

DECÁLOGO DE PROTECCIÓN DE DATOS PARA EL ÁMBITO EDUCATIVO

1 El personal de la Consejería, 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 y Juventud son las responsables de los tratamientos de los datos y deben mantener actualizada la información dirigida a los interesados sobre los principios básicos en la Protección de Datos y cómo tratarlos correctamente



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

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



4

Deben utilizarse los medios y herramientas corporativos de la Comunidad de Madrid puestos a disposición para la actividad profesional (plataforma EducaMadrid, correo electrónico, carpetas de red o nube institucional) evitando hacer uso de ellas para actividades privadas, ni utilizar dispositivos o aplicaciones de uso privado para almacenar datos en la actividad profesional

5



Es una buena práctica compartir la información confidencial con quienes están autorizados para ello mediante un acceso privado a una carpeta de nuestra nube corporativa. En caso de requerirse una comunicación legítima de datos personales a terceros deberán emplearse mecanismos de cifrado



6

Debemos seguir una política de mesas limpias, evitando dejar a la vista documentación con datos personales, así como transportarlos en soportes digitales fuera del lugar de trabajo. En caso necesario, el contenido deberá estar cifrado. Debe asegurarse que no se puede recuperar la información personal cuando se destruyan documentos o soportes digitales

7



Evitemos imprimir documentos de manera innecesaria y destruyámoslos inmediatamente cuando dejen de ser necesarios, siguiendo escrupulosamente el protocolo de destrucción segura de documentación



8

Utilicemos contraseñas robustas utilizando mayúsculas y minúsculas, dígitos y algún signo de puntuación. 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.



10

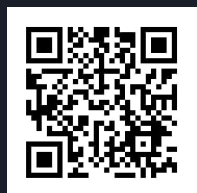
Se debe poner en conocimiento del responsable del tratamiento y de la Delegación de Protección de Datos cualquier incidencia relativa a accesos no autorizados a datos personales, o a su destrucción, pérdida o alteración ilícita

2020



Delegación de protección de datos ****

CONSEJERÍA DE EDUCACIÓN Y JUVENTUD



<https://dpd.educa2.madrid.org>