker characteristics) processed by Perplexity's speech-recognition and AI pipeline without any DPDP-specific parental-consent mechanism. The platform's privacy policy does not specifically address voice data from minor users.	Disable voice-input features by default for Indian minor accounts until a parent-verified consent step has been completed specifically for audio-feature activation. Voice data from minor sessions must not be retained beyond the query response, must not be used for speech-model training, and must not be used to build voice profiles.

ANTHROPIC (CLAUDE)				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Anthropic requires users to be at least 18 years old (or the age of majority). However, there is no robust identity verification to prevent Indian minors from signing up. If a minor creates an account, the platform processes their data without the "verifiable" consent required by Indian law.	Implement Age-Gate verification for the Indian market, requiring government ID or a parent-linked verification process for users under 18 to ensure compliance with the DPDP Act's strict consent mandate. Integrate verification in the form of a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian. guardian provides authorization.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	While Claude is designed with "Constitutional AI" for safety, it may still provide complex or unfiltered information on sensitive topics (e.g., self-harm or restricted substances) if prompted creatively, which could harm a minor's psychological well-being.	Implement "Minor-Specific Constitutional Guardrails" for Indian users, specifically tuned to recognize and redirect queries involving adolescent mental health or safety to official Indian helplines and resources. They should also include a protocol for Flagging of suicidal or harmful behaviour exhibited by the minor to the parent or concerned guardian authority to ensure child safety.

3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Anthropic collects "Usage Data" and "Communication Data" to improve its services and safety. If this data is used to analyse a minor's specific interaction patterns or personality traits, it constitutes prohibited behavioural monitoring.	Disable "Service Improvement" data usage for minor accounts in India. Ensure that conversations with minors are not used to train future iterations of Claude or to create persistent user profiles.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	Anthropic collects account information, messages, and technical metadata. Collecting conversational history for "product development" may be seen as exceeding the minimum necessary data for providing a one-to-one AI response to a child.	Establish a "Purpose-Bound" silo for minor data in India, where information is strictly used for the immediate session and safety monitoring, with no secondary use for commercial or research purposes.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Claude stores chat history for as long as the account is active. For a minor, this creates a long-term archive of personal thoughts and intellectual queries that may be retained longer than is educationally or functionally necessary.	Implement automatic "Chat Expiry" for minor accounts in India, and provide a prominent, simplified "Right to Erasure" button that purges all logs from primary and backup servers. This can be done by implementing automatic session-end deletion or a 24-hour auto-purge for all minor-generated chat logs in India, ensuring no permanent digital footprint of the child's queries remains on Anthropic servers.

6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Anthropic is a US-based company and processes data globally. This requires ensuring that the personal data of Indian minors is handled with the same level of protection required by the DPDP Act when moved across borders.	Utilize Standard Contractual Clauses that explicitly incorporate the Indian DPDP Act’s protections for minors, ensuring that US-based processing does not dilute the privacy rights of Indian students.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Current grievances are directed to a global privacy email. This lacks the localized, time-bound response framework required for Data Fiduciaries in India, particularly regarding the high-priority protection of children.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	While Claude is primarily a subscription or free-tier service without third-party ads, "Pro" version prompts or invitations to join a "Team Plan" to a minor user could be interpreted as targeted marketing.	Suppress all promotional "nudges" and subscription upsells within the interface for minor accounts. Any commercial communications regarding the platform must be sent exclusively to a verified parent.
9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	The Privacy Policy is a sophisticated legal document available in English. This is a significant barrier for non-English speaking parents in India who must understand what they are consenting to for their child.	Provide simplified, visual "Data Facts" labels if possible in all 22 scheduled Indian languages, explaining exactly what information Claude collects and how it is used in a format

				accessible to all parents.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Anthropic formally sets its minimum age at 18, which nominally aligns with the DPDP threshold, making Claude unique among the platforms reviewed in not having a minimum-age gap. However, this formal alignment is substantively hollow: age verification relies entirely on self-declaration at sign-up, with no technical control preventing a 14-year-old from creating an account. The absence of enforcement means Anthropic's nominal compliance provides no meaningful protection for Indian minor users.	Replace self-declaration with a technically enforced age-verification mechanism for the Indian market. Require users declaring an age below 18 to complete government-ID verification or a parent-linked consent flow (guardian OTP to a verified mobile number) before account activation. Periodic re-verification should be implemented to detect accounts where age may have been misrepresented at sign-up.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Claude supports image uploads including camera-captured photos on mobile devices (iOS and Android apps). Indian minor users who bypass the age gate can photograph personal documents, school materials, identity documents, and individuals, submitting these images to Anthropic's AI processing pipeline, without DPDP-mandated parental authorisation. Given Claude's capability for detailed image analysis, the nature and sensitivity of images that may be submitted by minors is broad and potentially significant.	Implement a mandatory, parent-verified consent prompt before image-upload and camera-capture features are enabled on Indian accounts where the declared age is below 18 or age has not been technically verified. Images submitted by minor accounts must be processed only for the immediate session query, deleted from Anthropic's servers immediately after response generation, and explicitly excluded from model training and product-improvement datasets.

12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	Anthropic's current privacy controls allow users to delete conversations and submit data deletion requests, but there is no parent-specific consent-withdrawal portal, no India-specific guidance, and no granular withdrawal mechanism that distinguishes between different categories of processing (e.g., model training vs. safety monitoring vs. session response). Parents of minor users have no dedicated pathway to withdraw consent, and Anthropic does not confirm timelines for deletion of data from backup or training systems.	Create a dedicated, India-specific 'Parental Consent Withdrawal' page for Claude accounts if possible in all 22 scheduled Indian languages. The page must support granular withdrawal by processing category, provide confirmed deletion timelines for active storage and backup systems, and confirm whether and when training-pipeline contributions are removed. Withdrawal must take effect immediately for all non-essential processing.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Anthropic uses third-party infrastructure providers (primarily Amazon Web Services for cloud hosting) and may share data with safety-auditing partners and enterprise API integration partners. For Indian minor users who access Claude without verified parental consent, their conversational data, which may include personal disclosures, academic content, and creative writing, flows to these third parties without DPDP-mandated guardian authorisation. Anthropic's privacy policy does not publish an itemised list of sub-processors accessible to Indian parents.	Publish an India-specific 'Claude Sub-Processor Register' listing all third parties that receive or process minor users' conversational data from India, the categories of data shared, and the applicable DPDP-equivalent obligations. Provide parents a mechanism to opt out of non-essential third-party data flows. All sub-processor contracts involving Indian minor data must incorporate DPDP child-protection standards, and annual compliance audits must be made available to Indian

				regulators upon request.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited and session-bound.	Claude currently operates primarily as a text and image-input interface; dedicated voice-input is not a primary modality at present on most platforms.	Commit publicly to not enabling voice or audio-input features for Claude's Indian platform until a dedicated, DPDP-compliant parental-consent infrastructure for audio data is in place and has been verified by the Data Protection Board. Any future voice features must require parent-verified consent before activation, with voice data deleted after each session, excluded from model training, and processed exclusively for the immediate conversational response.

CANVA				
SL. NO.	**ISSUE (PROVISION)**	**RULE**	**RISK ANALYSIS**	**RISK MITIGATION**
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	Canva Education often relies on school-led consent. For individual users, Canva uses age-gates that can be easily bypassed. The DPDP Act requires a "verifiable" standard for all minors under 18, which school-only or self-declared consent may not legally satisfy for individual accounts.	Implement robust verification mechanisms for Indian users, such as a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian or a portal for guardians to explicitly authorize and link their minor child's design profile.
2	**Processing Likely to Harm the**	Section 9(2) prohibits processing	Canva's "Magic Media" (AI image generation) and community templates	Implement strict AI safety filters and template moderation

	Well-being of a Child	that may cause detrimental effects on the well-being of a child.	could potentially expose minors to inappropriate content or allow them to generate imagery that impacts their mental well-being or digital safety and can have detrimental psychological effects.	specifically for minor accounts, ensuring that generative AI tools and public library searches are restricted to age-appropriate results.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	Canva tracks design preferences, frequently used elements, and tool interactions to provide "Recommended for you" content. Under the Act, using a child's creative habits to build a behavioural profile is restricted. This can also impact the creativity and the freee-will of the child.	Disable "Personalized Recommendations" and interest-based tracking for minor accounts in India. Ensure the interface remains functional without tracking the child's design choices for profiling purposes.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The platform collects technical data, including IP addresses, cookies, and device identifiers for "product improvement" and "marketing." For a minor, collecting metadata beyond what is needed to save a design may exceed the "minimum necessary" rule.	Implement a "Privacy-by-Design" mode for minors that restricts data collection to essential account credentials and design assets, automatically opting them out of all non-functional telemetry.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the purpose is fulfilled or consent is withdrawn.	Design assets and account metadata are often stored indefinitely to allow users to return to their work. For minors, retaining a long-term archive of their creative and personal data increases the risk of identity theft or data misuse.	Implement automatic archival/deletion policies for inactive minor accounts and ensure that "Deleting a Design" results in an immediate and total purge of that asset and its associated metadata from all cloud backups. Implement automatic session-end deletion or

				a 24-hour auto-purge for all minor-generated chat logs in India, ensuring no permanent digital footprint of the child's queries remains on Canva servers.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	Canva is headquartered in Australia and uses global cloud infrastructure (like AWS). This requires ensuring that Indian minors' data is subject to the same protections as the DPDP Act when processed overseas.	Ensure that all cross-border transfers are governed by Standard Contractual Clauses (SCCs) that specifically mandate compliance with the Indian DPDP Act, ensuring legal recourse for Indian guardians regardless of the server location.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Currently, users are directed to a global "privacy@canva.com" address. This lacks the localized, time-bound accountability required to handle the high-priority data rights of children under the Indian framework.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	While Canva does not sell data to third-party advertisers, it uses "internal" marketing to upsell Canva Pro. Using a minor’s design activity to trigger "Pro" feature nudges could be viewed as a form of targeted marketing.	Suppress all promotional upsells and marketing notifications within the minor’s interface. Any communications regarding premium subscriptions or new features must be sent exclusively to the verified parent’s account.
9	**Notice and Language Accessibility**	Section 5 requires notice in English or	While the interface is available in several Indian languages, the formal Privacy Policy is	Provide simplified, multilingual "Privacy Cards" if possible in all or any 22 scheduled

		any of the 22 scheduled languages.	primarily in English. This hinders the ability of many Indian parents to provide the "informed" consent required by law.	Indian languages, using icons and clear language to explain how a minor's creative data is protected.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Canva's general platform minimum age is 13; Canva Education accounts can be provisioned for even younger children via school agreements. The DPDP Act's 18-year threshold means that Canva's large Indian individual user base aged 13–17, who use the platform for school projects, social media content, and creative work, are legal 'children' requiring verifiable parental consent.	Implement an India-specific age-verification layer applying the 18-year DPDP threshold to all individual accounts. For educational institution accounts, school-level authorization must be supplemented by individual guardian consent confirmations meeting the DPDP 'verifiable' standard for each enrolled student. Age gates must not rely solely on self-declaration.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable parental consent for minors.	Canva's design tools extensively use camera access for photo uploads, AI background removal (Magic Eraser, Background Remover), and AI image-generation prompts based on uploaded photos. For Indian minor accounts, camera permissions are managed at the OS level with no dedicated parental-consent mechanism for AI processing of camera-captured imagery, which may include biometric-adjacent facial data captured via Canva's 'present and record' feature, avatar generation, and photo-editing tools.	Implement a mandatory, parent-verified in-app consent prompt before camera access is activated for any Canva AI feature on Indian minor accounts. AI features that process facial imagery (avatar generation, face-swap tools, background removal from portrait photos) must require specific, granular parental consent. Facial data from minor accounts must not be retained, shared with third-party AI vendors, or used to train Canva's AI models.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of	Canva provides general account-deletion tools but does not offer a parent-facing consent-	Build a dedicated 'Parental Consent Withdrawal' feature for Indian minor Canva

		consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	withdrawal portal specific to minor accounts. Withdrawal requires navigating Canva's settings to request account deletion, a process that does not: (a) distinguish between deleting an account and withdrawing consent for specific processing activities, (b) confirm deletion of design assets from Canva's cloud backups, (c) provide an India-specific deletion timeline, or (d) offer regional-language guidance. Parents managing children's Canva accounts face a practically opaque withdrawal mechanism.	accounts if possible in all 22 scheduled Indian languages, providing granular withdrawal options for: AI-feature data use, analytics tracking, third-party sharing, and design-asset cloud storage. Withdrawal must trigger immediate deletion of all associated data from active and backup systems, with a category-level deletion confirmation issued to the parent within the DPDP-prescribed timeframe.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes; parents must be informed and given control.	Canva uses advertising networks (Google Analytics, Meta Pixel), analytics providers, and cloud-infrastructure partners (AWS). For Indian minor accounts, design metadata, usage patterns, and device identifiers flow to these third parties, including Meta's advertising infrastructure, under Canva's general privacy policy without DPDP-specific child-protection obligations. The Meta Pixel integration in particular means that minor users' Canva design activity may feed into Meta's advertising profile without parents being aware or having any opt-out mechanism.	Immediately disable all advertising-network tracking pixels (including Meta Pixel and Google Analytics advertising features) for Indian minor accounts. Publish an India-specific 'Minor Data Sharing Register' listing all third parties that receive data about Canva's Indian minor users, and provide parents a granular opt-out dashboard if possible in all 22 scheduled Indian languages. All sub-processor contracts involving minor data must incorporate DPDP child-protection obligations.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice	Canva's 'Presentations' feature includes a voice-narration recording tool	Implement a dedicated, parent-verified in-app consent prompt before

		recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited.	that allows users to record spoken narration over slides, creating audio content stored on Canva's servers. For Indian minor users creating school presentations, this means spoken voice recordings, potentially identifiable by voice characteristics, are uploaded to and retained by Canva without a DPDP-specific parental-consent mechanism. Additionally, Canva's AI-powered automatic captioning and video features process audio content without guardian-specific authorisation.	voice-narration recording or any audio-capture feature is activated on Indian minor accounts. Voice recordings created by minor accounts must be explicitly tagged as minor-generated content, subject to immediate deletion from Canva's servers upon session completion unless the parent explicitly consents to retention, and excluded from any AI training or product-improvement use. Auto-captioning features that process audio from minor accounts require separate parental consent.

xAI (Grok)

SL. NO.	ISSUE (PROVISION)	RULE	RISK ANALYSIS	RISK MITIGATION
1	**Parental Consent for Processing Children's Data**	Section 9(1) of the DPDP Act requires verifiable parental consent before processing personal data of a child.	xAI primarily provides Grok through the X (formerly Twitter) platform or dedicated apps. If a minor accesses Grok via an X account that lacks verified parental linkage, xAI processes that child's data without the "verifiable" consent mandated by Indian law.	xAI should implement strict age-verification gates for Indian users and require a parent-verified access before allowing any user under 18 to interact with the Grok interface. Implement robust verification mechanisms for Indian users, such as a small, verifiable transaction from a parent's account, to ensure consent is genuinely provided by a parent or legal guardian before

				providing acccess to Grok.
2	**Processing Likely to Harm the Well-being of a Child**	Section 9(2) prohibits processing that may cause detrimental effects on the well-being of a child.	Grok is designed to be age inappropriate questions that other AIs avoid. For a minor, exposure to unfiltered, sarcastic, or mature-themed AI responses could negatively impact their psychological well-being or social development.	Implement a "Safe-Mode" default for minors in India that restricts Grok's personality profile to be purely educational and supportive, filtering out sarcasm or age inappropriate humour that is inappropriate for younger audiences.
3	**Tracking and Behavioural Monitoring**	Section 9(3) forbids tracking or behavioural monitoring of children.	xAI uses interactions to "train and fine-tune" its models. Tracking a child's conversational patterns and using them to refine the AI's behavior or to "understand" the user's personality is a direct violation of the ban on behavioural monitoring.	Exclude all data from Indian minor accounts from the training pipeline. Ensure that Grok does not "remember" or profile a child's past queries to influence the tone or substance of future interactions.
4	**Data Collection and Purpose Limitation**	Section 7 mandates that data be processed only for a specified and lawful purpose.	The policy details collection of account data, message content, and interaction metadata. Collecting granular conversational data for broad "AI research" may exceed the "minimum necessary" requirement for an Indian child seeking a specific piece of information.	Implement a "Minimalist Logging" protocol for minors, where only the prompt and response are processed in a transient manner, with all non-essential metadata (like device hardware IDs) being immediately discarded.
5	**Data Retention and Deletion**	Section 8(7) requires erasure of personal data once the	Interaction data is stored to maintain "conversation context." For a minor,	Implement automatic session-end deletion or a 24-hour auto-purge for all minor-generated

		purpose is fulfilled or consent is withdrawn.	an indefinite archive of their AI chats creates a long-term risk of data misuse. The Act requires data to be deleted once it is no longer serving its primary purpose.	chat logs in India, ensuring no permanent digital footprint of the child's queries remains on xAI servers.
6	**Cross-Border Data Transfers**	Section 16 governs the transfer of personal data outside India.	xAI is a US-based entity. Moving the personal data of Indian children to US servers requires ensuring that the destination provides protection equivalent to the DPDP Act’s high standards for minors.	Adopt India-specific Data Transfer Agreements that explicitly hold xAI accountable to the DPDP Act's standards, regardless of whether the data is processed in Texas or other global data center locations.
7	**Grievance Redressal and Accountability**	Section 10(2) and Section 13 require an efficient grievance redressal process.	Currently, xAI provides a global privacy portal (relyance.ai). This does not meet the DPDP requirement for a localized, named "Grievance Officer" in India who can respond to parental complaints within statutory timelines.	Appoint a dedicated Grievance Officer for India and launch a localized support portal for parents to raise and track data-related concerns within the statutory 72-hour acknowledgment window.
8	**Targeted Advertising**	Section 9(3) strictly prohibits advertising directed at children.	While Grok itself may not show ads, it is often tied to X Premium. Using a minor’s engagement with Grok to "nudge" them toward a paid subscription or to personalize their X feed constitutes prohibited profiling and marketing.	Completely decouple Grok usage from X-feed personalization for minor accounts. Ensure that no promotional materials for X Premium or xAI API services are displayed to users under 18 in India.

9	**Notice and Language Accessibility**	Section 5 requires notice in English and any of the 22 scheduled languages.	The xAI Privacy Policy is a standard English legal document. For "informed" parental consent across India's diverse population, a single-language English policy is insufficient under the DPDP framework.	Publish "Grok Privacy Basics" if possible in all or any 22 scheduled Indian languages, using plain language to explain exactly how a child's data is siloed and protected within the xAI ecosystem.
10	**Age Threshold Discrepancy**	Section 2 (f) DPDP Act defines a 'child' as any person below 18 years; Section 9 (1) requires verifiable parental consent is mandatory for all such users. irrespective of platform-set minimum age.	Grok is accessed through X (Twitter), which maintains a minimum age of 13 globally. In India, the DPDP Act's 18-year threshold means that every Indian X user aged 13-17 who accesses Grok, including through the Grok standalone app, is a legal 'child' requiring verifiable parental consent. Critically, Grok's deliberately provocative personality makes the five-year age-threshold gap particularly hazardous for Indian teenage users who lack the maturity filter the platform's content model assumes.	Implement a Grok-specific age gate for Indian users, separate from X's general 13-year minimum, requiring all users under 18 in India to complete a parent-verified consent step before accessing Grok features. Grok's default response mode for minor accounts must be set to 'Safe Mode' and should not be user-adjustable without fresh parental authorisation.
11	**Webcam / Camera Access Consent**	Section 9(1) and Section 7: Camera-captured imagery constitutes personal data; collection requires informed, specific, verifiable	Grok on X (Twitter) may analyse camera-captured images shared in X posts, DMs, or via Grok's image-analysis feature. Indian minor users can photograph and submit images for Grok's AI analysis, images that may include faces, personal spaces,	Implement a mandatory, parent-verified in-app consent prompt before Grok's image-analysis features or any camera-dependent X feature is activated for Indian minor accounts. Camera-captured images submitted to Grok for analysis must

		parental consent for minors.	identity documents, or sensitive documents, without any DPDP-specific parental-consent mechanism. Additionally, X's 'X Spaces' and visual content features involve camera access for live video that may be analysed by xAI systems without guardian authorisation.	be deleted immediately after the AI response is generated, must not be retained for training xAI's vision models, and must not be shared with X's advertising or recommendation systems.
12	**Consent Withdrawal Mechanism**	Section 6(4) DPDP Act mandates withdrawal of consent must be as easy as giving it; Section 8(7) requires data deletion upon withdrawal.	xAI/Grok does not offer a dedicated, parent-facing consent-withdrawal mechanism. Withdrawal of consent for Grok's AI processing of a minor's interactions is bundled with X account management, an indirect and complex process that does not: (a) confirm which xAI processing activities have ceased, (b) address deletion of data used in Grok's training pipeline, (c) provide India-specific guidance, or (d) meet the DPDP standard of withdrawal being as accessible as giving consent. This is particularly problematic given Grok's explicit use of interaction data for model training.	Build a dedicated 'Parental Consent Withdrawal for Grok' portal accessible independently of X account management if possible in all 22 scheduled Indian languages. Withdrawal must: (a) immediately cease all Grok AI processing of the minor's data, (b) trigger removal from xAI's training pipeline retroactively, (c) provide category-level deletion confirmation, and (d) be completable within the DPDP-prescribed statutory timeframe without requiring the parent to navigate X's general account settings.
13	**Data Shared with Third Parties & Control**	Section 7 and Section 9(3): Children's data shared with third parties must be limited to stated purposes;	Grok operates within the X/Twitter ecosystem, which has extensive third-party data-sharing arrangements with advertisers, data brokers, API partners,	Publish a dedicated India-specific 'Grok Minor Data Sharing Register' listing all third parties and intra-X-ecosystem entities that receive data from Indian minor users'

		parents must be informed and given control.	and, through Elon Musk's interconnected ventures, potentially other entities. For Indian minor users, Grok interaction data, including the content of AI conversations, may flow through X's data-sharing infrastructure to third parties under terms not specifically assessed for DPDP child-protection compliance. Parents have no itemised view of these data flows and no India-specific opt-out mechanism.	Grok interactions, the legal basis for each sharing arrangement, and the applicable DPDP-equivalent protections. Provide parents a granular, India-specific opt-out dashboard if possible in all 22 scheduled Indian languages and prohibit Grok interaction data from Indian minor accounts from entering X's advertising data ecosystem.
14	**Voice / Audio Recording Consent**	Section 9(1) and Section 7: Voice recordings constitute personal data; parental consent is required before audio capture from minors; processing must be purpose-limited.	Grok's future voice-interaction features, X's audio tweet format, and X Spaces live-audio functionality all involve microphone access and potential audio processing by xAI systems. For Indian minor users, participation in X Spaces or any future Grok voice mode constitutes audio-data collection without a DPDP-specific parental-consent mechanism. Given Grok's personality model, designed to engage with provocative and mature topics, voice-mode interactions with minor users would present compounded risks of both harmful-content exposure and biometric audio-data collection without guardian authorisation.	Implement a dedicated, parent-verified consent step before any audio feature (X Spaces participation, voice-input to Grok, audio tweets) is activated for Indian minor accounts. Audio from minor accounts must not be retained beyond the session, must be excluded from xAI's speech and language model training, and must not feed into X's content moderation or advertising systems. A commitment to never enabling voice-mode Grok for Indian minor accounts without a pre-established DPDP parental-consent framework must be published publicly.

BALANCING MINOR AUTONOMY WITH PARENTAL VIGILANCE

The DPDP Act mandates "verifiable parental consent," recognizing that minors require protection from complex data profiling and behavioural tracking. However, effective privacy must balance this oversight with a minor's evolving need for digital autonomy. While parental vigilance safeguards against systemic risks, over-regulation can stifle a teen's independent development. Platforms must bridge this gap by providing high-privacy defaults, limiting sensitive content and unwanted contact, while allowing older teens more control unless a parent enables active supervision. True compliance empowers both: providing parents with oversight tools while ensuring minors receive transparent, child-friendly information to navigate their own privacy rights.

4. Cross-Cutting Compliance Themes

4.1 The Verification Gap: Self-Declaration as Structural Non-Compliance

Across all fourteen platforms, the most prevalent and structurally critical compliance gap is the reliance on self-declaration for age verification and parental consent. Whether a minor declares their own age at sign-up (Instagram, Perplexity, Canva, Grok) or a parent follows an email link (ChatGPT, Khan Academy), none of these mechanisms constitute 'verifiable' confirmation under the DPDP Act's standard. High-assurance verification or verifiable payment transactions from a parent's account is absent across the board.

4.2 The Tracking-Personalisation Conflict

Section 9(3)'s prohibition on behavioural monitoring and tracking of children is in direct structural conflict with the core product design of most AI tools reviewed. Learning analytics (Khan Academy, SATHEE, DIKSHA), personalisation engines (Gemini, ChatGPT, Instagram), and usage-history features (Perplexity Threads, Gemini prompt logs, WhatsApp metadata) all constitute forms of behavioural monitoring that are categorically prohibited for users under 18. Platforms must either architect minor-specific stateless modes or accept that their current product design cannot lawfully serve users below 18 in India.

4.3 Camera and Biometric Data: Particularly Acute Risks

Several platforms, Photomath, Microsoft Math Solver, ChatGPT, Gemini, Instagram, Canva, and Grok, involve significant camera access and image processing as core product functions. For minor users, camera-captured imagery constitutes personal data requiring informed, specific, verifiable parental consent under Sections 9(1) and 7. AI-powered face filters (Instagram), avatar generation (Canva), and multimodal image input (ChatGPT, Gemini) process biometric-adjacent facial data from minors without guardian-specific authorisation.

4.4 Government Platforms as Compliance Failures: SATHEE and DIKSHA

The compliance analysis reveals a particularly concerning pattern: India's own government-run educational platforms, SATHEE (IIT Kanpur) and DIKSHA (Ministry of Education), exhibit some of the most severe compliance gaps reviewed. SATHEE applies no age gate and collects only email addresses despite serving JEE/NEET aspirants who are almost entirely under 18. DIKSHA, which serves children as young as Class 1 (age 5-6), has no differentiated child protection framework. These government platforms should model compliance so that private players in the market are obligated to adhere compliance in alignment with Indian statutory requirements.

4.5 Language Accessibility as a Consent Precondition

Section 5 of the DPDP Act requires privacy notices in English or any of the 22 scheduled Indian languages. The majority of platforms reviewed make their Privacy Policies available only in English, with a small subset (notably Google, Meta, OpenAI properties) offering privacy information in some regional Indian languages. For parents in non-English speaking households, a substantial majority of India's population, English-only privacy disclosures structurally undermine the 'informed' nature of any consent provided.

5. Conclusion

The DPDP Act, 2023 sets a clear and demanding standard for the protection of children's data in India. This report's analysis of fourteen AI tools extensively used by Indian minors demonstrates a systemic and pervasive pattern of non-compliance across multiple dimensions. The most critical failures are structural: the five-year age-threshold gap between platform-set minimums and India's 18-year DPDP definition of 'child'; the absence of technically enforced, high-assurance parental verification mechanisms; and the direct conflict between core product features (personalisation, analytics, tracking) and Section 9(3)'s absolute prohibition on behavioural monitoring of children.

The regulatory framework is clear: Section 9(2)'s prohibition on processing detrimental to a child's well-being admits no exemptions, not educational necessity, not commercial viability, and not technical difficulty. Platforms operating in India must treat DPDP compliance not as a box-ticking exercise but as a fundamental product design constraint that determines whether their services may lawfully be used by any of India's estimated 450+ million users under the age of 18.

POLICY NOTE

Ensuring Child Data Protection Compliance During the Transitional Implementation of the DPDP Framework

- In the context of the ongoing phased implementation of the Digital Personal Data Protection (DPDP) framework, any processing of children's data that is inconsistent with the statutory intent of the DPDP Act shall be subject to immediate scrutiny and corrective action.

- Binding directions shall be issued to all relevant authorities and platform operators mandating the initiation of corrective measures and strict, time-bound alignment with the requirements of the DPDP Act and Rules. Non-compliance during the transition phase shall not be treated as a permissible norm.

- All platforms shall be obligated to implement, in a phased but enforceable manner, verifiable parental consent mechanisms, age-appropriate design standards, and proportionate age verification systems. Deferral or dilution of these obligations shall not be permitted beyond the scope of the notified implementation roadmap.

- Government-affiliated platforms, including SATHEE and DIKSHA, shall be placed under heightened regulatory oversight, with mandatory disclosures on compliance preparedness, periodic reporting, and demonstrable progress towards full alignment. Any failure to meet expected standards shall invite immediate review.

- Platforms shall be required to ensure the deployment of regional language interfaces and child-specific privacy disclosures as a baseline compliance requirement to enable informed and meaningful consent. Absence of such measures shall be treated as a material deficiency.

- The Data Protection Board of India shall issue binding, sector-specific guidance addressing AI platforms and the processing of minors' data to eliminate regulatory uncertainty. All international platforms operating in India shall be required to submit India-specific compliance roadmaps, with clearly defined milestones, subject to regulatory review. The Government shall establish a centralized public compliance dashboard to track platform readiness and adherence to child data protection norms, and undertake targeted awareness initiatives for parents, particularly young parents and first-time digital users.

- The educational exemption under Rule 11 shall be interpreted narrowly and strictly, confined exclusively to explicitly defined educational or safety-related processing activities. Any attempt to invoke this exemption to bypass core data protection obligations shall be treated as a misuse of statutory provisions. The prohibition under Section 9(2) shall operate as an absolute boundary. No exemption shall be interpreted to permit AI-driven processing that is detrimental to the well-being of children.

- Platforms shall establish child-sensitive grievance redressal mechanisms and be subject to periodic independent audits to ensure verifiable compliance. Data collection and processing of children's data shall be limited strictly to what is necessary for the specified purpose.

- A stringent, continuously monitored, and enforcement-oriented compliance framework shall be instituted to ensure full and effective alignment with the DPDP regime within the prescribed implementation timeline, culminating in May 2027.

References

1. Anthropic. (n.d.). Privacy policy. https://www.anthropic.com/legal/privacy
2. Canva. (2025). Privacy policy. https://www.canva.com/en_in/policies/privacy-policy/
3. Cyber SRCC. (2026, January 20). Handling children’s data under DPDP: Risk controls and policy standards. https://cybersrcc.com/blogs/Handling%20Children%E2%80%99s%20Data%20Under%20DPDP:%20Risk%20Controls%20and%20Policy%20Standards/2026-01-20
4. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
5. DIKSHA - Government of India. (2025). Terms of use. https://diksha.gov.in/term-of-use.html#privacyPolicy
6. Facebook. (2024, November 14). Meta Privacy Policy - How Meta collects and uses user data. https://www.facebook.com/privacy/policy
7. Gemini Apps Help. (2019). Gemini Apps Privacy Hub. https://support.google.com/gemini/answer/13594961?hl=en
8. Google. (2022). Privacy Policy – Privacy & Terms – Google. https://policies.google.com/privacy?hl=en-US
9. Google. (2026). Google Family Link - Children’s Privacy Policy. https://families.google.com/familylink/privacy/child-policy/
10. Han, H. J. (2023, January 27). Indian government app exposed children’s personal data. Human Rights Watch. https://www.hrw.org/news/2023/01/27/indian-government-app-exposed-childrens-personal-data
11. Instagram. (2024). About Instagram teen privacy and safety settings. https://help.instagram.com/3237561506542117
12. Instagram Help Center. (2025). https://help.instagram.com/995996839195964/
13. Jadaun, S. (2026, March 14). Regulating children’s social media use in India: Why a ban alone will not protect our young. Bar & Bench. https://www.barandbench.com/columns/regulating-childrens-social-media-use-in-india-why-a-ban-alone-will-not-protect-our-young
14. Kalra, L. (2025, November 21). Decoding the Digital Personal Data Protection Act 2023. EY Insights. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023

15. Khan Academy. (n.d.). Privacy policy. https://www.khanacademy.org/about/privacy-policy
16. Kirmani, T. (2025, January 9). DPDP rules: No social media for under 18s without parental approval. Outlook India. https://www.outlookindia.com/national/dpdp-rules-no-social-media-for-under-18s-without-parental-approval
17. Mali, P. (n.d.). DPDP Rules 2025 – Analysis of its implications on industry and compliance guidance. https://www.dpdpa.com/blogs/DPDP%20Rules%202025-%20Analysis%20of%20Industry%20implications.html
18. Medianama. (2024, February 1). New privacy study into children's apps stresses the urgency for putting DPDP Act into effect. https://www.medianama.com/2024/02/223-arrka-privacy-study-childrens-apps-2/
19. Meta. (2016). Teen privacy and safety settings | Meta Help Centre. https://www.meta.com/en-gb/help/policies/1754656424993737/
20. Microsoft. (2023). Privacy for young people. https://www.microsoft.com/en-us/privacy/young-people
21. Microsoft. (2024). Microsoft Privacy Statement. https://www.microsoft.com/en-GB/privacy/privacystatement
22. Microsoft. (2026). List of countries or regions that have statutory age limits for children. https://support.microsoft.com/en-us/account-billing/list-of-countries-or-regions-that-have-statutory-age-limits-for-children-a7393f56-5107-44b1-be44-655589bdeb92
23. Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. The Gazette of India. https://dpdpa.com/DPDP_Rules_2025_English_only.pdf
24. Nhando, D. (2026, February 6). Unmasking EdTech's surveillance infrastructure in the age of AI. Tech Policy Press. https://www.techpolicy.press/unmasking-edtechs-surveillance-infrastructure-in-the-age-of-ai/
25. OpenAI. (2023). Privacy policy. https://openai.com/en-GB/policies/row-privacy-policy/
26. OpenAI Help Center. (2025). Parental controls on ChatGPT - FAQ. https://help.openai.com/en/articles/12315553-parental-controls-on-chatgpt-faq
27. Perplexity AI. (2024). Privacy policy. https://www.perplexity.ai/hub/legal/privacy-policy
28. Photomath. (2023). Privacy policy. https://photomath.com/privacy/
29. Pratim Gohain, M. (2026, February 19). Survey: Kids use AI daily, but most don't know how it works. Times of India. http://timesofindia.indiatimes.com/articleshow/128532960.cms

30. SATHEE JEE. (2026). Privacy policy. https://sathee.iitk.ac.in/privacy-policy/
31. Tulsyan, A. (2025, November 20). DPDP rules and the future of child data safety. ORF Online. https://www.orfonline.org/expert-speak/dpdp-rules-and-the-future-of-child-data-safety
32. Web Foundation / Digital Watch. (2025, November 21). DPDP law takes effect as India tightens AI-era data protections. https://dig.watch/updates/dpdp-law-takes-effect-as-india-tightens-ai-era-data-protections
33. WhatsApp. (2021, January 4). Privacy policy. https://www.whatsapp.com/legal/privacy-policy
34. WhatsApp. (2026). Privacy disclosure for parent-managed accounts. https://www.whatsapp.com/legal/privacy-disclosure-for-parent-managed-accounts
35. xAI. (2025). Privacy policy. https://x.ai/legal/privacy-policy

ABOUT THE ORGANISATION

The Advanced Study Institute of Asia (ASIA), established in 2023 serves as an interdisciplinary research center dedicated to enhancing the understanding of Asia, particularly South and Southeast Asia. Situated in New Delhi, ASIA aims to navigate the complexities of various fields, including International Relations, health, law, and societal issues, by leveraging the expertise of leading scholars and practitioners.

ASIA

ADVANCED STUDY INSTITUTE OF ASIA

SGT UNIVERSITY

Shree Guru Gobind Singh Tricentenary University

NAAC A+