

Unesco Chair on E-Learning and Teaching
Mehralborz University IRAN

unesco Chair

ایمنی آنلاین در آموزش

پیامدها برای دانش‌آموزان، معلمان، والدین و مسئولان و دست‌اندرکاران نظام آموزشی در عصر هوش مصنوعی و فناوری‌های دیجیتال پیشرفته

ترجمان اندیشه یونسکو
شماره نهم
آبان ۱۴۰۵

صندوق کودکان سازمان ملل متحد (یونیسف) دفتر هند[1] و دفتر منطقه‌ای یونسکو در جنوب آسیا[2]

فوریه ۲۰۲۶

1. UNICEF India
2. UNESCO Regional Office for South Asia

ایمنی آنلاین در آموزش

پیامدها برای دانش‌آموزان، معلمان، والدین و مسئولان و دست‌اندرکاران نظام آموزشی در عصر هوش مصنوعی و فناوری‌های دیجیتال پیشرفته

راهنمای سیاستی ۲۰۲۶

فهرست مطالب

۱. زمینه و بستر موضوع ۵

۲. چرا هند باید بر ایمنی آنلاین کودکان تمرکز کند؟ ۷

۳. چه راهکارهایی مؤثرند؟ راهبردهای اثربخش برای ایمنی آنلاین در آموزش...۹
۱٫۳ سیاست‌گذاری و مقررات برای محیط‌های یادگیری ایمن ۹
۲٫۳ رویکردهای چندذی‌نفعی، کل‌مدرسه‌ای و کل‌جامعه‌ای و بین‌بخشی ۱۰
۳٫۳ برنامه‌های آموزشی مبتنی بر مهارت‌های زندگی و سواد دیجیتال ۱۱

۴. توصیه‌های سیاستی ۱۲
۱٫۴ نظام ۱۲
۲٫۴ دسترسی ۱۳
۳٫۴ یادگیری ۱۳

راهنمای سیاستی
تضمین ایمنی آنلاین[1] در بخش آموزش هند

۱. زمینه و بستر موضوع

پیشرفت سریع فناوری‌های دیجیتال، دولت هند را بر آن داشته است که ابتکارات جامع یادگیری دیجیتال را در اولویت قرار دهد. این رویکرد، با به‌رسمیت شناختن نقش تحول‌آفرین فناوری آموزشی در کاهش شکاف‌های نظام آموزشی و همچنین تجهیز دانش‌آموزان به مهارت‌های موردنیاز قرن بیست‌ویکم، شکل گرفته است.

سیاست ملی آموزش هند (NEP)[2] مصوب سال ۲۰۲۰، زمینه‌ساز این تحول است. این سیاست با ترویج سواد دیجیتال[3]، بهره‌گیری از فناوری‌ها و ابزارهای تحول‌آفرین و تضمین دسترسی عادلانه به آموزش، مسیر این تغییر را هموار می‌کند. ابتکاراتی مانند «هند دیجیتال»[4] و «معماری ملی دیجیتال آموزش » (NDEAR)[5] ، راهبرد «دیجیتال در اولویت»[6] هند را به نمایش می‌گذارند؛ راهبردی که هم از بهبود نتایج یادگیری و هم از افزایش کارآمدی امور اداری پشتیبانی می‌کند.

همه‌گیری کووید-۱۹ موجب شتاب‌گرفتن چشمگیر این روند شد. در دوران همه‌گیری، یادگیری دیجیتال برای ادامه تحصیل بیش از ۲۸۶ میلیون دانش‌آموز اهمیت حیاتی پیدا کرد. در این دوره، از منابع دولتی، از جمله سکوی DIKSHA[7] و درگاه PM e-VIDYA[8]، برای تداوم آموزش استفاده شد.

بااین‌حال، هم‌زمان با ورود فناوری‌ها و سکوهای دیجیتال به نظام‌های آموزشی برای تدریس و یادگیری و افزایش دسترسی کودکان به اینترنت در خارج از محیط مدرسه، گسترش بی‌سابقه این فناوری‌ها خطراتی را نیز به همراه آورده است که ممکن است بر حفاظت و ایمنی کودکان تأثیر بگذارد. ازاین‌رو، یکی از الزامات اساسی گسترش آموزش دیجیتال، تدوین دستورالعمل‌ها و رویه‌های مؤثر و مستحکم برای تضمین ایمنی و به‌زیستی کودکان و نوجوانان است.

چارچوب‌های سیاستی آموزش در هند، اهمیت ایمنی دیجیتال را به رسمیت می‌شناسند؛ بااین‌حال، اجرای این سیاست‌ها همچنان پراکنده و ناهماهنگ است.

- سیاست ملی آموزش (NEP) مصوب ۲۰۲۰: بر سواد دیجیتال و ادغام فناوری در آموزش تأکید می‌کند.

1. Online Safety
2. The National Education Policy
3. Digital literacy
4. Digital India
5. National Digital Educational Architecture
6. digital-first

۷. زیرساخت دیجیتال برای آموزش در هند: برنامه رسمی وزارت آموزش دولت هند که طیف گسترده ای از منابع آموزشی را برای دانش آموزان، معلمان، و و الدین در سراسر کشور، در بر می‌گیرد.

۸. یک اپلیکیشن موبایل و پلتفرم یادگیری دیجیتال برای ارائه منابع آموزشی رایگان به دانش آموزان در تمام سطوح است.

- دستورالعمل‌های PRAGYATA: نقشه راهی برای آموزش دیجیتال ارائه می‌دهند و برای مدت استفاده روزانه از صفحه‌نمایش محدودیت تعیین می‌کنند. بر اساس این دستورالعمل‌ها، برای دانش‌آموزان پایه‌های اول تا هشتم، حداکثر دو نوبت ۳۰ تا ۴۵ دقیقه‌ای و برای دانش‌آموزان پایه‌های نهم تا دوازدهم، حداکثر چهار نوبت توصیه شده است.
- چارچوب ملی برنامه درسی آموزش مدرسه‌ای (NCF-SE)[9] مصوب ۲۰۲۳: برقراری ضوابط روشن برای استفاده از رایانه و اینترنت را توصیه می‌کند. این چارچوب تأکید دارد که دانش‌آموزان باید ایمنی سایبری، استفاده مناسب از فناوری و اینترنت و نیز کارکرد صفحه‌نمایش‌ها و ابزارهای دستی و اختلالاتی را که ممکن است بر اثر استفاده از آن‌ها ایجاد شود، بیاموزند[10].

با وجود این تعهدات، همچنان چالش‌هایی وجود دارد. کمبودهای زیرساختی، شکاف دیجیتالی‌ای را آشکار می‌سازند که الگوهای طرد و به‌حاشیه‌راندن را بازتولید می‌کند. تنها ۶۳٫۵ درصد از مدارس هند، فارغ از نوع مدیریت، به امکانات اینترنت دسترسی دارند؛ موضوعی که دسترسی عادلانه به یادگیری دیجیتال ایمن و تحت مدیریت مدارس را محدود می‌کند.

بر اساس گزارش سالانه وضعیت آموزش (ASER)[11] در سال ۲۰۲۴، ۸۹/۱ درصد از نوجوانان ۱۴ تا ۱۶ ساله گزارش کرده‌اند که در خانه تلفن هوشمند دارند. از این میان، ۷۶ درصد عمدتاً از این دستگاه‌ها برای استفاده از رسانه‌های اجتماعی و تنها ۵۷ درصد برای اهداف آموزشی استفاده می‌کنند.

نگرانی‌ها دیگر صرفاً به این موضوع محدود نیست که آیا کودکان به فناوری دیجیتال دسترسی دارند یا خیر؛ بلکه چگونگی استفاده آن‌ها از این فناوری‌ها نیز به مسئله‌ای مهم تبدیل شده است.

یونیسف در سال ۲۰۲۴، برای ارزیابی وضعیت ایمنی آنلاین نوجوانان و جوانان در هند، پیمایشی را از طریق سکوی U-Report انجام داد.

نتایج این پیمایش نشان داد که ۴۰ درصد از جوانان روزانه بیش از چهار ساعت را در فضای آنلاین سپری می‌کنند. این میزان استفاده، اگرچه فرصت‌هایی را برای توسعه مهارت‌های دیجیتال فراهم می‌آورد، آسیب‌پذیری آنان را در برابر خطرات دیجیتال نیز افزایش می‌دهد.

پیمایش ملی ارزیابی آموزشی (PRS)[12] در سال ۲۰۲۴ نیز نشان داد که ۳۲ درصد از دانش‌آموزان از سوی هم‌کلاسی‌های خود مورد تمسخر قرار گرفته‌اند و ۲۵ درصد از شرکت در فعالیت‌ها کنار گذاشته شده‌اند. این یافته‌ها از رواج رفتارهای نامناسب در محیط فیزیکی مدرسه حکایت دارند؛ رفتارهایی که اغلب در تعاملات آنلاین نیز بازتاب می‌یابند.

گسترش برنامه‌های فناوری آموزشی (EdTech) بدون وجود مقررات استاندارد، این خطرات

9. National Curriculum Framework for School Education

۱۰. (بند ۲،۳،۳،۵)

11. Annual Status of Education Report

12. Parakh Rashtriya Sarvekshan

را تشدید کرده و کودکان را بیش از پیش در معرض مسائل مرتبط با حریم خصوصی و امنیت داده‌ها قرار داده است. نقص‌های امنیتی در برنامه‌های یادگیری دیجیتال ممکن است اطلاعات هویتی و شخصی میلیون‌ها دانش‌آموز و معلم را افشا کند.

شکاف جنسیتی در سواد دیجیتال و ایمنی آنلاین نیز همچنان پابرجاست. بر اساس پیمایش ASER سال ۲۰۲۴، ۶۵/۲ درصد از پسران می‌دانند چگونه یک نمایه کاربری را مسدود کنند یا گذرواژه خود را تغییر دهند؛ درحالی‌که این رقم در میان دختران تنها ۵۸/۷ درصد است.

از منظر سیاست‌گذاری، اگرچه ۹۳ درصد از مدارس دارای سیاست حفاظت از کودک منطبق با قانون POCSO هستند، تنها ۷۰ درصد از آن‌ها سیاستی برای مقابله با قلدری دارند و در سال گذشته فقط ۳۸ درصد از معلمان در دوره‌های آموزشی فناوری اطلاعات و ارتباطات (ICT) شرکت کرده‌اند.

علاوه بر این، نتایج PRS سال ۲۰۲۴ نشان داد که تنها ۴۵ درصد از مدارس، سواد دیجیتال را در برنامه درسی خود گنجانده‌اند و کمتر از ۳۰ درصد آن‌ها برنامه‌های رسمی آموزش ایمنی سایبری[۱۳] دارند.

این داده‌ها بر ضرورت فوری تقویت سیاست‌ها، توانمندسازی حرفه‌ای معلمان و طراحی مداخلات حساس به جنسیت تأکید می‌کنند تا محیطی امن و فراگیر برای یادگیری دیجیتال کودکان و نوجوانان هند فراهم شود.

۲. چرا هند باید بر ایمنی آنلاین کودکان تمرکز کند؟

کنوانسیون حقوق کودک دولت‌ها را موظف می‌کند که حق هر کودک برای آموزش و برخورداری از حمایت در برابر تمامی اشکال خشونت را محترم بشمارند و تضمین کنند. کمیته حقوق کودک سازمان ملل متحد در تفسیر عمومی شماره ۲۵ خود، صراحتاً این موضوع را به رسمیت شناخته است. «دولت‌های عضو باید از فعالیت مؤثر سازوکارهای حفاظت از کودکان در فضای آنلاین و اجرای سیاست‌های حفاظتی اطمینان حاصل کنند و درعین‌حال، سایر حقوق کودکان را نیز در تمامی محیط‌هایی که به محیط دیجیتال دسترسی دارند، محترم بشمارند. این محیط‌ها شامل خانه، مراکز آموزشی، کافی‌نت‌ها، مراکز جوانان، کتابخانه‌ها، مراکز بهداشتی و محیط‌های مراقبتی جایگزین می‌شوند».

بر اساس یادداشت فنی جهانی یونیسف با عنوان «حفاظت از کودک در یادگیری دیجیتال»، خطرات آنلاین را می‌توان به‌طور کلی در قالب الگوی «چهار C» طبقه‌بندی کرد: محتوا (Content)، ارتباط (Contact)، رفتار (Conduct) و قرارداد (Contract).

خطرات مرتبط با محتوا: زمانی رخ می‌دهند که کودکان با مطالب نامناسب مواجه شوند.

خطرات مرتبط با ارتباط: به تعاملات زیان‌باری اشاره دارند که ممکن است به فریب و جلب اعتماد کودک با اهداف سوء، بهره‌کشی جنسی، تعقیب و مزاحمت، اخاذی یا آزار منجر شوند.

خطرات مرتبط با رفتار: زمانی پدید می‌آیند که کودک شاهد رفتارهای زیان‌بار باشد،

13. cyber safety

در آن‌ها مشارکت کند یا قربانی آن‌ها شود؛ رفتارهایی مانند قلدری سایبری یا انتشار عامدانه محتوای توهین‌آمیز از سوی خود کودک.

خطرات مرتبط با قرارداد: به توافق‌های بهره‌کشانه‌ای اشاره دارند که ممکن است شامل هزینه‌های پنهان یا از دست رفتن کنترل فرد بر داده‌های شخصی خود باشند.

بر اساس مطالعه‌ای که اخیراً از سوی سازمان همکاری و توسعه اقتصادی (OECD) انجام شده است، نوجوانانی که در فضای دیجیتال فعالیت می‌کنند، اغلب تجربه‌های منفی دارند. بیش از یک‌سوم نوجوانان ۱۵ ساله، معادل ۳۶ درصد، گزارش کرده‌اند که هنگام مواجهه با محتوای آنلاین نامتناسب با سن خود ناراحت شده‌اند. ۴۲ درصد از دریافت پیام‌های توهین‌آمیز ناراحت شده‌اند؛ بیش از نیمی از آنان، یعنی ۵۳ درصد، از محتوای تبعیض‌آمیز آزرده شده‌اند و نزدیک به ۴۰ درصد از نوجوانان نیز از این موضوع آسیب دیده‌اند که اطلاعات مربوط به آن‌ها بدون رضایتشان به اشتراک گذاشته شده است.

جدول۱. احتمال برآوردشده تجربه مشکلات سلامت روان در نوجوانان ۱۵ ساله، برحسب مدت استفاده از رسانه‌های اجتماعی

مدت استفاده از رسانه‌های اجتماعی	افسردگی	اضطراب
بدون استفاده	%۴۵	%۵۱
کمتر از یک ساعت در روز	%۴۷	%۵۱
یک تا سه ساعت در روز	%۵۳	%۵۸
بیش از سه ساعت در روز	%۵۷	%۶۲

منبع: برنامه بین‌المللی ارزیابی دانش‌آموزان (PISA)، سال ۲۰۲۲

بنابراین، مجهزکردن کودکان به مهارت‌های استفاده ایمن از فناوری، آن‌ها را قادر می‌سازد به اطلاعات دسترسی پیدا کنند، ارتباطات معناداری با همسالان خود برقرار سازند و از فرصت‌های دیجیتال بهره‌مند شوند؛ درحالی‌که از به‌زیستی خود نیز محافظت می‌کنند. محیط‌های دیجیتال، مانند سکوهای یادگیری یا رسانه‌های اجتماعی، می‌توانند فرصت‌هایی برای یادگیری چندوجهی، برقراری ارتباط و ایجاد روابط عمیق‌تر و معنادارتر با همسالان فراهم کنند. بااین‌حال، بهره‌مندی از ابزارهای دیجیتال و تجربه لذت‌بخش استفاده از آن‌ها زمانی به حداکثر می‌رسد که حفاظ‌ها و محدودیت‌های مناسب برقرار باشند.

پژوهش‌ها نشان می‌دهند که استفاده متعادل از این ابزارها ایمن‌تر است؛ زیرا استفاده بیش‌ازحد از رسانه‌های اجتماعی، به‌ویژه بیش از دو ساعت در روز، با پیامدهای نامطلوب سلامت روان، از جمله افسردگی، اضطراب، نگرانی درباره تصویر بدنی و اختلال خواب ارتباط دارد. دختران نیز اغلب بیش از پسران تحت تأثیر این پیامدها قرار می‌گیرند.

این نگرانی‌ها موجب شده است کشورهای متعددی مقررات خود را سخت‌گیرانه‌تر کنند؛ ازجمله استرالیا که پیشگام ممنوعیت کامل استفاده کودکان زیر ۱۶ سال از رسانه‌های اجتماعی بوده است. مالزی و چندین کشور اروپایی نیز در این مسیر گام برداشته‌اند.

فراتر از محدودیت‌های زمانی استفاده، وجود تدابیر حفاظتی بیشتری ضروری است تا فناوری به تقویت یادگیری و بهزیستی کمک کند، نه آنکه آن‌ها را تضعیف کند.
این تدابیر باید مانع از آن شوند که ابزارهای دیجیتال و هوش مصنوعی وابستگی به فناوری را برای واگذاری فرایندهای شناختیِ ضروری برای یادگیری افزایش دهند، یادگیری طوطی‌وار یا مشارکت سطحی را تقویت کنند یا امکان تقلب علمی را فراهم آورند.
پژوهش اخیر «کودکان آنلاین اتحادیه اروپا»[14] در سال ۲۰۲۶ نشان داده است که ۷۲ درصد از کودکان ۹ تا ۱۶ ساله از هوش مصنوعی مولد استفاده می‌کنند. درعین‌حال، کودکان کم‌سن‌تر در مقایسه با منابعی که به‌صورت مشارکتی تولید شده‌اند، مانند ویکی‌پدیا، اعتماد بیشتری به خروجی‌های هوش مصنوعی مولد دارند؛ این در حالی است که شواهد نشان می‌دهند هوش مصنوعی اغلب قابل اتکا نیست.
افزون بر این، حدود ۱۵ درصد از کودکان هم‌اکنون برای دریافت توصیه‌های مرتبط با سلامت جسمانی و حمایت عاطفی از هوش مصنوعی مولد استفاده می‌کنند.
بنابراین، به همان اندازه اهمیت دارد که اطمینان حاصل شود دانش‌آموزان مهارت‌های سواد انتقادی دیجیتال و سواد هوش مصنوعی را پرورش می‌دهند تا بتوانند از فناوری با قدرت تشخیص و داوری مناسب، هم برای اهداف آموزشی و هم برای امور شخصی استفاده کنند.
همچنین لازم است تجربه‌های یادگیری دیجیتال به‌گونه‌ای طراحی شوند که هوش مصنوعی در داربست‌بندی یادگیری و فرصت‌های «تقلا و تلاش سازنده»[15] مداخله نکند. این رویکرد به یادگیرندگان امکان می‌دهد با مفاهیم درگیر شوند، اشتباه کنند و به درک عمیق‌تری دست یابند، به‌جای آنکه تلاش شناختی لازم را با استفاده از راه‌حل‌های خودکار دور بزنند.
درعین‌حال، باید نقش محوری معلمان، یادگیرندگان و تعاملات انسانی معنادار در فرایندهای یادگیری حفظ شود.

۳. چه راهکارهایی مؤثرند؟ راهبردهای اثربخش برای ایمنی آنلاین در آموزش

شواهد جهانی و بهترین تجارب نشان می‌دهند که ایجاد محیطی امن برای یادگیری دیجیتال مستلزم رویکردی چندلایه است که سیاست‌گذاری، آموزش و فناوری را با یکدیگر ترکیب کند. مداخلات اثربخش در سه سطح ملی، مدرسه‌ای و فردی اجرا می‌شوند.

۱،۳ سیاست‌گذاری و مقررات برای محیط‌های یادگیری ایمن

- وجود قوانین و سیاست‌هایی که از کودکان محافظت کنند، بنیادی است. این قوانین باید حفاظت از داده‌ها و حاکمیت بر داده‌ها، محتوای متناسب با سن و سازوکارهای گزارش‌دهی موارد سوءاستفاده را در بر گیرند. بر اساس گزارش یونیسف با عنوان «ارزیابی ابتکارات ایمنی آنلاین» (۲۰۲۲)، در نبود حمایت‌های قانونی و مقرراتی، تلاش‌های

14. EU Kids Online
15. Productive Struggle

آموزشی تأثیر محدودی خواهند داشت.

- وجود قواعد روشن، نظام‌های گزارش‌دهی و پاسخ‌گویی و نیز حمایت نهادی، ازجمله تأمین منابع و آموزش، اهمیت اساسی دارد. برای نمونه، برنامه ملی KiVa فنلاند [۱۶] میزان وقوع قلدری سنتی و قلدری سایبری را تا ۵۰ درصد کاهش داده است. این تجربه نشان می‌دهد که چارچوب‌های ساختاریافته در سطح مدرسه می‌توانند ایمنی و به‌زیستی دانش‌آموزان را به‌طور چشمگیری بهبود دهند.
- همکاری با صنعت فناوری، ازجمله سکوها، رسانه‌های اجتماعی و توسعه‌دهندگان برنامه‌های کاربردی، به ارتقای ایمنی از طریق طراحی کمک می‌کند. این همکاری باید با مشارکت دولت‌ها در سیاست‌گذاری و تنظیم مقررات، سازمان‌های غیردولتی در آگاهی‌بخشی و مدارس در اجرا همراه باشد.
- ابزارهایی مانند فیلترینگ، نظارت و مدیریت محتوا، تنظیمات حریم خصوصی و رویکرد «ایمنی از مرحله طراحی» [۱۷] از اجزای ایجاد محیط‌های دیجیتال ایمن‌تر هستند. کشورهایی مانند استونی نیز با استفاده از سامانه‌های هویت دیجیتال برای جلوگیری از دسترسی افراد زیر سن قانونی به محتوای بزرگسالان، پیشگام بوده‌اند.
- ارزیابی، پایش و تولید شواهد: برنامه‌های آموزشی و آگاهی‌بخشی باید به‌طور دقیق ارزیابی شوند تا مشخص شود چه اقداماتی، برای چه افرادی و در چه شرایطی اثربخش هستند. چارچوب‌های سنجش بهتر، شاخص‌های پیامد یکسان و پیگیری‌های بلندمدت‌تر به تعیین پایداری و اثربخشی برنامه‌ها کمک می‌کنند. چارچوب ارزیابی یونیسف در شرق آسیا و اقیانوسیه نمونه‌ای از این رویکرد است.

۲،۳ رویکردهای چندذی‌نفعی، کل‌مدرسه‌ای [۱۸] و کل‌جامعه‌ای و بین‌بخشی [۱۹]

- برنامه‌هایی اثربخش‌تر هستند که آموزش و نظام‌های گزارش‌دهی در مدرسه را با چارچوب‌های قانونی، خدمات حفاظت از کودک و تدابیر حفاظتی سکوهای فناوری هماهنگ می‌کنند. دلیل این امر، هم‌پوشانی میان خشونت آنلاین و آفلاین است؛ موضوعی که در چارچوب INSPIRE سازمان جهانی بهداشت [۲۰] نیز مورد تأکید قرار گرفته است.
- در طراحی مداخلات مؤثر باید تفاوت گروه‌های سنی در نظر گرفته شود؛ زیرا آنچه برای کودکان کم‌سن‌تر مؤثر است، لزوماً برای نوجوانان مناسب نیست. برای مثال، کودکان کم‌سن‌تر ممکن است در برابر مواجهه ناخواسته با محتوای زیان‌بار، دست‌کاری و متقاعدسازی آسیب‌پذیرتر باشند و به حمایت‌های پیش‌فرض قوی‌تری نیاز داشته باشند. در مقابل، نوجوانان بیشتر در معرض قلدری سایبری، فشار همسالان و مقایسه اجتماعی قرار دارند و به استقلال هدایت‌شده نیازمندند.

16. Finland's national KiVa programme
17. Safety by Design
18. whole-school
19. whole community & multi-sectoral approaches
20. WHO's INSPIRE framework

- مشارکت والدین و مراقبان: هنگامی که برنامه‌ها علاوه بر دانش‌آموزان، والدین و مراقبان را نیز هدف قرار می‌دهند و با آموزش به آن‌ها کمک می‌کنند مهارت‌های لازم برای نظارت و راهنمایی ایمن را کسب کنند، نتایج بهتری حاصل می‌شود. این نتایج شامل افزایش ایمنی آنلاین جوانان و تقویت اعتماد است.
- این موضوع اهمیت ویژه‌ای دارد؛ زیرا بسیاری از خطرات میان خانه، مدرسه و محیط‌های آنلاین جابه‌جا می‌شوند و رفتار والدین بر رفتار کودکان تأثیر می‌گذارد.



۳٫۳ برنامه‌های آموزشی مبتنی بر مهارت‌های زندگی[21] و سواد دیجیتال

- برنامه‌های مدرسه محوری که سواد دیجیتال را به کودکان آموزش می‌دهند، ازجمله نحوه استفاده ایمن از ابزارها، درک حریم خصوصی و شناسایی خطرات، در کنار مهارت‌های زندگی مانند تنظیم هیجان، حل مسئله و درخواست کمک، می‌توانند آسیب‌ها را کاهش دهند.
- ارزیابی محتوای دیجیتال، به‌ویژه در شرایط کنونی که محتوا توسط کاربران و هوش مصنوعی تولید می‌شود، اهمیت اساسی دارد. این ارزیابی باید احتمال وجود سوگیری علیه گروه‌های به‌حاشیه رانده‌شده جامعه و نیز نقض حقوق مالکیت فکری را بررسی کند.
- مداخلاتی که در چندین جلسه اجرا می‌شوند، در مقایسه با کارگاه‌های تک‌جلسه‌ای، اثربخش‌تر هستند. مواجهه‌های مکرر و متنوع با موضوع، از طریق بازی، گفت‌وگو، ویدئو و قالب‌های تعاملی، به تقویت درک و یادگیری کمک می‌کند.
- معلمان نقش مهمی در تضمین استفاده ایمن از فناوری دارند. شواهد نشان می‌دهند که راهبردهای میانجی‌گری، مانند تعیین قواعد، تسهیل گفت‌وگوها و مداخله هنگام بروز رفتارهای پرخطر، اهمیت زیادی دارند.
- اهمیت زمینه و بافت اجتماعی: شواهد حاصل از کشورهای جنوب جهانی نشان

21. life skills

می‌دهند که بسیاری از برنامه‌ها به این دلیل شکست می‌خورند که هنجارهای فرهنگی و اجتماعی محلی، زبان، وضعیت اقتصادی و اجتماعی و الگوهای دسترسی دیجیتال را در نظر نمی‌گیرند. طراحی برنامه‌ها و مداخلات حساس به جنسیت، در حوزه ایمنی آنلاین کودکان اهمیت ویژه‌ای دارد؛ زیرا دختران و پسران با خطرات متفاوتی مواجه می‌شوند.

- تقویت تاب‌آوری دیجیتال[۲۲]: باید به دانش‌آموزان کمک کرد تا نه‌تنها از آسیب دوری کنند، بلکه توانایی مقابله با آسیب و بازیابی پس از آن را نیز به دست آورند. مهارت‌هایی مانند تفکر انتقادی، شناخت اطلاعات نادرست، مقابله با تجربه‌های منفی آنلاین و درخواست کمک، ضروری هستند.

۴. توصیه‌های سیاستی

ایجاد یک زیست‌بوم دیجیتال ایمن مستلزم رویکردی چندوجهی است که حفاظت آنلاین را در تمامی ابعاد نظام آموزشی ادغام کند.

۱،۴ نظام

تدوین و اجرای سیاست ملی ایمنی آنلاین: دولت‌ها باید چارچوب حکمرانی روشنی ایجاد کنند تا از رویکرد پراکنده در پذیرش فناوری‌های آموزشی فراتر روند.

- تدوین سیاست ملی آینده‌نگر بر پایه شواهد حاصل از تجربه کودکان هندی در زمینه ایمنی آنلاین، با هدف ایجاد فرایندها و سازوکارهای ایمنی و مشخص‌کردن خطراتی مانند استفاده بیش‌ازحد از صفحه‌نمایش و قلدری سایبری. این سیاست همچنین باید حداقل استانداردهایی برای ارزیابی ایمنی تمامی محصولات و خدمات فناوری آموزشی پیش از پذیرش آن‌ها در مدارس تعیین کند. این ارزیابی باید حریم خصوصی داده‌ها، حفاظت از داده‌ها، انصاف و عدالت را در بر گیرد.
- ترویج اصل «ایمنی از مرحله طراحی » به‌عنوان یک اصل محوری؛ به‌گونه‌ای که تمامی خدمات فناوری مورد استفاده در آموزش، با درنظرگرفتن منافع عالیه کودک، به‌صورت عادلانه و فراگیر طراحی شوند و رعایت دقیق استانداردهای حفاظت از کودک، اولویت اصلی در طراحی آن‌ها باشد.
- نهادینه‌کردن تقویت ایمنی آنلاین کودکان و حکمرانی داده‌های دیجیتال از طریق گنجاندن این موضوعات در برنامه‌ها و بودجه‌های آموزشی.
- انجام ارزیابی‌های دقیق از تأثیر ابزارهای فناوری آموزشی بر ایمنی، به‌زیستی و نتایج یادگیری کودکان، پیش از گسترش استفاده از این ابزارها در سراسر نظام مدارس.

تدوین سیاست‌های روشن برای استفاده از ابزارهای دیجیتال در مدارس: تعیین مرزها و انتظارات روشن برای پیشگیری از سوءاستفاده ضروری است.

- تمامی مدارس ملزم شوند سیاستی با عنوان «سیاست استفاده قابل‌قبول»[۲۳] برای فناوری دیجیتال تدوین کنند. این سیاست باید به روشنی مشخص کند چه نوع استفاده‌ای مجاز است و نقض قواعد چه پیامدهایی دارد.

22. Build digital resilience
23. Acceptable Use Policy

- برای ارتباط معلمان و دانش‌آموزان خارج از چارچوب نیازهای آموزشی تعریف‌شده، مرزهای روشن و پیامدهای مشخص تعیین شود تا از تماس‌های نامناسب جلوگیری شود.
- دستورالعمل‌هایی درباره مدت مواجهه با صفحه نمایش و استفاده آموزشی از فناوری‌های پیشرفته و نوظهور، مانند هوش مصنوعی، تدوین شود.
- رضایت آگاهانه و شفافیت کامل در قبال والدین و کودکان تضمین شود؛ به‌گونه‌ای که مشخص باشد چه داده‌هایی از دانش‌آموزان جمع‌آوری می‌شود، چرا این داده‌ها جمع‌آوری می‌شوند و آیا جلسات کلاسی ضبط و ذخیره خواهند شد یا خیر.
- حریم خصوصی داده‌ها و مدیریت مناسب داده‌ها در فناوری‌های زیست‌سنجی، مانند فناوری تشخیص چهره، تضمین شود. این فناوری‌ها به‌طور گسترده در مدارس استفاده می‌شوند و ممکن است از طریق طرد، اجبار یا ایجاد مشکلات مربوط به حفاظت از داده‌ها و حریم خصوصی، به کودکان آسیب برسانند. برای مثال، استفاده از ردیابی چهره برای سنجش میزان مشارکت دانش‌آموزان توصیه نمی‌شود؛ زیرا مبانی علمی فناوری تشخیص هیجان هنوز اعتبارسنجی نشده است.

۲٫۴ دسترسی[۲۴]

ادغام حفاظت آنلاین در چارچوب‌های ایمنی مدارس: ایمنی در محیط آنلاین و آفلاین به یکدیگر مرتبط‌اند و باید به‌صورت جامع و یکپارچه مورد توجه قرار گیرند.

- تمامی سیاست‌های ایمنی مدارس، ازجمله سیاست‌های مقابله با قلدری، باید به‌طور صریح به خشونت تسهیل‌شده از طریق فناوری، مانند قلدری سایبری و آزار و اذیت آنلاین، بپردازند. این موضوع در دستورالعمل‌های ایمنی مدارس وزارت آموزش هند در سال ۲۰۲۱ نیز گنجانده شده است؛ بااین‌حال، اجرای عملی آن نیازمند توجه فوری است.
- سازوکارهای روشن، در دسترس و فراگیر برای گزارش‌دهی ایجاد و ترویج شوند تا دانش‌آموزان، معلمان و والدین بتوانند موارد سوءاستفاده را گزارش کنند. این سازوکارها باید با مسیرهای ارجاع مشخص برای دریافت حمایت روانی اجتماعی، ازجمله خط تلفنی مشاوره Manodarpan[۲۵]، مرتبط باشند.

۳٫۴ یادگیری

تقویت ظرفیت تمامی ذی‌نفعان در زمینه ایمنی دیجیتال: ایمنی مسئولیتی مشترک است و هر یک از ذی‌نفعان باید از دانش و مهارت‌های لازم برخوردار باشند.

- اجرای فرایند شناسایی و ترسیم نقشه ذی‌نفعان، با هدف روشن‌کردن نقش‌ها، مسئولیت‌ها، منافع و حوزه‌های بالقوه همکاری میان بخش‌های مختلف و در سطوح گوناگون نظام آموزشی.
- اجرای برنامه‌های مستمر و الزامی توسعه حرفه‌ای معلمان در زمینه سواد دیجیتال، سواد

24. Access
25. Manodarpanxxiii tele-helpline

هـوش مصنوعـی، شناسـایی خطـرات آنلایـن، حریـم خصوصـی داده‌هـا و آموزش‌وپـرورش تحول‌آفریـن از منظر جنسـیت.

- تدویـن برنامه‌هـای آگاه‌سـازی بـرای مدیـران مـدارس، ازجملـه مدیـران و معاونـان، دربـاره خطـرات آنلایـن، سـواد هـوش مصنوعـی، حریـم خصوصـی داده‌هـا و آموزش‌وپـرورش تحول‌آفریـن از منظر جنسـیت. ایـن برنامه‌ها بایـد توانایـی آنـان را بـرای اجـرای دسـتورالعمل‌ها و سیاسـت‌های ایمنـی مـدارس، بـا توجـه بـه خطـرات فعلـی و نوظهـور فنـاوری، تقویـت کننـد.
- گنجاندن سـواد دیجیتال، سـواد هوش مصنوعی[۲۶]، ایمنی سـایبری و شـهروندی دیجیتال[۲۷] در برنامه درسـی رسـمی و برنامه‌های فوق‌برنامه.
- اسـتفاده از جلسـات اولیـا و مربیـان و کمیته‌هـای مدیریـت مـدارس[۲۸] بـرای برگـزاری جلسـات توجیهـی کـه والدیـن را بـه مهارت‌هـای لازم بـرای نظـارت و مدیریـت ایمنـی دیجیتـال فرزندانشـان در خانـه مجهـز کنـد؛ ازجملـه مهارت‌هـای اسـتفاده ایمـن از فناوری‌هـای هـوش مصنوعـی.
- اطمینـان از اینکـه سیاسـت‌ها و قوانیـن مرتبـط بـا ایمنـی آنلایـن کـودکان، بـه زبانـی قابل‌فهـم بـرای کـودکان و والدیـن[۲۹] و بـه تمامـی زبان‌هـا در دسـترس باشـند و در اختیـار مـدارس، جوامـع محلـی و سـازمان‌های نماینـده والدیـن و کـودکان قـرار گیرنـد.

26. AI literacy
27. digital citizenship
28. parent–teacher meetings and School Management Committees(SMCs)
29. child–friendly and parent–friendly language

Unesco Chair on E-Learning and Teaching
Mehralborz University
IRAN

unesco
Chair

4 QUALITY EDUCATION

Sustainable Development Goals