
# Protección de Datos. Profesorado SAED, PTSC y Orientadores

## Parte II

Ponente:
Herminia Gil Pérez.
Jefa del Servicio de Protección de Datos de la Delegación de Protección de Datos en la Consejería de Educación y Juventud 917200468

Protecciondatos.educacion@madrid.org

www.dpd.educa2.madrid.org

# PARTES I Y II

1. Legislación relacionada con la educación y la protección a menores.
2. La responsabilidad del docente en la protección de datos personales e identidad digital de los alumnos.
3. Análisis y gestión de riesgos del tratamiento de datos sensibles.
4. La seguridad en el tratamiento informático de la información
5. El uso del correo electrónico, la mensajería instantánea y el Registro electrónico de la Administración.
6. El intercambio seguro de información.
7. EducaMadrid, un entorno fiable, confidencial y disponible para los docentes.

# SEGUNDA PARTE

4. La seguridad en el tratamiento informático de la información
5. El uso del correo electrónico, la mensajería instantánea y el Registro electrónico de la Administración.
6. El intercambio seguro de información.
7. EducaMadrid, un entorno fiable, confidencial y disponible para los docentes.

# 4. La seguridad en el tratamiento informático de la información

## ¿Cómo saber si estamos haciendo un tratamiento seguro de la privacidad?

# Grabaciones de voz y de imagen

- Desde el punto de vista de protección de datos debemos valorar:

- El derecho a la intimidad: por ejemplo, una conversación grabada entre jefe y empleado es legal si ha versado únicamente sobre temas profesionales y no personales.
- El secreto de las comunicaciones: Si intervenimos en la conversación grabada, no se considera vulnerado el secreto.
- El derecho a la información.


Aunque la grabación pueda ser legal, la publicación o difusión puede constituir una infracción del derecho a la intimidad.

# Grabaciones de voz

Para que una grabación pueda considerarse un medio de prueba, los Tribunales exigen:

1. Que no exista provocación, engaño o coacción por parte del sujeto que graba.
2. Que el sujeto que graba forma parte activa de la conversación, siendo partícipe en la misma.
3. Que se grabe en un lugar público.
4. Que si se graba en un lugar privado se tenga autorización o consentimiento del titular.

No obstante, la propia Ley de protección de datos exime de la necesidad de consentimiento cuando con los datos obtenidos en la grabación se pretenda la satisfacción de un interés legítimo, como es la necesidad de probar una conversación en un procedimiento judicial.

# Grabaciones de voz

La normativa sobre protección de datos establece para el responsable del tratamiento (padre o **tutor que realiza la grabación**) el **deber de informar** a las personas de las que está recogiendo la información (**profesores que participan** en la conversación con el padre o tutor) sin que sea necesario recabar su consentimiento.

La grabación no constituiría una vulneración del marco legal si se cumplen las siguientes condiciones:

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

# Grabaciones de imagen

Para grabar a personas en lugares públicos debemos distinguir la finalidad que se pretende conseguir:

- Grabar imágenes en público con fines informativos, como hacen los medios de comunicación, es legal cuando se graba a personajes públicos o cuando la imagen es casual o accesoria y lo relevante es la información.
- Publicar o difundir las imágenes grabadas con fines publicitarios o comerciales, no es legítimo y se requiere el consentimiento explícito de las personas grabadas.
- Si publicamos en Youtube, aunque no seamos una empresa, se supone un interés de promoción, independientemente de que exista o no beneficio económico.

https://www.elmundo.es/espana/2020/02/26/5e558c13fdddff0d738b460b.html

# Grabaciones de imagen

Podemos grabar a personas en lugares públicos o privados con el fin de proteger bienes o con fines disuasorios, es decir, por motivos de seguridad. Entonces hablamos de **videovigilancia**.

Grabar imágenes con un interés público o legítimo, debe cumplir con los principios de limitar la finalidad y minimizar la captación de los datos estrictamente necesarios.

La información necesaria sobre esta actividad de tratamiento debe encontrarse expuesta al público en lugares accesibles.


http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos

CONSEJERÍA DE EDUCACIÓN Y JUVENTUD
Comunidad de Madrid

# ZONA VIDEOVIGILADA

**RESPONSABLE:**

Dirección General de Educación Infantil y Primaria

**PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:**

- Centro educativo
- Dirección General de Educación Infantil y Primaria
  C/ Alcalá, nº 32, 28014 Madrid (dgeip.educacion@madrid.org)
- Delegado de Protección de Datos de la Consejería de Educación y Juventud (protecciondatos.educacion@madrid.org)

**MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:**
www.madrid.org/protecciondedatos

CONSEJERÍA DE EDUCACIÓN Y JUVENTUD
Comunidad de Madrid

# ZONA VIDEOVIGILADA

**RESPONSABLE:**

Dirección General de Educación Secundaria, Formación Profesional y Enseñanzas de Régimen Especial

**PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:**

- Centro educativo
- Dirección General de Educación Secundaria, Formación Profesional y Enseñanzas de Régimen Especial - C/ O´Donnell, nº 12, 28009 Madrid (dg.secfpyre@madrid.org)
- Delegado de Protección de Datos de la Consejería de Educación y Juventud (protecciondatos.educacion@madrid.org)

**MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:**
www.madrid.org/protecciondedatos

# Grabaciones de imagen

La AEPD establece que:

1. La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.
2. No podrán instalarse en espacios protegidos por el derecho a la intimidad como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada como los gimnasios.
3. Salvo en circunstancias excepcionales, no podrán utilizarse con fines de control de asistencia escolar.
4. Se pueden instalar cámaras en los patios de recreo y comedores cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.
5. La grabación en las aulas mientras los alumnos realizan pruebas de nivel de conocimientos sería desproporcionado.

# El consentimiento para la recogida de datos personales, incluido el contenido audiovisual, en el ámbito escolar

En España, el consentimiento para tratar sus datos sólo se considerará lícito cuando tenga como mínimo 14 años (Art. 7 LOPDGDD).

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

Si es menor de 14 años, el consentimiento será lícito cuando lo otorgue el titular de la patria potestad o tutela sobre el niño.

# Buenas prácticas en el tratamiento de datos de menores en entornos escolares

- Fotos
  - ❑ Fotos con fines educativos ( sin consentimiento)
  - ❑ Fotos sin fines educativos pero complementarios (con consentimiento)

# Protección de datos de los menores en Internet (Art. 92 de la LOPDGDD)

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad **garantizarán** la protección del interés superior del menor y sus derechos fundamentales, **especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales** a través de servicios de la sociedad de la información.
Cuando dicha **publicación o difusión** fuera a tener lugar **a través de servicios de redes sociales** o servicios equivalentes deberán contar con el **consentimiento** del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

p://video.agpd.es/TuDecidesEnInternet/TuControlas/VIDEO_04_UN_CRACK_DE_LA_BMX_V3.mp4

# Protección de datos de los menores en Internet

Policía Nacional. Consejos al ciudadano. Internet. Uso seguro de Internet

https://www.policia.es/consejos/internet.html

**La Policía Nacional lanza un contrato para padres e hijos menores de 13 años con el fin de que fijen por escrito unas normas para establecer un buen uso de móviles, tablets y ordenadores**

https://www.diariosur.es/tecnologia/contrato-navidades-ciberseguras-menores-tecnologia-1224190718-ntrc.html#vca=todonoticias&vso=rrss-fb&vmc=on&vli=todonoticias&1577170676

CENTRO EDUCATIVO XXXXXXX

CONSENTIMIENTO INFORMADO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DEL ALUMNADO MATRICULADO EN CENTROS EDUCATIVOS DE TITULARIDAD PÚBLICA DE LA COMUNIDAD DE MADRID

Los centros educativos tratan datos de carácter personal del alumnado con distintas finalidades. Algunas se realizan con fines estrictamente educativos, pero para el resto de finalidades se requiere el consentimiento, bien de los representantes legales, bien de los propios alumnos y alumnas. Además, siempre se requerirá el consentimiento para la difusión de datos personales.

*Consentimiento informado para el tratamiento de datos personales en centros educativos*

# Cuándo **no** es necesario solicitar el consentimiento

En el ejercicio de la actividad educativa, los centros pueden hacer uso de aplicaciones con contenido audiovisual donde participe el alumnado sin que para ello sea necesario recabar el consentimiento.

Por ejemplo, grabar una conversación en inglés en clase para valorar la pronunciación; grabar a un alumno mientras corre para corregir la pisada; grabar un experimento para valorar la destreza en su ejecución, etc.

También es posible la publicación por parte del centro, sin que sea preciso el consentimiento, de imágenes, vídeos o voz del alumnado en Internet abierto, tales como páginas web, blogs y redes sociales, siempre que se haga de manera que no sea posible la identificación de las personas que aparecen en ellas.

Por ejemplo, se ve a la persona de espalda o de lejos; se ven sus piernas corriendo o sus manos trabajando, etc.

## Cuándo **no** es necesario solicitar el consentimiento

# Cuándo **no** es necesario solicitar el consentimiento

De esta manera el centro evita participar en la formación de la huella digital del alumnado, al que concienciará de la importancia de modelar su huella digital personal con responsabilidad.

Por esta razón el centro nunca debería solicitar el consentimiento para publicar imágenes identificables en abierto de ninguna persona.

## *No* es necesario solicitar el consentimiento

El centro utiliza preferentemente las plataformas educativas y herramientas institucionales de la Comunidad de Madrid, quien garantiza que los datos no serán cedidos a terceros no autorizados y que con su uso no se colabora en la formación de la huella digital de las personas en Internet.

## Pero *Sí* es necesario informar…

Cuando el centro considere adecuado difundir contenido audiovisual realizado en el ejercicio de la función educativa de manera restringida entre las familias, se necesita el consentimiento para dicha difusión, informándoles a la vez de que se hace para su uso en el ámbito personal, familiar y de amistad.

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. Entonces el centro educativo debe suprimir solamente en el contenido audiovisual que se difundirá las imágenes de ese niño o niña. El hecho de que un padre se oponga, no impide la difusión de las imágenes del resto de los niños o niñas.

## Cuándo **es necesario** solicitar el Consentimiento

Por otro lado, cuando la grabación se realiza dentro del centro por familiares o amistades del alumnado o por el profesorado fuera de su actividad docente, como por ejemplo, en la fiesta de Navidad o fin de curso, carnavales, jornadas culturales, etc., su destino será exclusivamente para el uso en el ámbito personal, familiar y de amistad, siendo los autores y receptores de las grabaciones los únicos responsables del uso inadecuado de las mismas, como puede ser la publicación de contenido audiovisual sin el consentimiento de personas ajenas que figuren en el mismo.

## Cuándo **es necesario** solicitar el Consentimiento

Cuando el centro haga uso de aplicaciones y herramientas ajenas a las institucionales de la Consejería de Educación y Juventud se exige la **suscripción de un contrato de encargado de tratamiento con las empresas propietarias de las mismas, que requiere recabar el consentimiento de las familias** para que estas puedan tratar sus datos personales

## Cuándo es necesario solicitar el Consentimiento

# ¿Por qué solicitaremos el consentimiento?

**PARA LAS SIGUIENTES FINALIDADES**:

A. La publicación de imágenes, vídeos o audios en las que aparezca este/a alumno/a de manera no identificable en la web del centro o en redes sociales, (Facebook, Instagram, YouTube, Twitter…)

SI ☐ NO ☐

B. La publicación de imágenes, vídeos o audios, de este/a alumno/a, con acceso restringido mediante contraseña, en el entorno de la Consejería de Educación (EducaMadrid): Mediateca, Aulas Virtuales o Blogs de aula y uso de la nube.

SI ☐ NO ☐

*… Porque* ***ejerceremos nuestra responsabilidad proactiva en*** *pro del interés superior del menor, pero también del resto de la comunidad educativa*

Puede darse el caso de padres que consideren que sus hijos pueden ser identificables aunque se haya borrado su rostro. Por ejemplo, el niño más alto del colegio, el pelo rojo, una forma de andar o cualquier otra características que pueda identificar inequívocamente a una persona.

Esto puede ser fundamental en casos de acoso o maltrato y, **si publicamos sin que estos padres lo sepan, el daño que se pueda llegar a causar ya no tendrá rectificación posible**. Por lo tanto, solicitando este consentimiento, estamos garantizando que la familia no tiene ningún problema en que se publiquen imágenes de sus hijos o hijas, aunque estas no sean identificables.

| **Información sobre protección de los datos de carácter personal recogidos para finalidades distintas de las estrictamente educativas** | |
|---|---|
| **RESPONSABLE** | Responsables en función del tipo de centro:<br><br>En las Escuelas públicas infantiles de gestión directa e indirecta, casas de niños de la Red Pública de la Comunidad de Madrid, colegios públicos de educación infantil, primaria y especial, el representante es:<br>Dirección General de Educación Infantil y Primaria, C/ Alcalá, 30-32. C. P. 28013. dgeip.educacion@madrid.org<br>Institutos de educación secundaria y centros públicos específicos de formación profesional y de enseñanzas de régimen especial:<br>Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial. C/ O´Donnell, 12. C.P.: 28009. dgsecfpyre@madrid.org |
| **DELEGADO DE PROTECCIÓN DE DATOS** | **protecciondatos.educacion@madrid.org**<br>C/ Alcalá, nº 32. Planta baja, C.P. 28014, Madrid<br>Tel: 917200379 – 917200076 – 917200304 - 917200486 |
| **FINALIDAD** | Divulgativa de las actividades del centro, con el objeto de cohesionar la comunidad educativa en beneficio del proceso educativo de los alumnos. |
| **LEGITIMACIÓN** | Los centros educativos están legitimados para recabar y tratar los datos personales de los alumnos para finalidades distintas a las estrictamente educativas solicitando su consentimiento, conforme a lo dispuesto en artículo 6.1.a) del Reglamento Europeo 2016/679 de Protección de Datos Personales.<br><br>El consentimiento se solicitará y deberá en su caso otorgarse para cada una de las finalidades citadas en los apartados descritos, que previamente habrán sido sometidas a un análisis de riesgos o evaluación de impacto que garanticen la confidencialidad de los datos. |
| **DESTINATARIOS O TRANSFERENCIAS INTERNACIONALES** | Serán destinatarios de los datos personales las redes sociales y las aplicaciones y plataformas educativas ajenas a las institucionales de la Comunidad de Madrid. **Los datos como mínimo, serán seudonimizados, preferiblemente anonimizados**, y no contendrán valoraciones explícitas sobre conductas o rendimientos.<br><br>Para el caso de plataformas o aplicaciones externas, podrían producirse transferencias internacionales cuando los servidores estén alojados fuera de la UE. |
| **DERECHOS** | Los representantes legales del alumnado menor de edad pueden ejercitar, si lo desean, los derechos de acceso y rectificación de datos, así como solicitar que se limite el tratamiento de sus datos personales u oponerse al mismo, dentro de lo dispuesto en la normativa vigente, dirigiendo una solicitud al centro docente, o bien a la Dirección General responsable del tratamiento o al Delegado de Protección de Datos de la Consejería competente en materia de Educación, por el registro (electrónico o presencial) de la Comunidad de Madrid, rellenando el formulario correspondiente y aportando la documentación que considere oportuna.<br><br>Además, en caso de disconformidad con el tratamiento de los datos personales, podrán interponer una reclamación ante la Agencia Española de Protección de Datos mediante escrito (C/ Jorge Juan, 6, 28001-Madrid) o formulario en su Sede electrónica: https://sedeagpd.gob.es/ |
| **MÁS INFORMACIÓN** | Puede consultar, adicional y detalladamente, la información y normativa aplicable en materia de protección de datos en la web de la Agencia Española de Protección de Datos https://www.aepd.es/.<br><br>Además, en la web de la Comunidad de Madrid, https://www.comunidad.madrid podrá consultar diversos aspectos sobre la protección de datos personales. |

En resumen…

| CONSENTIMIENTO | |
|---|---|
| **PARA TOMAR IMÁGENES QUE NO SE VAN A DIFUNDIR** | **PARA TOMAR IMÁGENES QUE SÍ SE VAN A DIFUNDIR** |
| **NO** | **SÍ** |
| • No necesitamos pedir el consentimiento para tomar imágenes cuando estamos **realizando nuestra función docente,** porque es una metodología más de trabajo:<br><br>Por ejemplo, grabar una conversación en inglés en clase para valorar la pronunciación; grabar a un alumno mientras corre para corregir la pisada; grabar un experimento para valorar la destreza en su ejecución, etc. | • Cuando estas mismas imágenes queremos difundirlas con un fin pedagógico, para conocimiento de la comunidad educativa, de manera restringida mediante usuario y contraseña y siempre que se haya valorado previamente la necesidad de publicarlas.<br><br>• Cuando vamos a difundir otro tipo de imágenes que no están directamente relacionadas con la función educativa. Por ejemplo, en jornadas culturales, fiestas navideñas, carnavales, visitas a museos, excursiones, etc.<br><br>• Cuando el centro haga uso de aplicaciones y herramientas ajenas a las institucionales de la Consejería de Educación y Juventud se exige la suscripción de un contrato de encargado de tratamiento con las empresas propietarias de las mismas, que requiere recabar el consentimiento de las familias para que estas puedan tratar sus datos personales, |
| **PUBLICACIÓN DE IMÁGENES** | |
| **IDENTIFICABLES** | **NO IDENTIFICABLES** |
| El centro debe valorar la conveniencia de no de intervenir en la formación de la huella digital del alumnado, que es algo que sólo a él o a sus representantes legales corresponde. Por ello nunca debería publicar en abierto imágenes identificables, ni solicitarle el consentimiento para ello, | • En redes sociales, (Facebook, Instagram, YouTube, Twitter…)<br><br>• En la página web del centro, con acceso restringido mediante contraseña<br><br>• Con acceso restringido mediante contraseña, en (EducaMadrid): Mediateca, Aulas Virtuales o Blogs de aula y uso de la nube. |

# El uso de herramientas ajenas a las corporativas de la Consejería de Educación y Juventud

Cuando los centros educativos utilicen aplicaciones ajenas deben tomar las siguientes precauciones:

- velar por que estas reúnan todas las **garantías** para cumplir con las normativa **sobre protección de datos**, debiendo informar claramente:
    - En materia de seguridad
    - Sobre la ubicación de los datos
    - Período de conservación de los datos
    - Todos los responsables del tratamiento
- **Realizar un análisis de riesgos** previo a la introducción de datos de carácter personal, diseñando un procedimiento de **anonimización de datos** y no alojar en dichas aplicaciones más que los datos **imprescindibles**.

# Qué hacen ClassDojo o G Suite con mis Datos:

## Los guardan, los ceden, los explotan…?

# ClassDojo

https://www.classdojo.com/es-es/privacy/#what-information-does-classdojo-collect

# Darse de alta en ClassDojo supone un contrato

Cada profesor, cuando se da de alta en la plataforma CD, lo hace como usuario registrado del servicio y los "Términos del Servicio" o "Acuerdo" constituyen el contrato legal entre el usuario y ClassDojo (https://www.classdojo.com/es-es/terms/?redirect=true), donde expresamente se informa de que

"Al registrarse para obtener una cuenta o acceder o utilizar el Servicio ClassDojo, usted reconoce que ha leído y acepta estar sujeto a este Acuerdo. Si está utilizando el Servicio en nombre de una institución que tiene un acuerdo por escrito con ClassDojo, ese acuerdo rige su uso del Servicio ".

Es decir, los profesores del centro que se han registrado en la plataforma tienen un contrato con el prestador del servicio.

# ClassDojo requiere el consentimiento de las familias

**ClassDojo, Inc., según declara en su política de privacidad, cumple con todos los requisitos** de las leyes americanas COPPA (Ley de protección de la privacidad en línea para niños), FERPA (Ley de Derechos y Privacidad de Educación Educativa Familiar), con el RGPD europeo y se encuentra certificada bajo el Escudo de Seguridad UE-EEUU. Además, debido a los requisitos de COPPA y similares a otras herramientas educativas basadas en la nube, ClassDojo **requiere que las escuelas obtengan el consentimiento de los padres si crean cuentas de estudiantes en su nombre.**

# ¿ClassDojo compartirá la información que recopila?

… no compartimos información personal con terceros, excepto en las circunstancias limitadas descritas en esta Política de privacidad y como se establece a continuación:

**Otros usuarios con los que comparte y se comunica en ClassDojo**:

Tenga en cuenta que la información (incluida la información personal o la información personal de los niños) o el contenido que usted divulga voluntariamente a otros, incluso a otros usuarios de ClassDojo con los que interactúa a través del Servicio (como mensajes que puede enviar a otros usuarios u otros maestros y líderes escolares) colaboras con): las personas con las que lo compartes pueden verlo, copiarlo, almacenarlo y utilizarlo. **No podemos controlar las acciones de las personas con quienes usted elige compartir información y no somos responsables de la recopilación, uso o divulgación de dicha información o contenido por parte de terceros.**

**Integraciones de terceros en nuestro Servicio:**

cuando, como maestro, líder escolar, estudiante o padre, utiliza aplicaciones, sitios web u otros servicios de terceros que utilizan o están integrados con nuestro Servicio, pueden recibir información sobre qué publicas o compartes Por ejemplo, **cuando comparte una actividad de Big Ideas en Twitter o Facebook, estos servicios reciben la información que comparte a través de esta funcionalidad y la información que está compartiendo desde ClassDojo. También podemos tener integraciones de terceros en el sitio web de ClassDojo (áreas que no han iniciado sesión para usuarios). …**

# Tipos de información compartida

**Tipos de cuenta que comparten esta información**
Maestro, padre, líder escolar y estudiante (a través del maestro)
**Cómo ClassDojo recopila estos datos**
Directamente por el usuario en nuestro sitio web o aplicación móvil, o **si es el alumno por el maestro**; a través del Directorio Escolar por maestros y líderes escolares; también, cuando los usuarios completan encuestas o nos contactan a través del Servicio al Cliente / correo electrónico
**El propósito de que ClassDojo recopile esta información**
Establecer la identidad de uno dentro de una comunidad escolar, o para necesidades de apoyo / responder a encuestas; para invitar a más maestros a través del Directorio escolar
**Cómo se usa esta información**
Para enviar un mensaje SMS para invitar a un usuario (potencialmente) no conectado a ClassDojo; si es por apoyo o una encuesta, para permitir que un miembro del equipo de ClassDojo se contacte con el individuo
**Dónde se almacenan estos datos (y qué proveedores de servicios externos los tienen, si los hay)** Datos almacenados en servidores de AWS **en los EE. UU.**
**¿Se comparten estos datos con otros proveedores de servicios externos y, de ser así, con quién y por qué motivo?** Sendgrid **en los EE. UU.**, Para ayudarnos a enviar correos electrónicos más amigables
**¿Se transfiere esta información fuera del Espacio Económico Europeo (EEE)?** **Sí, a los EE. UU.**
**¿Cuál es la base legal para procesar esta información bajo el RGPD?**
**Intereses legítimos** y cumplimiento del contrato

# G Suite for Education

https://edu.google.com/intl/es-419_ALL/why-google/privacy-security/?modal_active=none

https://www.duna.cl/noticias/2020/02/25/fiscal-de-estados-unidos-denuncia-supuesto-espionaje-de-google/

- ✓ Política de privacidad de Google
  https://policies.google.com/privacy?hl=es#infocollect

- ✓ Política de privacidad de Google for education (ver FAQ)
  https://edu.google.com/intl/es-419_ALL/why-google/privacy-security/?modal_active=none

- ✓ Aviso de privacidad de G Suite for Education
  https://gsuite.google.com/terms/education_terms.html?_ga=2.159315327.457408965.1571648204-624759599.1536302783

- ✓ Acuerdo de G Suite for Education
  https://gsuite.google.com/intl/en/terms/education_privacy.html

- ✓ Adenda o enmienda de procesamiento de datos a G suite y/o acuerdo de producto complementario
  https://gsuite.google.com/intl/es/terms/dpa_terms.html

# lo que compartimos con Google…

## Aviso de Privacidad de G Suite for Education

### Información que recogemos

Las cuentas de G Suite para Centros Educativos son cuentas de Google creadas y gestionadas por un centro educativo para que las utilicen los alumnos y los profesores. Al crear estas cuentas, **el centro educativo podría facilitar a Google información personal de los alumnos y los profesores**, generalmente nombres de usuario, direcciones de correo electrónico y contraseñas, pero también puede puede incluir direcciones de correo electrónico secundarias, teléfonos y direcciones. Google **también** puede recoger **información personal** directamente de los usuarios de las cuentas de G Suite para Centros Educativos, como **su número de teléfono, su foto de perfil u otros datos que añadan a la cuenta de G Suite para Centros Educativos**.

# lo que compartimos con Google…

## Cómo utilizamos la información que recogemos

### En los servicios principales de G Suite para Centros Educativos

Los servicios principales de G Suite para Centros Educativos ("Servicios Principales") se enumeran en el Resumen de Servicios e incluyen Gmail, Calendar, Classroom, Contactos, Drive, Documentos, Formularios, Grupos, Hojas de cálculo, Google Sites, Presentaciones, Talk/Hangouts, Vault y Sincronización de Chrome. Estos servicios se ofrecen a los centros educativos de acuerdo con el Acuerdo de G Suite para Centros Educativos y, si procede, la Adenda sobre Tratamiento de Datos. Los usuarios y los padres pueden preguntar al centro educativo si ha aceptado la Adenda sobre Tratamiento de Datos.

La información personal del usuario que se recoge en los Servicios Principales se utiliza únicamente para ofrecer dichos servicios…

# lo que compartimos con Google…

## En los servicios de Google en general

Además de los Servicios Principales, **los usuarios de G Suite para Centros Educativos pueden acceder a otros servicios de Google que ponemos a disposición del público en general, como Google Maps, Blogger y YouTube**. Los llamamos "Servicios Adicionales" porque no forman parte de los Servicios Principales.
La Política de Privacidad de Google describe de forma exhaustiva cómo los servicios de Google utilizan generalmente la información, incluida la de los usuarios de G Suite para Centros Educativos. En resumen, utilizamos la información que recogemos de todos nuestros servicios para proporcionarlos, mantenerlos, protegerlos y mejorarlos, para desarrollar otros nuevos y para proteger a Google y a nuestros usuarios. También utilizamos esta información para ofrecer a los usuarios contenido personalizado, como resultados de búsqueda más relevantes. **Google puede combinar información personal de un servicio con información de otros servicios de Google, incluida información personal**.

# lo que Google comparte …

Para procesamiento externo

**Proporcionamos información personal a nuestros afiliados y otras empresas o personas de confianza para que la procesen por nosotros**, de acuerdo con nuestras instrucciones y de conformidad con nuestra Política de privacidad y cualquier otra medida de confidencialidad y seguridad adecuada. Por ejemplo, utilizamos proveedores de servicios para ayudarnos con la atención al cliente.

Por razones legales

**Compartiremos información personal fuera de Google si creemos de buena fe que el acceso, uso, preservación o divulgación de la información es razonablemente necesario** para:

- Cumplir con cualquier ley aplicable, regulación, proceso legal o solicitud gubernamental exigible. Compartimos información sobre el número y tipo de solicitudes que recibimos de los gobiernos en nuestro Informe de Transparencia .
- Hacer cumplir los Términos de servicio aplicables, incluida la investigación de posibles infracciones.
- Detectar, prevenir o abordar de otra manera el fraude, la seguridad o los problemas técnicos.
- Proteger contra daños a los derechos, la propiedad o la seguridad de Google, nuestros usuarios o el público según lo exija o permita la ley.

# Cloud Act

El Acta de Aclaración del Uso de Datos en el Extranjero Lícito o el Acta de Nube ( HR 4943 ) es una ley federal de los Estados Unidos promulgada en 2018 por la aprobación de la Ley de Apropiaciones Consolidadas, 2018, PL 115-141, sección 105, acuerdos ejecutivos sobre acceso a datos por gobiernos extranjeros. Principalmente, la Ley CLOUD modifica la Ley de comunicaciones almacenadas (SCA) de 1986 para permitir que la policía federal obligue a las empresas de tecnología con sede en los EE. UU. a través de una orden o citación para proporcionar los datos solicitados almacenados en los servidores, independientemente de si los datos están almacenados en suelo de los EE. UU.

# Recomendamos especialmente a los profesores TIC la lectura de las siguientes guías, informes y notas técnicas de la AEPD:

https://www.aepd.es/areas/innovacion/index.html

- Ingeniería de la Privacidad

  https://www.aepd.es/blog/2019-09-11-ingenieria-privacidad.html

- Orientaciones y garantías en los procedimientos de ANONIMIZACIÓN de datos personales

  https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

- Guía de Privacidad desde el Diseño

  https://www.aepd.es/media/guias/guia-privacidad-desde-diseno.pdf

- LA K-ANONIMIDAD COMO MEDIDA DE LA PRIVACIDAD

  https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf

# 5. El uso del correo electrónico, la mensajería instantánea y el Registro electrónico de la Administración.

El **correo electrónico**, no es un medio adecuado para notificar una información porque no permite dejar constancia de su recepción y tampoco permite garantizar la seguridad de los datos confidenciales una vez recibida por el receptor.

Debido a que se pierde el control de la seguridad de la información que se comunica:

- No debe utilizarse el **correo electrónico** personal para fines profesionales.
- El correo corporativo o profesional no debe redireccionarse al correo personal o viceversa, especialmente si contiene datos de carácter personal.

Se pueden producir revelaciones indebidas de información a terceros.

La cuenta corporativa (xxx@educa.madrid.org) para uso laboral es propiedad de la empresa o institución en la cual se presta servicios, que es quien determina tanto el usuario como el proveedor y el dominio, y también las finalidades y condiciones de uso a que está sometido. La atribución de esta cuenta de correo se hace por motivos estrictamente laborales.

La mensajería instantánea ajena a la Comunidad de Madrid, como la aplicación Whatsapp, se considera como red social y como tal, debe evitarse su uso para comunicar datos de carácter personal en el ámbito laboral por la pérdida de control de la confidencialidad que ello supone. Cuando un centro educativo deba comunicar información de carácter personal a las familias deberá hacerlo a través de la plataforma ROBLE o ponerla a su disposición en un ámbito restringido de su página web o en la nube de EducaMadrid (Cloud)

Cuando debamos comunicar información desde el centro a la DAT o a otros órganos de la Consejería, así como a otras Administraciones Públicas o a la Policía, es recomendable no hacer uso del correo electrónico y mucho menos de la mensajería instantánea.

El cauce adecuado entre Administraciones Públicas es el Registro electrónico.

# 6. El intercambio seguro de información.

## Cómo debemos comunicar datos personales

El canal adecuado para comunicar o transferir información entre Administraciones Públicas o entre órganos de una misma Administración es su **Registro Electrónico**, porque lo dice la ley 39/2015, de Procedimiento Administrativo Común y porque el intercambio es seguro al realizarse directamente a través de sus propias plataformas de Registro .

Si por alguna razón justificada no es posible utilizar el Registro Electrónico para comunicar datos personales, ya sean de categoría especial o no, debemos elegir la forma más segura de la que dispongamos.

Una forma de evitar la pérdida, extravío o sustracción de dispositivos de memoria externa, es utilizar el sistema de almacenaje en la nube de EducaMadrid: Cloud.

Cuando sea inevitable utilizar el correo electrónico para comunicar datos de carácter personal, estos deberán estar incorporados en un fichero adjunto y la forma más segura para garantizar la autenticidad e integridad de las comunicaciones es que vaya cifrado. También podemos utilizar la firma electrónica al remitir el correo.

La última opción que debemos elegir para trabajar con datos de carácter personal relacionados con nuestra actividad laboral, es transportarlos en dispositivos de memoria externa u ordenadores portátiles.

Si lo hacemos, deberíamos cifrar el dispositivo de manera integral.

# 7. EducaMadrid, un entorno fiable, confidencial y disponible para los docentes.

El entorno de EducaMadrid dispone de todas las medidas de seguridad necesarias y son establecidas por la Consejería de Educación.

Sin embargo, la privacidad de los datos no depende únicamente de garantizar la seguridad de los mismos, sino que es necesario analizar los riesgos que supone, sobre todo para los menores, que los contenidos con datos personales no se alojen en las aplicaciones con acceso abierto.

# Cómo gestionar la privacidad de manera apropiada

## Cómo gestionar la privacidad de manera apropiada

- Pensar antes de publicar, enviar o aceptar. Estamos creando una identidad digital que nos acompañará toda la vida
- Minimizar la difusión de datos personales. No sobreexponer información personal.
- Concienciarnos de que se pierde el control de lo que se sube a Internet o se comunica a otras personas que no son de nuestra completa confianza.

- Gestionar las opciones de privacidad en aplicaciones y servicios web (navegadores, redes sociales, dispositivos móviles), revisando la información que compartimos de forma pública o privada, comprobando los tipos de búsqueda y actividad de navegación y contenidos vistos a través de los buscadores.
- Cuidar las contraseñas: no compartirlas, que sean robustas, no reutilizarlas…
- Establecer sistemas de bloqueo de pantalla.
- Tapar la webcam cuando no se utilice.

## Cómo gestionar la privacidad de manera apropiada

# Cómo gestionar la privacidad de manera apropiada

- Cerrar la sesión al salir
- Acostumbrarnos a leer los términos de uso y las políticas de privacidad de las aplicaciones y aprender a hacer uso de nuestros derechos (acceso, rectificación, oposición, limitación…)
- Concienciarnos de que siempre que deseemos compartir información de otras personas debemos pedirles permiso y demandar esta conducta responsable a los demás (amigos, familiares, conocidos)
- La información que se incluye en las plataformas educativas debe compartirse entre los docentes e interesados en privado.

# GRACIAS