ECIJA

NOTA INFORMATIVA

Responsabilidades y obligaciones en la utilización de dispositivos digitales en la enseñanza infantil, primaria y secundaria

La Agencia Española de Protección de Datos (AEPD) ha emitido una Guía sobre el uso de dispositivos digitales en centros educativos de enseñanza infantil, primaria y secundaria.

Lo que necesitas saber

- Los centros educativos deben implementar medidas para regularizar el uso de dispositivos digitales en el entorno educativo, tales como teléfonos móviles, portátiles y tablets etc.

- Valorar la necesidad del uso de dispositivos uso en la actividad educativa se configura como un factor clave para su regulación. Los centros pueden prohibir, limitar o no regular el uso de dispositivos digitales, lo que impactará a su nivel de responsabilidad y el nivel de riesgos para la privacidad de los alumnos.

- Los centros deben asegurarse de que los proveedores de servicios externos (como las plataformas educativas) no realicen actividades no autorizadas que excedan de la función educativa, protegiendo así los datos personales de los alumnos.

- El uso de dispositivos digitales puede generar riesgos de discriminación y patrones adictivos. Es fundamental que los centros educativos utilicen estos dispositivos de manera responsable y consciente, priorizando la protección de la privacidad y seguridad de los alumnos.

La Agencia Española de Protección de Datos (AEPD) ha emitido una Guía sobre el uso de dispositivos digitales en centros educativos de enseñanza infantil, primaria y secundaria(responsabilidades-uso-dispositivos-moviles-centros-docentes.pdf(aepd.es)). La Guía aborda la evolución del uso de estos dispositivos, que han pasado de ser ordenadores de escritorio administrados por los centros a dispositivos personales como teléfonos móviles, portátiles y tablets, que pertenecen a los alumnos o sus familias.

Los alumnos generan mucha información personal mientras utilizan este tipo de **dispositivos por lo que los centros educativos deben valorar la conveniencia de** su utilización en las aulas y concienciar a los alumnos sobre los riesgos asociados, prestando especial atención a aquellas situaciones en las que los datos personales de los alumnos pueden ser accesibles por terceros.

En relación con lo anterior, esta nota informativa expone los aspectos más relevantes mencionados por la Guía.

(I) Legitimación para el tratamiento de los datos

Para poder llevar a cabo estos tratamientos, los centros deberán contar con la habilitación legal que les capacite para ello. Como responsables del tratamiento, los centros están legitimados para tratar los datos personales de los alumnos con base en **el cumplimiento de una misión de interés público**.

Esta base de legitimación habilita a los centros a llevar a cabo todas aquellas actividades de tratamiento que sean necesarias para conseguir el fin pedagógico que tienen encomendado, incluyendo datos de categoría especial relacionados con su salud (con el objetivo de proteger los intereses vitales de los alumnos o por existir un interés público esencial), su orientación sexual, raza, sexo, etc.

Sin embargo, esta habilitación no alcanza al **uso de la imagen de los menores** con fines promocionales o de difusión de determinadas actividades a través de redes sociales u otras plataformas. Por tanto, en estos casos, será necesario recurrir al **consentimiento** del alumno o de sus representantes legales.

En función de la actividad, se plantean distintos escenarios que determinarán los riesgos del tratamiento, los protocolos a implementar por los centros y las distintas relaciones entre los actores que forman parte del tratamiento (alumnos, docentes, el propio centro y terceros ajenos a la organización).

(II) Protocolos para el uso de dispositivos digitales

El aumento significativo en el uso de los dispositivos digitales por parte de los alumnos requiere que los centros educativos adopten medidas de **prohibición o limitación de su uso.** En función de los distintos protocolos que los centros educativos implementen, la AEPD diferencia distintos efectos y responsabilidades.

- **Prohibición de llevar y usar teléfonos móviles en los centros:** En este supuesto, los alumnos deberán depositar sus dispositivos en lugares designados y recogerlos al finalizar la jornada escolar. En caso de que se produzca un tratamiento ilícito

por parte de los alumnos, como puede ser la difusión de datos de otros alumnos, profesores, difusión de videos, etc., los mayores de 14 años podrían recibir una multa, y sus padres o tutores legales serían responsables solidarios del pago. No obstante, si el centro educativo no actuase con la diligencia debida respecto al uso de los dispositivos, podría responder solidariamente ante la multa impuesta por la AEPD.

- **Limitación del uso de los dispositivos digitales en el aula:** Esta situación se produce cuando el centro permite el uso de los dispositivos para determinadas actividades de carácter educativo, como puede ser realizar búsquedas en internet, el uso de un código QR para acceder a un cuestionario, etc. En estos casos, los centros serán responsables del tratamiento, siempre que el uso de estos servicios o productos digitales haya sido autorizado/aprobado por ellos, como podría ser el uso de ordenadores portátiles, tablets, teléfonos móviles u otros para llevar a cabo actividades educativas por los alumnos.

  En consecuencia, la AEPD invita a que los docentes reflexionen sobre si la utilización de los dispositivos es **adecuada, necesaria y si existen alternativas menos intrusivas que respeten la privacidad de los alumnos**, examinando si el uso de los dispositivos aporta más beneficios que perjuicios a los derechos e intereses de los alumnos.

- **Ausencia de regulación sobre su uso:** Es el supuesto más complejo, por lo que los diversos usos de estos dispositivos se analizarán caso por caso para verificar la responsabilidad de los agentes implicados. Los centros educativos serán responsables cuando los alumnos cometan un tratamiento ilícito por el uso de dispositivos o aplicaciones autorizados por el centro, al carecer de regulación para su uso. En sentido contrario, en el caso de que el alumno cometa una infracción en materia de protección de datos sin atender a las indicaciones que se han dado desde el centro, el centro podría quedar eximido de responsabilidad. Esta ausencia de regulación del uso de los dispositivos en los centros educativos entraña un riesgo para los alumnos, los cuales pueden llegar a no ser conscientes de las consecuencias para ellos y para la privacidad de terceros, compartiendo datos de otros alumnos, docentes o miembros de la organización (a través de sus propias redes sociales como Instagram o Facebook, aplicaciones de mensajería como WhatsApp, etc.).

(III) Tipos de tratamiento

En función de los distintos escenarios posibles, la AEPD califica los tipos de tratamientos que se pueden llevar a cabo a través de los dispositivos, para la función educativa, para lo cual pueden estar implicados proveedores de servicios ajenos a los centros educativos (por ejemplo, Google for Education, Microsoft Teams, Edusing, etc.):

- Tratamientos para acceso a contenido docente.

- Tratamientos de comunicación alumno – profesor.

- Tratamientos para dirigir el proceso formativo del alumno.

- Tratamientos para la gestión de actividades o asistencia directamente con el alumno.

Así, el uso de datos personales en el marco de estas actividades, combinadas con la intervención de terceras entidades o individuos que no forman parte de la organización, debe ser supervisado por los centros, puesto que suponen la comunicación de datos a terceros, que serán encargados de tratamiento.

(IV) Implicaciones de terceros en el tratamiento de los datos

A menudo, como se ha mencionado en el apartado anterior, las plataformas o sistemas que utilizan los alumnos conllevan la participación de terceras entidades o individuos que no forman parte de la organización, que actúan como proveedores, y tienen la calificación de **encargados de tratamiento**, en la mayoría de las ocasiones.

Cuando se recurre a un proveedor de servicios, los centros deberán actuar diligentemente en su elección, de manera que se garantice no se llevan a cabo más actividades que las indicadas por el centro y que se cumplan **las indicaciones establecidas por ellos**. En ocasiones, estos proveedores establecen relaciones independientes con el alumno, lo cual supone el tratamiento de sus datos personales para otros fines ajenos a los previstos por los centros (formularios dentro de las apps, habilitar enlaces que redirijan a otros sitios web, publicidad, etc.).

Estas nuevas actividades son **ajenas a la supervisión y control** de los centros, lo que supone un alto riesgo tanto para los propios centros como para los alumnos.

En este sentido, la AEPD incide en que los centros deben poner el foco en **garantizar** que los servicios que proporcionan estos proveedores de servicio no condicionen a los alumnos a establecer nuevas relaciones que impliquen otros tratamientos de datos personales.

(V) Riesgos derivados del uso de dispositivos digitales

El uso de los dispositivos digitales descritos no solo implica riesgos en materia de protección de datos, sino que también pueden poner de manifiesto **posibles desigualdades** para que los alumnos accedan a ellos, cuando los dispositivos no se proporcionen desde los centros, debido a las condiciones económicas, el acceso a la red, la situación familiar, etc.

Por otra parte, los alumnos pueden no ser conscientes de los riesgos a la hora de compartir datos personales de ellos mismos, sus compañeros u otros miembros de la comunidad educativa. Por ello, la **AEPD resalta la importancia** de estos riesgos, cuando el tratamiento de datos va más allá de los estrictamente necesarios para el ejercicio de la función educativa, máxime si su uso **expone a los alumnos** a patrones adictivos o persuasivos, que pueden afectar a la salud mental de los alumnos.

(VI) Conclusiones

Con la publicación de esta Guía, la AEPD invita a la reflexión de si el uso de los dispositivos digitales es estrictamente necesario para la función educativa, considerando el riesgo para la privacidad de los alumnos.

Por otra parte, en caso de que se considere necesario el uso de dispositivos digitales, los centros deben tener presente su deber como responsables, guardando especial atención al control de los proveedores de servicios que tengan acceso a los datos personales de los alumnos.

En síntesis, es fundamental que los centros educativos conozcan los riesgos que implica el uso de los dispositivos digitales y que se utilicen de manera responsable y consciente en los entornos educativos, para poder asegurar que se respete la privacidad y la seguridad de los alumnos.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60