Comunidad de Madrid

CONSEJERÍA DE EDUCACIÓN
E INVESTIGACIÓN

Política de protección de datos

Consejería de Educación
Comunidad de Madrid

Curso 2020/2021

I.E.S. Joaquín Rodrigo

Información extraída de informes y recomendaciones de:

Enlace al documento completo

Legislación vigente

- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

de 27 de abril de 2016
relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Plena aplicación desde el 25 de mayo de 2018.

- **Ley Orgánica 3/2018 (LOPDGDD)** de 5 de diciembre, de Protección de Datos Personales garantía de los derechos digitales.

- **Ley Orgánica 2/2006**, de 3 de mayo, de Educación.

¿Qué es un dato de carácter personal?

Toda información sobre una persona física identificada o identificable («el interesado»).

Se considerará **persona física identificable** toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Uso de recursos propios de Educamadrid

- Portal educativo
- Correo web
- Mensajería instantánea
- Cloud Educamadrid
- Aula virtual
- Mediateca
- Bibliotecas
- MOOC
- Recursos TIC

Comunidad de Madrid

CONSEJERÍA DE EDUCACIÓN
E INVESTIGACIÓN

Uso de nuevas plataformas

- Microsoft Teams
- WebEx
- JITSI
- Aula Planeta

Comunidad de Madrid

CONSEJERÍA DE EDUCACIÓN
E INVESTIGACIÓN

Responsabilidad del tratamiento de datos

Herramientas y recursos propios

- En los centros educativos de **titularidad privada o privado - concertada**, el responsable del tratamiento de datos es el propio centro.
- En los **centros educativos públicos**, el responsable es la Consejería de Educación e Investigación.
- Aunque la **dirección de un centro público** ejerce sus competencias de acuerdo con la autonomía de gestión que le otorga la LOE, **NO ES RESPONSABLE** del tratamiento de datos de carácter personal, dado que el centro público no es un órgano directivo con capacidad de decisión sobre el tratamiento de datos personales, sino que forma parte de la estructura orgánica de la Consejería.

Comunidad de Madrid

CONSEJERÍA DE EDUCACIÓN
E INVESTIGACIÓN

Política de privacidad y seguridad

Recursos nuevos

- **Responsable del tratamiento de mis datos**: Consejería de Educación y Juventud (Dirección General de Bilingüismo y Calidad de la Enseñanza, Dirección General de Educación Infantil y Primaria y Dirección General de Educación Secundaria, FP y RE).
- **Licitud del tratamiento**: el centro docente y la Administración educativa están legitimados para recabar y tratar los datos personales, conforme lo dispuesto en la LOE 2/2006:

  c) el tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

  e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

- **Tratamientos de datos** (elaboración de perfiles): no se realizan.
- **Comunicación de datos a terceros** (materiales didácticos): alumnos y familiares para uso personal.
- Para **ejercer los derechos en la política de protección de datos**: https://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos

Comunidad de Madrid

CONSEJERÍA DE EDUCACIÓN E INVESTIGACIÓN

Licitud del tratamiento

Recursos nuevos

2.C.24 (página 3 del documento que recoge la política de protección de datos de la Consejería de Educación de la CAM).

ACTIVIDAD DE TRATAMIENTO

Utilización por parte del profesorado y del alumnado, en el ejercicio de la función educativa, de las herramientas y recursos de la plataforma educativa de servicios online de la Consejería de Educación e Investigación (EducaMadrid)

BASE JURÍDICA

RGPD 6.1 e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

FINES DEL TRATAMIENTO

Proporcionar al alumnado y los docentes entornos de aprendizaje online, así como herramientas de comunicación (correo electrónico educativo, mensajería instantánea, etc.), de colaboración (cloud, webs, foros, etc.) y de elaboración de materiales educativos (gestor de contenidos).

COLECTIVO DE INTERESADOS

Alumnos, empleados, ciudadanos

CATEGORÍA DE DATOS PERSONALES

Datos de carácter identificativo, datos académicos y profesionales.

Nombre y apellidos, DNI, NIE, NIA, correo electrónico, foto, dirección, número de teléfono, firma.

CESIONES

No se realizan cesiones de datos personales

Uso de aplicaciones ajenas a las de CM

Deben utilizarse únicamente aquellas aplicaciones que ofrezcan información sobre:

- los tratamientos efectuados,
- las finalidades de los tratamientos y sus responsables,
- información sobre la ubicación de los datos,
- el periodo de retención,
- garantías con relación a su seguridad.

Uso de aplicaciones ajenas a las de CM

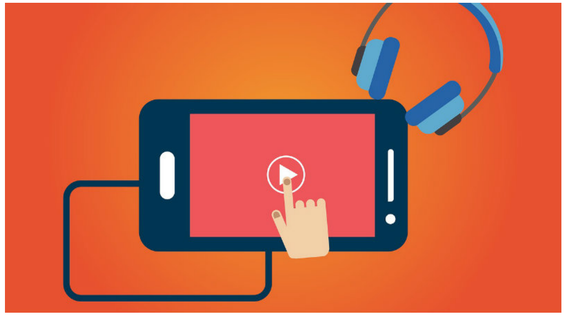
- Las aplicaciones educativas ajenas a las de CM "**deben estar incluidas en la política de seguridad de los centros educativos**".
- Se debe solicitar la autorización al **responsable del tratamiento**, que en el caso de los centros públicos es la **Dirección General competente** (Dirección General de Bilingüismo y Calidad de la Enseñanza). Correo electrónico: protecciondatos.educacion@madrid.org
- La solicitud conlleva la **evaluación de la aplicación** desde el punto de vista de la seguridad de la información y la privacidad de los datos personales.
- **Solo tras la autorización** el centro podrá aprobar su puesta en funcionamiento y su incorporación a la PGA.
- Los centros **deben informar a los padres o tutores** del comienzo de la utilización de las aplicaciones y plataformas.
- Informe completo.

Responsabilidad del tratamiento de datos

Aplicaciones educativas externas

- El uso de aplicaciones educativas externas **sólo está justificado** cuando no se hayan puesto a disposición de los centros los medios o herramientas equivalentes.
- Se requerirá la **autorización de la Dirección General de Bilingüismo y Calidad de la Enseñanza**, por ser competente en fijar las directrices de uso de las aplicaciones y plataformas educativas. Correo electrónico: protecciondatos.educacion@madrid.org.
- Se debe realizar una **evaluación de cada aplicación** desde el punto de vista de seguridad de la información.
- Una vez autorizado el uso de una aplicación, **el centro educativo la deberá incluir en la PGA** justificando su uso e incorporando la información sobre los tratamientos de datos.
- Toda la información **deberá ponerse en conocimiento a las familias y los alumnos mayores de 14 años** a través de su publicación en la página web del centro y de cualquier otro medio que asegure la recepción.
- Cuando en la aplicación se vayan a incorporar datos personales, el centro deberá recabar el **consentimiento de las familias y de los alumnos** para el tratamiento de los datos por la empresa prestadora del servicio.
- Cuando la App vaya a utilizarse dentro del centro educativo en **dispositivos móviles ajenos a la Consejería** (ordenador portátil, tableta o teléfono móvil propiedad del profesor), **estos dispositivos se están integrando en la red de la corporación**. Si se permite su uso, debe establecerse una política reguladora del ámbito al que pueda afectar (gestión de tareas, gestión del aula, etc.)

Grabaciones de contenido audiovisual



Enlace al documento completo

Grabaciones que NO requieren consentimiento previo (sí el deber de informar)

- **Grabación con fines de control laboral**. El centro habrá de informar con carácter previo y de forma expresa, clara y concisa acerca de esta medida. Existen excepciones y limitaciones.
- **Grabaciones de videovigilancia**. La medida debe ser proporcional a la finalidad que ha motivado la instalación de las cámaras. Existen excepciones y limitaciones.
- **Grabaciones de actividades educativas**. Su uso es avalado por la LOE, por lo que no es preceptivo solicitar consentimiento.

- **Publicación por parte del centro de imágenes, vídeos o voz del alumnado en Internet abierto**: no es preciso el consentimiento cuando se hace de manera que no sea posible la identificación de las personas que aparecen (de espalda, de lejos, etc.). Es recomendable poner las imágenes a disposición de las familias antes de su publicación.
- **Grabación de un progenitor a un profesional docente (profesor o tutor)**. Posible vulneración del derecho a la intimidad y del secreto de las comunicaciones (sentencias del Tribunal Supremo definen cuándo no constituyen intromisión).
- **Grabación de una sesión docente por parte del profesional**. Debe limitarse su acceso al personal docente y a los alumnos a los que vaya dirigida sin que pueda ser utilizada para otros fines, como su divulgación pública, que requeriría el consentimiento expreso de los afectados.

La grabación NO constituye una vulneración del marco legal si:

- El padre o el tutor participa en la conversación que él mismo graba.
- La conversación grabada versa exclusivamente sobre la educación de su hijo o tutelado (interés legítimo).
- La persona que realiza la grabación informa previamente a su realización a las personas que van a ser grabadas (deber de informar).

El padre o tutor legal que realiza la grabación se considerará responsable del tratamiento, por lo que tiene el deber de preservar la grabación y no difundirla ni exponerla a terceros y destruirla cuando haya dejado de ser necesaria para los fines perseguidos.

Información legal al inicio de la grabación de una sesión de clase

"En cumplimiento de la legislación vigente* en la materia de protección de datos personales, se informa a los alumnos y a sus familias de que esta sesión va a ser grabada. La grabación se guardará de forma segura en _____(por ejemplo, Cloud de Educamadrid, Microsoft Stream, etc.) y será conservada durante el tiempo necesario para el uso exclusivamente educativo.

Si los alumnos o sus familias desean grabar la sesión, previamente deben pedir el consentimiento al profesor y deben saber que el destino de la grabación debe ser exclusivamente para el uso en el ámbito personal y familiar, siendo ellos los únicos responsables de un eventual uso inadecuado de las mismas.

La distribución, copia o utilización de esta grabación, cualquiera que fuera su finalidad, están prohibidas por la legislación vigente y puede ser objeto de una sanción económica por parte de la *Agencia Española de Protección de datos, de acuerdo con el Título IX de la LOPDGDD (artículos 70 a 78).*"

Grabaciones que SÍ precisan consentimiento previo

- **Grabación de una sesión docente por parte del alumnado.** Debe ser fundada en motivos pedagógicos, lo que únicamente puede decidir el profesor. Es necesario el consentimiento del docente y del resto de los alumnos.
- **Grabación de la reunión del Claustro de profesores o del Consejo Escolar**. *"**Podrán** grabarse las sesiones que celebre el órgano colegiado. El fichero resultante de la grabación, junto con la certificación expedida por el Secretario de la autenticidad e integridad del mismo, y cuantos documentos en soporte electrónico se utilizasen como documentos de la sesión, podrán acompañar al acta de las sesiones, sin necesidad de hacer constar en ella los puntos principales de las deliberaciones."* (Ley 40/2015 de Régimen Jurídico del Sector Público, arts. 15 - 18). **No es una imposición legal, sino una posibilidad**, por lo que la decisión de grabar o no las sesiones debería adoptarse por acuerdo de la mayoría de los miembros del órgano correspondiente.
- **Grabación de actividades complementarias voluntarias y extraescolares.** Se necesita el consentimiento para la difusión de cualquier contenido audiovisual entre las familias. Es decir, un padre no se puede oponer a que se grabe a su hijo con fines educativos, pero sí puede oponerse a que se difundan sus datos personales. Si son los padres los que realizan las grabaciones, los autores y los receptores de las grabaciones son los únicos responsables del uso inadecuado de las mismas.

Comunicación de datos personales y envío de documentación a través de medios electrónicos

- **La comunicación de datos personales debe efectuarse de la manera más segura posible,** por lo que deberá remitirse por canales oficiales (aplicaciones corporativas accesibles a través de la intranet y del registro electrónico).
- **Excepcionalmente**, si no es posible, podrá emplearse el **correo electrónico**, aunque no constituye un medio notificación ya que no permite asegurar la constancia fehaciente de la entrega y recepción por el destinatario.
- Cuando no se disponga de un medio oficial conveniente o adecuado, el correo electrónico debe ser la última opción. La DPD recomienda el uso del sistema de Nube en red.
- **Precauciones para el envío de la documentación por coreo electrónico:**

1. Los datos personales deberán incorporarse en **documentos anexos cifrados**. No se consignarán datos personales en el campo de asunto ni en el texto del mensaje. Para identificar el contenido pueden emplearse datos como el número de expediente o las iniciales de nombre y apellidos de la persona.
2. Se incluirá un texto explicando que la información de carácter personal se incluye cifrada proporcionando un contacto distinto del mismo correo electrónico para que el destinatario final pueda **recabar la clave del descifrado** que debe contener al menos ocho caracteres con minúsculas, mayúsculas, números, símbolos o signos de puntuación.

Los mensajes de correo electrónico deben incorporar la siguiente advertencia

"Este mensaje va dirigido de manera exclusiva a su destinatario y la información contenida en él, así como la que consta en cualquiera de sus ficheros adjuntos, es RESERVADA y CONFIDENCIAL. Si usted lee este mensaje y no es el destinatario indicado (o responsable de remitirlo a la persona indicada) por favor, comuníquenoslo por este medio y proceda a destruirlo o borrarlo. En todo caso absténgase de utilizar, reproducir, alterar, archivar, o comunicar a terceros el presente mensaje y/o ficheros anexos, pudiendo incurrir, en caso de llevar a cabo tales acciones, en responsabilidades legales."

Técnica de cifrado de archivos mediante la aplicación JZIP (para correos electrónicos, CD o DVD).
Técnica de cifrado al dispositivo de manera integral (USB).

Transporte de documentos

- En el caso de **documentos digitalizados o en formato electrónico**, se aconseja el uso del servicio Cloud de EducaMadrid para garantizar un acceso seguro.

- Transporte de documentos en **dispositivos de almacenamiento físico** (USB, CD, DBD), es recomendable que la información se cifre previamente a su almacenamiento en el dispositivo.

Medidas de seguridad

- **Violaciones de seguridad de los datos personales:** toda violación de la seguridad que ocasiona la destrucción, la pérdida o la alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o el acceso no autorizados a estos datos.
- **Situaciones**:
    - pérdida o el robo de un dispositivo,
    - el acceso no autorizado a la base de datos (incluso por parte del propio personal),
    - el envío de información personal a un destinatario erróneo,
    - la alteración de datos sin autorización o la pérdida de disponibilidad de los datos (por ejemplo, por haber sufrido un ataque a los sistemas con un software de secuestro, ransomware, que cifra los datos).
- **Si se produce una violación de la seguridad de los datos**, el responsable de tratamiento la notificará a la autoridad de control sin dilación indebida y, si es posible, en un plazo máximo de 72 horas, salvo cuando sea improbable que constituya un riesgo para los derechos y las libertades de las personas (artículo 33 del RGPD).
- El responsable **deberá comunicarlo a las personas afectadas**, sin dilaciones indebidas y en un lenguaje claro y sencillo, a menos que la información esté cifrada, no existe riesgo alto o suponga un esfuerzo desproporcionado.

Recomendaciones que deberían incluirse la PGA

- Los usuarios deben **tener especial cuidado al publicar imágenes y vídeos mediante Apps y herramientas en nube** para no poner en riesgo la intimidad de otras personas, independientemente del tipo de aplicación, sea esta corporativa o no.
- Se recomienda **leer la información sobre la política de privacidad y condiciones de uso** antes de empezar a utilizar cualquier herramienta y siempre evitar introducir información de carácter confidencial.
- Antes de utilizar **las redes sociales** se recomienda **informar y formar** a los alumnos sobre la configuración de opciones de privacidad en el perfil de usuario.
- Al facilitar datos de cualquier ámbito, se debe **evitar incorporar datos como el domicilio de los menores y otros datos personales** que puedan poner en riesgo su seguridad.
- **Las contraseñas deben ser robustas**, evitando las que sean fáciles de adivinar por otras personas, con suficientes caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales.
- Acceso a fichas didácticas para los alumnos.

Recomendaciones que deberían incluirse en el RRI

- Retrasos/faltas de asistencia, abandonos de las videoconferencias.
- Incumplimiento de las normas de participación online.
- Faltas de respeto a los compañeros / profesores online.
- Suplantación de la identidad.
- Difusión de las imágenes grabadas sin permiso.
- Cyberbulling.
- Incorrecciones en el formato de correos electrónicos.
- Incumplimiento de las normas de presentación de trabajos.
- ¿?

IES Joaquín Rodrigo
Curso 2020/2021

agencia española protección datos

Delegación de protección de datos
CONSEJERÍA DE EDUCACIÓN Y JUVENTUD