DECÁLOGO DE PROTECCIÓN DE DATOS EN EL ÁMBITO EDUCATIVO

IES Laguna de Joatzel

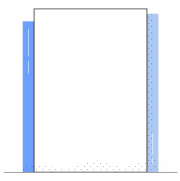
1 El personal de la Consejería de Educación, Universidades, Ciencia y Portavocía, en el ejercicio de sus funciones, necesita tratar datos de carácter personal de los alumnos y sus tutores legales, cuando aquellos son menores, así como de los propios empleados.
Las Direcciones Generales de la Consejería de Educación, Universidades, Ciencia y Portavocía son las responsables del tratamiento de los datos y deben mantener actualizada la información dirigida a los interesados sobre los principios básicos para la protección de los datos y su correcta gestión.
Solamente los responsables puede determinar los fines y los medios del tratamiento. No podemos tomar la iniciativa de tratar datos por nuestra cuenta, ya que no nos pertenecen.

2 Los datos tratados siempre son de titularidad de la persona a la que identifican y son confidenciales, por lo que nunca deben facilitarse a otras personas que no estén autorizadas para tratarlos o que no sean sus representantes legales.
La confidencialidad en el ejercicio de la actividad profesional debe guardarse incluso cuando haya finalizado la relación profesional o de servicio con la Comunidad de Madrid.
No debemos guardar datos localmente en nuestros equipos y menos aún en dispositivos personales y nunca debemos comunicarlos, aunque se trate de compañeros de trabajo, si no tienen autorización para consultarlos o tratarlos.

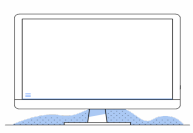
3 Se debe recoger la información personal mínima necesaria, evitando conservar documentos que contienen más datos de los que se necesitan y únicamente deben tratarse para la finalidad o finalidades para los que se recogieron.
No guardemos información personal que no necesitemos en un momento determinado en previsión de que podamos necesitarla en el futuro. Conservarla sin motivo cambia la finalidad con la que nos la confiaron.

4 Deben utilizarse los medios y herramientas corporativas que la Comunidad de Madrid pone a disposición de los profesionales de educación (plataforma *EducaMadrid*, correo electrónico, nube institucional, Raíces…), evitando usarlas para actividades privadas. También se debe evitar la utilización de dispositivos o aplicaciones de uso privado para almacenar datos en la actividad profesional. Hay que tener en cuenta que la Comunidad de Madrid pone a disposición de sus trabajadores las herramientas que le permiten tener el control de la información. Si utilizamos herramientas distintas de las corporativas, estamos cediendo información sin autorización del titular de los datos ni del responsable del tratamiento, es decir, nuestra organización.

5 Con el objetivo de reducir el riesgo para la seguridad de los datos, se debe compartir la información confidencial con quienes están autorizados para acceder a ella mediante un acceso privado a una carpeta de nuestra nube corporativa. Esta es una buena práctica en materia de protección de datos.
En caso de requerirse una comunicación legítima de datos personales a terceros deberán emplearse mecanismos de cifrado.
Siempre hay que evitar redirigir los mensajes de correo a cuentas privadas.

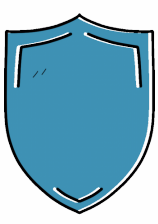


6 No debemos dejar a la vista documentación con datos personales ni transportar dichos datos en soportes digitales fuera de nuestro centro de trabajo. En caso necesario, el contenido deberá estar cifrado.
Hay que asegurarse de que no se puede recuperar la información personal cuando se destruyan documentos o soportes digitales.



7 Se debe evitar imprimir documentos de manera innecesaria. Si hay que imprimirlos, es imprescindible destruirlos inmediatamente cuando dejen de ser necesarios, siguiendo escrupulosamente el protocolo de destrucción segura de documentación.
Además de contribuir a proteger el medio ambiente, acceder a la información en las plataformas corporativas nos permite mantenerla segura.

8 Las contraseñas que utilicemos deben ser robustas, con mayúsculas y minúsculas, dígitos y algún signo de puntuación o carácter especial. Tienen que estar bien custodiadas, evitando que otras personas las conozcan.
Es recomendable utilizar un programa de gestión de contraseñas y generar claves aleatorias seguras.



9 Debemos conocer la política de seguridad de la información de la Comunidad de Madrid y seguir sus normas de uso y de buenas prácticas para cumplir con el Esquema Nacional de Seguridad.
La formación en este ámbito es esencial.

10 Se debe poner en conocimiento del responsable del tratamiento de la información y de la Delegación de Protección de Datos cualquier incidencia relativa a accesos no autorizados a datos personales o a su destrucción, pérdida o alteración ilícita.

Si tienes dudas puedes...

Visitar la página web de la Delegación de protección de datos (https://dpd.educa2.madrid.org/)

Contactar con la Delegación de Protección de Datos por correo electrónico (proteccióndatos.educacion@madrid.org)

Santiago Rodríguez López
Responsable *#CompDigEdu*

Documento elaborado adaptando la información del decálogo de protección de datos para el ámbito educativo publicado por la Delegación de Protección de Datos de la Consejería de Educación, Universidades, Ciencia y Portavocía.