

Uso de SchoolAI “Spaces” como chatbot de apoyo al estudio para alumnado de ESO en un centro público gallego. *(Simulación de informe)*

Fecha de elaboración: 29 de abril de 2026

Herramienta analizada: SchoolAI / SchoolAI Spaces

URL principal: app.schoolai.com / schoolai.com

Uso propuesto: creación de un “Space” basado en apuntes del docente para que el alumnado de ESO pueda consultar dudas y estudiar en casa de forma voluntaria, no evaluable y no obligatoria.

1. Objeto del informe

El presente informe tiene por objeto valorar, desde una perspectiva legal, ética, técnica y de protección de datos, la posibilidad de utilizar la funcionalidad **SchoolAI Spaces** como chatbot educativo de apoyo al estudio para alumnado de Educación Secundaria Obligatoria en un centro público de Galicia.

El uso previsto consiste en generar un espacio conversacional alimentado con materiales o apuntes elaborados por el docente, con la finalidad de que el alumnado pueda realizar consultas fuera del horario lectivo. Según la descripción facilitada, no se pretende utilizar la herramienta para calificar, evaluar, asignar tareas obligatorias ni adoptar decisiones académicas.

La valoración se realiza con criterio conservador, priorizando la protección de datos personales de menores y el cumplimiento del RGPD, LOPDGDD, AI Act y criterios de la AEPD aplicables al contexto educativo público. Este enfoque responde al procedimiento de evaluación institucional previsto para herramientas digitales educativas en centros públicos gallegos.

2. Alcance de la valoración

Este informe analiza exclusivamente el uso directo de SchoolAI Spaces por parte de alumnado menor de edad.

Quedan fuera de esta valoración, salvo referencia expresa, los siguientes usos:

- uso interno por el profesorado para preparar materiales;
- generación de resúmenes, preguntas de repaso o actividades no interactivas;
- uso sin datos personales del alumnado;
- uso sin acceso directo del alumnado a la plataforma;
- uso amparado por un contrato institucional ya validado por la Administración educativa competente.

3. Fuentes públicas revisadas

Para la elaboración de este informe se han considerado las siguientes fuentes públicas:

- política de privacidad de SchoolAI;
- términos de servicio de SchoolAI;
- páginas públicas de confianza, privacidad, seguridad y seguridad del alumnado de SchoolAI;
- documentación pública de SchoolAI sobre cumplimiento **FERPA, COPPA y GDPR;**

- criterios recientes de la AEPD y otras autoridades de protección de datos sobre plataformas educativas digitales;
- información oficial de la Comisión Europea sobre transferencias internacionales UE–EE. UU.;
- información oficial de la Comisión Europea sobre el enfoque de riesgo del AI Act.

SchoolAI declara en su política de privacidad que su servicio está diseñado para educadores e instituciones educativas y que se adhiere a FERPA y COPPA. La misma política reconoce derechos para personas interesadas de la UE, EEE y Reino Unido en el marco del GDPR/UK GDPR. ([SchoolAI](#))

4. Descripción funcional del uso propuesto

La funcionalidad analizada es **SchoolAI Spaces**, entendida como un espacio conversacional en el que el alumnado puede interactuar con una IA siguiendo instrucciones y materiales proporcionados por el docente.

En el caso concreto planteado, el uso tendría las siguientes características:

- finalidad de apoyo al estudio;
- uso voluntario;
- uso fuera del aula;
- ausencia de calificación;
- ausencia de obligatoriedad;
- ausencia de consecuencias académicas directas;
- base documental formada por apuntes o materiales del docente;
- interacción conversacional libre del alumnado con un sistema de IA.

Estos elementos reducen algunos riesgos pedagógicos y de evaluación, pero no eliminan los riesgos jurídicos, técnicos y de protección de datos derivados de la interacción directa de menores con una plataforma externa.

5. Hechos verificados sobre tratamiento de datos

La política de privacidad de SchoolAI declara que la plataforma puede recoger datos de cuenta, datos de estudiantes, contenido generado por usuarios, datos de uso y datos técnicos. Entre los datos de estudiantes menciona información proporcionada por instituciones educativas, docentes o los propios estudiantes, incluyendo nombres, cursos y datos de rendimiento escolar; asimismo, el contenido generado por el usuario incluye preguntas formuladas, respuestas generadas por la IA y feedback. ([SchoolAI](#))

La política también declara que puede recoger datos técnicos como dirección IP, navegador, información del dispositivo y sistema operativo, así como información sobre la interacción con el servicio. ([SchoolAI](#))

SchoolAI indica que puede compartir información con proveedores externos que prestan servicios necesarios para la plataforma, e identifica entre sus proveedores a Amazon AWS, ElephantSQL y OpenAI. La política declara además que OpenAI y otros proveedores de IA no utilizan información personal identificable, conversaciones, completions, inferencias u otros datos para entrenamiento de modelos. ([SchoolAI](#))

La plataforma declara que tiene sede en Estados Unidos y que, si se accede al servicio desde fuera de Estados Unidos, la información puede transferirse, almacenarse y tratarse en dicho país. ([SchoolAI](#))

6. Consideración sobre la declaración FERPA, COPPA y GDPR

Debe tenerse expresamente en cuenta que SchoolAI declara en su documentación pública un compromiso significativo con la privacidad y seguridad de los datos del alumnado.

En su página de confianza, SchoolAI afirma que cuenta con certificación **SOC 2 Type 2**, que no vende información del alumnado, que no utiliza datos de estudiantes para entrenar modelos de IA y que sus socios están contractualmente obligados a esos estándares. También afirma cumplimiento de FERPA, COPPA y 1EdTech. (SchoolAI)

En su página específica de privacidad, SchoolAI indica que almacena datos de estudiantes en centros de datos con certificación SOC 2 Type 2, con cifrado en tránsito y en reposo, y que mantiene cumplimiento FERPA y COPPA. También afirma que los datos de estudiantes no se venden, no se comparten con anunciantes y no se usan para entrenar modelos de IA. (SchoolAI)

Además, en documentación pública de SchoolAI se afirma expresamente que la plataforma mantiene cumplimiento con **FERPA, COPPA y GDPR**, indicando que los datos de estudiantes se protegen conforme a estándares de privacidad. (SchoolAI)

Esta declaración constituye un **elemento favorable** en la evaluación preliminar. No obstante, no equivale por sí sola a una autorización suficiente para el uso directo con alumnado menor de edad en un centro público gallego. FERPA y COPPA son marcos normativos estadounidenses y no sustituyen las obligaciones derivadas del RGPD, la LOPDGDD y los criterios de la AEPD. En cuanto al GDPR, la declaración del proveedor debe completarse con documentación verificable: contrato de encargo del tratamiento, identificación de subencargados, base jurídica del tratamiento, régimen de conservación y supresión de datos, garantías aplicables a transferencias internacionales, información a familias y alumnado, y validación por el responsable del tratamiento o Delegado/a de Protección de Datos.

Por tanto, la declaración FERPA/COPPA/GDPR **reduce parcialmente la incertidumbre**, pero **no elimina la necesidad de autorización institucional ni permite considerar automáticamente permitido el uso directo por alumnado de ESO**.

7. Análisis jurídico y de protección de datos

El carácter voluntario, no evaluable y de apoyo al estudio no elimina la existencia de tratamiento de datos personales. En un chatbot con entrada de texto libre, el alumnado puede introducir datos identificativos, académicos, familiares, emocionales o incluso datos especialmente sensibles, aunque el docente no los solicite.

Debe tenerse en cuenta que la AEPD y otras autoridades de protección de datos publicaron en marzo de 2026 un decálogo sobre contratación y uso de plataformas educativas digitales. Dichas autoridades recuerdan la protección específica que requiere el tratamiento de datos de menores y advierten que estas plataformas implican riesgos y desafíos específicos para la protección de datos personales. (AEPD)

El decálogo identifica diez puntos clave que deben tenerse en cuenta: derechos y libertades, determinación de la responsabilidad del tratamiento, legitimación y limitación de finalidades, evaluación de impacto y participación del DPD, transparencia e información, contrato de encargo y control de subencargados, garantías en transferencias internacionales, protección de datos desde el diseño y por defecto, seguridad de la información y garantía de derechos. (AEPD)

En este contexto, el uso de SchoolAI Spaces por alumnado de ESO no debería configurarse como una decisión individual de un docente, sino como una decisión institucional del responsable del tratamiento o de la Administración educativa competente.

8. Análisis de la modalidad gratuita o de cuenta docente individual

Los términos de servicio de SchoolAI establecen que, salvo acuerdo firmado separado, el uso de la tecnología se rige por sus términos generales. Para usuarios del nivel gratuito, la aceptación se produce al hacer clic en “acepto” o al usar el producto. ([SchoolAI](#))

Los mismos términos contemplan una categoría de **Free Tier Users** y señalan que no se requiere Order Form para ese tipo de usuarios. También establecen limitaciones específicas para la modalidad gratuita, incluida una limitación de responsabilidad. ([SchoolAI](#))

Este punto es especialmente relevante: una cuenta individual docente o gratuita no equivale, por sí misma, a un contrato institucional de encargado del tratamiento ni a una validación por parte del responsable del tratamiento en un centro público. SchoolAI menciona la existencia de un Data Processing Agreement cuando proceda o cuando sea exigido por la normativa aplicable, pero de la documentación pública no se desprende que dicho acuerdo quede automáticamente formalizado para cualquier docente que cree un Space desde una cuenta individual. ([SchoolAI](#))

9. Transferencias internacionales

La transferencia internacional de datos a Estados Unidos constituye uno de los elementos críticos de la valoración.

SchoolAI declara que está basada en Estados Unidos y que, si el servicio se usa desde fuera de ese país, la información puede transferirse, almacenarse y tratarse en Estados Unidos. ([SchoolAI](#))

La Comisión Europea indica que los datos personales pueden fluir libremente desde la UE hacia empresas estadounidenses que participen en el **EU-US Data Privacy Framework**. También señala que las salvaguardas adoptadas pueden facilitar el uso de otros mecanismos, como cláusulas contractuales tipo o normas corporativas vinculantes. ([European Commission](#))

Por tanto, para un uso institucional con alumnado menor de edad en un centro público gallego debería verificarse documentalmente el mecanismo concreto que ampara la transferencia: participación efectiva de SchoolAI y sus subencargados en el EU-US Data Privacy Framework, cláusulas contractuales tipo, evaluación de transferencia u otra garantía válida conforme al RGPD.

Una referencia genérica en la política de privacidad a que el usuario consiente la transferencia no se considera suficiente, por sí sola, para justificar el tratamiento de datos de menores en el marco de una actividad educativa promovida por un centro público.

10. Análisis ético y de inteligencia artificial

El uso propuesto implica interacción directa de menores con un sistema de IA generativa. Aunque la finalidad sea legítima desde el punto de vista educativo, existen riesgos de respuestas incorrectas, incompletas, sesgadas, descontextualizadas o no adecuadas al nivel madurativo del alumnado.

SchoolAI declara que sus sistemas incluyen controles de seguridad, adaptación a la edad, detección de situaciones de crisis y visibilidad completa por parte de docentes. También indica que las interacciones del alumnado pueden ser revisadas por educadores y que existen alertas ante mensajes relacionados con autolesión, abuso, negligencia o crisis. ([SchoolAI](#))

Estos mecanismos son positivos desde una perspectiva de supervisión, pero implican a su vez que la plataforma puede analizar conversaciones del alumnado y detectar contenidos sensibles. Esto refuerza la necesidad de una base jurídica clara, información previa, protocolo de actuación y delimitación de responsabilidades.

Desde la perspectiva del AI Act, la Comisión Europea identifica como sistemas de alto riesgo determinadas soluciones de IA usadas en instituciones educativas cuando pueden determinar el acceso a la educación o el curso de la vida profesional de una persona, por ejemplo mediante puntuación de exámenes. También prevé obligaciones de transparencia para chatbots, de modo que las personas sepan que interactúan con una máquina. ([Estrategia Digital Europea](#))

En el uso concreto propuesto, si el Space se limita estrictamente a resolver dudas sobre apuntes y no evalúa, no califica, no clasifica, no orienta itinerarios, no genera informes individuales ni se usa para tomar decisiones educativas, el riesgo de IA podría situarse en un nivel inferior al alto riesgo. No obstante, por tratarse de menores, contexto educativo y plataforma externa, debe mantenerse una cautela reforzada.

11. Riesgos identificados

Se identifican los siguientes riesgos:

1. **Tratamiento de datos personales de menores.**
La plataforma puede recoger contenido conversacional, datos técnicos, datos de uso y eventualmente datos identificativos o académicos.
2. **Entrada accidental de información sensible.**
El alumnado puede introducir información personal, familiar, emocional, médica o de otra naturaleza sensible en una conversación libre.
3. **Transferencia internacional de datos.**
La plataforma declara tratamiento en Estados Unidos, lo que exige garantías documentadas conforme al RGPD.
4. **Uso de subencargados y proveedores de IA.**
La plataforma utiliza proveedores externos, incluidos servicios de infraestructura y de IA.
5. **Insuficiencia de una cuenta individual docente.**
Una aceptación individual de términos no equivale a un acuerdo institucional de tratamiento de datos.
6. **Uso fuera del horario lectivo.**
El uso en casa reduce el control docente inmediato sobre las interacciones y sobre posibles incidentes.
7. **Riesgo de uso secundario de datos de interacción.**
Aunque no se pretenda evaluar, la existencia de registros de conversación puede generar tentación de usarlos para seguimiento individual.
8. **Riesgo de dependencia o sustitución del acompañamiento docente.**
Un chatbot de estudio puede inducir al alumnado a confiar en respuestas automatizadas no verificadas.
9. **Riesgo de desigualdad.**
El uso voluntario fuera del aula puede favorecer al alumnado con mejor acceso tecnológico o mayor apoyo familiar.
10. **Riesgo de indefinición de responsabilidades.**
Ante alertas de seguridad, mensajes preocupantes o incidentes, debe quedar claro quién responde, cuándo y con qué protocolo.

12. Elementos mitigadores

Constan los siguientes elementos favorables o mitigadores:

- declaración pública de no venta de datos del alumnado;
- declaración de no uso de datos de estudiantes para entrenar modelos de IA;
- declaración de cumplimiento FERPA, COPPA y GDPR;
- certificación SOC 2 Type 2 declarada por la plataforma;
- cifrado en tránsito y en reposo declarado por SchoolAI;
- control y visibilidad docente sobre interacciones;
- posibilidad de exportación y eliminación de datos según la documentación pública;
- mecanismos de alerta ante contenidos de riesgo;
- posibilidad de configurar instrucciones de edad y nivel educativo.

Estos elementos mejoran la valoración preliminar de la plataforma, pero no sustituyen las garantías formales que debe exigir un centro público o la Administración educativa antes de permitir el uso directo por alumnado menor de edad.

13. Criterio técnico sobre el uso propuesto

No se considera jurídicamente prudente habilitar el uso directo de SchoolAI Spaces por alumnado de ESO como iniciativa individual de un docente, aunque el uso sea voluntario, no obligatorio, no evaluable y de apoyo al estudio.

El elemento determinante no es la finalidad pedagógica, sino la existencia de interacción directa de menores con una plataforma externa de IA que recoge contenido conversacional y datos técnicos, utiliza proveedores externos y puede implicar transferencia internacional de datos.

El uso podría reconsiderarse únicamente si se formula como **piloto institucional controlado**, con documentación previa suficiente, autorización formal y medidas técnicas, jurídicas y organizativas específicas.

14. Condiciones para convertirlo en un piloto viable

Para que el uso de SchoolAI Spaces pudiera pasar de una situación de **no recomendable/no permitido como iniciativa individual** a una situación de **piloto institucional potencialmente viable**, deberían cumplirse las siguientes condiciones.

14.1. Documentación previa imprescindible

Antes de iniciar el piloto, deberían recabarse y conservarse, como mínimo, los siguientes documentos:

Documento requerido	Finalidad
Informe de necesidad educativa	Justificar por qué se necesita el chatbot y qué objetivo educativo concreto cumple.
Informe de proporcionalidad	Acreditar que no existe una alternativa institucional menos intrusiva o más segura.

Documento requerido	Finalidad
Contrato de encargo del tratamiento / DPA	Regular el tratamiento de datos conforme al RGPD.
Relación de subencargados	Identificar proveedores que acceden o tratan datos: IA, alojamiento, bases de datos, analítica, soporte.
Garantías de transferencias internacionales	Verificar EU-US Data Privacy Framework, cláusulas contractuales tipo u otro mecanismo válido.
Política de conservación y eliminación	Determinar plazos de retención, borrado de conversaciones, copias de seguridad y eliminación al finalizar el piloto.
Registro de actividades de tratamiento	Incorporar o actualizar el tratamiento vinculado al piloto.
Análisis de riesgos o evaluación de impacto	Valorar riesgos para derechos y libertades del alumnado, especialmente por menores e IA.
Informe o validación del DPD	Contar con revisión del Delegado/a de Protección de Datos.
Información a familias y alumnado	Explicar finalidad, funcionamiento, datos tratados, derechos y alternativa disponible.
Protocolo de incidencias	Definir actuación ante datos sensibles, mensajes de riesgo, errores graves o incidentes de seguridad.
Instrucciones de uso aceptable	Establecer normas claras para alumnado y profesorado.

La AEPD y otras autoridades han identificado precisamente estos ámbitos como puntos clave para plataformas educativas digitales: responsabilidad, legitimación, evaluación de impacto, DPD, transparencia, contrato de encargo, subencargados, transferencias internacionales, privacidad desde el diseño, seguridad y derechos de las personas. ([AEPD](#))

14.2. Decisiones institucionales necesarias

Para que el piloto sea defendible, deberían adoptarse al menos las siguientes decisiones:

- Aprobación expresa por el equipo directivo.**
El piloto no debe ser una decisión individual del docente.
- Consulta y validación por el Delegado/a de Protección de Datos.**
Debe revisarse el tratamiento de datos antes de iniciar el uso con menores.

3. **Determinación del responsable del tratamiento.**

En un centro público, debe aclararse si la responsabilidad corresponde al centro, a la Administración educativa o al órgano que determine la normativa aplicable.

4. **Definición de la base jurídica.**

Debe identificarse si el tratamiento se ampara en misión educativa/interés público, consentimiento u otra base válida. En caso de consentimiento, deben contemplarse las limitaciones aplicables a menores.

1. **Aprobación de la configuración técnica.**

El centro debe aprobar cómo se crean los Spaces, qué datos se suben, quién accede, qué registros se conservan y cuándo se eliminan.

2. **Designación de responsables operativos.**

Debe indicarse quién administra la herramienta, quién supervisa las interacciones y quién responde ante incidencias.

3. **Autorización de comunicaciones a familias.**

Las familias deben recibir información comprensible antes del inicio del piloto.

4. **Garantía de alternativa equivalente.**

El alumnado que no participe debe disponer de una vía de apoyo al estudio equivalente, sin perjuicio académico ni discriminación.

14.3. Configuración mínima del piloto

El piloto debería configurarse con restricciones estrictas:

- no introducir nombres, apellidos, correos, fotografías ni identificadores del alumnado;
- no cargar listados de clase;
- no cargar calificaciones;
- no cargar informes psicopedagógicos;
- no cargar datos de salud;
- no cargar trabajos del alumnado identificables;
- no permitir que la herramienta genere calificaciones, rankings, perfiles o recomendaciones académicas individualizadas;
- no usar Mission Control ni analíticas para evaluación o seguimiento individual;
- usar alias no identificativos;
- limitar el Space a contenidos curriculares y apuntes del docente;
- incluir instrucciones explícitas al alumnado para no introducir datos personales;
- configurar mensajes iniciales de advertencia sobre uso responsable;
- revisar periódicamente las conversaciones solo con finalidad de seguridad y mejora del recurso, no de evaluación;
- eliminar conversaciones conforme al plazo aprobado;
- documentar cualquier incidencia.

14.4. Comunicación mínima a familias y alumnado

La comunicación previa debería incluir, al menos:

- finalidad del piloto;

- carácter voluntario;
- duración prevista;
- herramienta utilizada;
- responsable del tratamiento;
- datos que pueden tratarse;
- datos que no deben introducirse;
- existencia de IA generativa;
- posibilidad de errores o respuestas inexactas;
- indicación de que no sustituye al profesorado;
- advertencia de que no debe usarse para situaciones personales, médicas, emocionales o urgentes;
- derechos de acceso, rectificación, supresión, oposición y otros aplicables;
- contacto del centro o DPD;
- alternativa equivalente para no participantes.

14.5. Criterios de suspensión del piloto

El piloto debería suspenderse inmediatamente si concurre cualquiera de las siguientes circunstancias:

- ausencia de contrato de encargo o DPA suficiente;
- falta de garantías claras para transferencias internacionales;
- tratamiento de datos identificativos no previsto;
- introducción reiterada de datos sensibles por parte del alumnado;
- uso de conversaciones para evaluar o perfilar;
- ausencia de respuesta adecuada ante incidentes;
- oposición fundada del DPD;
- imposibilidad de garantizar derechos de acceso, supresión o limitación;
- cambios sustanciales en términos, privacidad o subencargados sin revisión previa.

15. Veredicto técnico

15.1. Uso directo por alumnado desde iniciativa individual docente

No permitido / no recomendable.

No se considera admisible que un docente, a título individual, cree un Space y lo comparta directamente con alumnado de ESO para uso en casa sin autorización institucional, sin DPA, sin revisión del DPD y sin garantías documentadas de transferencia internacional.

15.2. Uso como piloto institucional

Potencialmente permitido con restricciones, pendiente de validación formal.

Podría ser viable únicamente si se aprueba como piloto institucional controlado y se cumplen las condiciones documentales, jurídicas, técnicas y organizativas indicadas en este informe.