Decálogo

PARA UN CORRECTO USO DE LOS DATOS DE CARÁCTER PERSONAL Y LOS DISPOSITIVOS ELECTRÓNICOS EN LOS CENTROS EDUCATIVOS

1. **En el ejercicio de nuestras funciones y tareas necesitamos tratar datos de carácter personal del alumnado y de sus familiares, lo que debe realizarse con la debida diligencia y respeto a su privacidad e intimidad. Son datos personales: El nombre y apellidos del alumnado, de sus familiares, su dirección o lugar de trabajo, teléfono o correo electrónico, datos bancarios o profesión. También lo es su imagen.**
   - Debemos evitar: Exponer en lugares públicos listados que contengan datos como el DNI, teléfono, domicilio o correo electrónico o el envío masivo de mensajes en los que las direcciones de cada destinatario aparezcan a vista pública.
   - Es preferible: Realizar comunicaciones individualizadas, vía iPasen o correo electrónico, a exponer listas públicas, siempre que sea posible. De transmitir un mensaje masivo por correo electrónico, anonimizar a cada destinatario, usando la opción CCO del cliente de correo.

2. **Cuando sea preciso obtener el consentimiento del alumnado o de sus tutores para la utilización de sus datos personales, por tratarse de finalidades distintas a la función educativa, se debe informar con claridad de cada una de ellas, permitiendo a los interesados oponerse a aquellas que así lo consideren.**
   - Debemos evitar: Los consentimientos de palabra de viva voz o por teléfono y el uso de modelos de recogida de consentimiento elaborados por nosotros mismos o extraídos de Internet.
   - Es preferible: Recoger por escrito los consentimientos, usando el modelo aprobado para ello por el centro, y haciéndoselo llegar a la familia con una antelación no inferior a 5 días.

AUTORIZACIÓN PARA EL USO DE DATOS PERSONALES

Por medio del presente, Yo, Don _____, con DNI/NIF núm. _____, de estado civil soltero, con domicilio en _____.

AUTORIZA a:

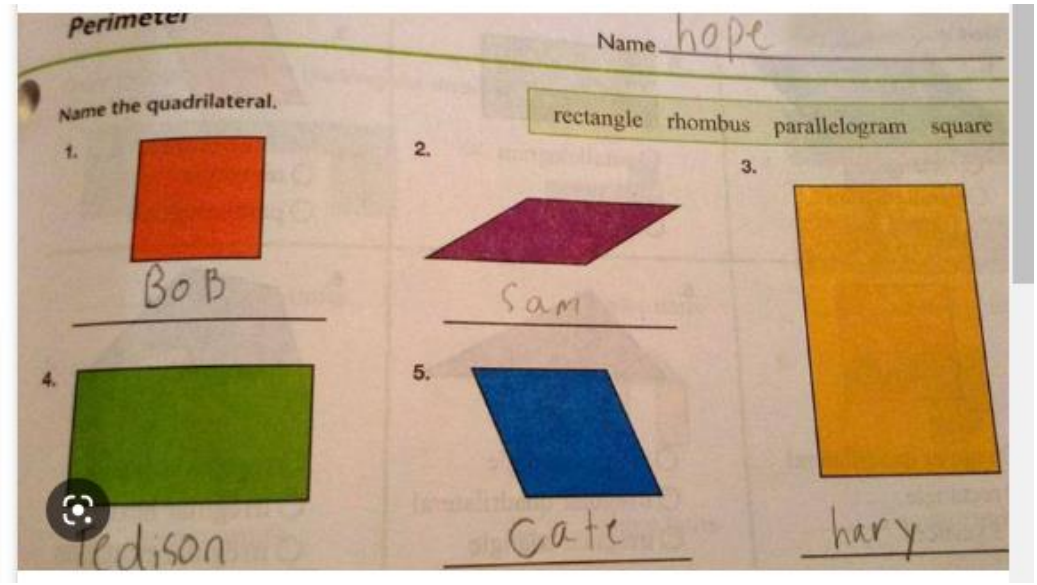
I. _____, con NIF _____, y con domicilio a efecto de notificaciones en _____, quien actúa como Responsable del Tratamiento de datos personales, para que en los términos legalmente establecidos

3. **Las comunicaciones entre el profesorado o entre este y el alumnado o sus tutores legales deben llevarse a cabo, preferentemente, a través de los medios puestos a disposición de ambos por el centro educativo (plataformas educativas, correo electrónico del centro).**
   - Debemos evitar: El uso de cuentas personales de correo o aplicaciones de mensajería instantánea (como WhatsApp) para la comunicación con las familias o entre el profesorado, para cualquier tema vinculado con la labor docente. Solo en aquellos casos de accidente o indisposición y con la finalidad de informar y tranquilizar a los tutores legales, se podrá usar para enviarles imágenes, con el fin de que conozca su estado real.
   - Es preferible: El uso del correo corporativo y el sistema de mensajería Séneca/iPasen.

4. **Las TIC son herramientas fundamentales para la gestión y el aprendizaje de los alumnos. El profesorado debe conocer las aplicaciones que vaya a utilizar, su política de privacidad y sus condiciones de uso de éstas antes de utilizarlas, debiendo rechazarse las que no ofrezcan información sobre el tratamiento de los datos personales que realicen.**
    - Debemos evitar: Toda herramienta o aplicación que no garantice la privacidad de sus comunicaciones, incluidas aquellas para realizar reuniones virtuales como Zoom o videollamadas desde cuentas privadas.
    - Es preferible: El uso de herramientas aprobadas para este fin por la administración educativa, mediante cuentas de correo corporativo, las cuales dan acceso a aplicaciones como Google Meet, Google Classroom, Microsoft Teams o Moodle corporativa.

5. **El profesorado debe tener cuidado con los contenidos que suben a Internet. Deben valorar la privacidad de uno mismo y la de los demás.**
    - Debemos evitar: Publicar ejercicios o trabajos que contengan nombres de los autores, a menos que contemos con su consentimiento expreso. Publicar estos como ejemplos de cómo no debe hacerse una determinada tarea o añadiendo comentarios que puedan resultar ofensivos o dañinos para la autoestima del autor.
    - Es preferible: Solicitar el consentimiento explícito, y por escrito, de los autores antes de publicar sus trabajos, aunque estos posteriormente sean anonimizados. Publicar una variedad de trabajos

de cada actividad, no solo los mejores, acompañados de comentarios positivos y de ánimo, por el trabajo realizado.



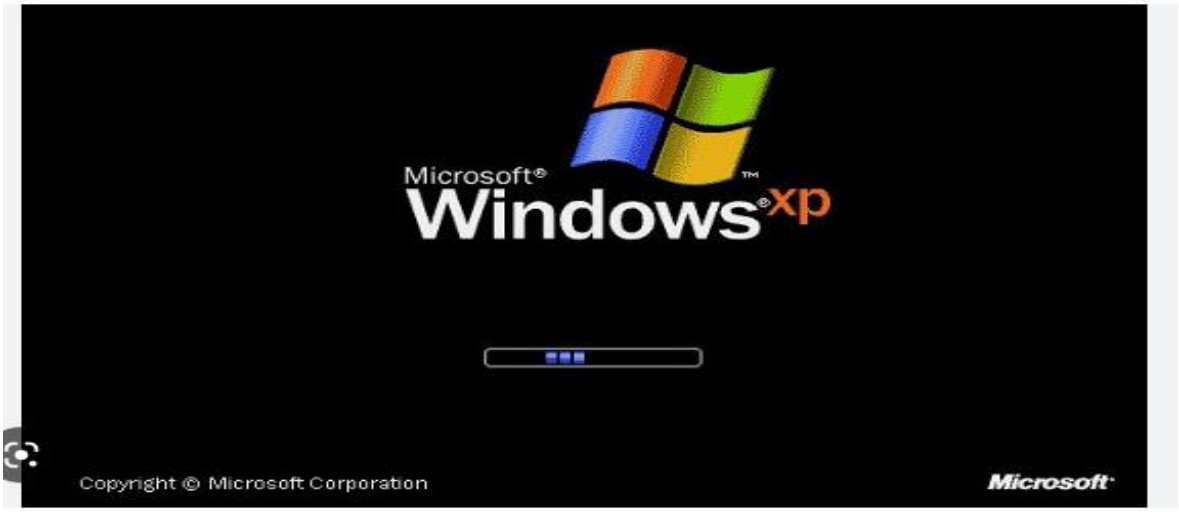
6. **Es imprescindible enseñar al alumnado que no pueden sacar fotos ni videos de otros alumnos, ni de personal del centro y hacerlos circular por las redes sociales, para evitar cualquier forma de violencia (ciberacoso, grooming, sexting o de violencia de género).**
   - Debemos evitar: El uso del móvil en todo el centro, incluidas las horas de guardia o el recreo.
   - Es preferible: De ser necesario para alguna actividad docente, comunicárselo por escrito a las familias con la debida antelación y dejar claro al alumnado que no podrá continuar usándolo fuera de dicha actividad. Únicamente en las actividades extraescolares se permitirá su uso, pero estableciendo claramente con el alumnado las limitaciones a respetar, antes de dicha actividad.

7. **Cuando los centros educativos organicen y celebren eventos (fiestas de Navidad, fin de curso, eventos deportivos) a los que asistan los familiares del alumnado.**
    - Debemos evitar: La grabación indiscriminada de asistentes e instalaciones del centro, sin relación alguna con su hijo/a o la actividad que se está desarrollando.
    - Es preferible: Informarles previamente de la posibilidad de grabar imágenes exclusivamente para su uso personal y doméstico, en las que aparezcan siempre ellos o sus hijos o hijas. Además, conocedores de que el centro proporcionará imágenes del evento, a través de la página web y redes sociales del mismo.

8. **Durante el uso de dispositivos electrónicos en el aula (móviles, tabletas, ordenadores), a pesar de que existen programas de control parental, es responsabilidad del profesorado evitar que el alumnado acceda a contenidos de riesgo (bulimia, anorexia, violencia, pornografía, pedofilia, consumo de drogas, juegos, fraudes comerciales, vídeos de moda con conductas de riesgo, etc.). Ha de tenerse en cuenta siempre la orientación por edades y temáticas de los videojuegos y programas de entretenimiento (código *PEGI*).**
    - Debemos evitar: El uso sin supervisión de dichos dispositivos, confiando únicamente en que los filtros instalados en la red corporativa bloquearán cualquier contenido inapropiado. La elección de un único recurso (programa, web, vídeo, etc.) para todo nuestro alumnado, sin tener en cuenta su edad y grado de madurez.

- Es preferible: La instalación de software de acceso remoto que nos permita supervisar la actividad de cada alumno o, en su defecto, la supervisión personal frecuente, así como limitar el acceso del alumnado a un número de contenidos concretos y pertinentes para la actividad a realizar, y adaptados a su edad y madurez.

9. **Proteja todos los dispositivos con conexión a la Red con antivirus, bloqueos de pantalla, contraseñas y códigos fuertes. Actualice los sistemas operativos y sus programas.**
   - Debemos evitar: El uso de programas desactualizados o directamente obsoletos, que puede dar lugar a ser objeto de ataques cibernéticos, virus o vulneración de nuestra privacidad.
   - Es preferible: De no poder costear la actualización de un recurso, buscar una alternativa Open-Source actualizada y segura, aunque ello suponga, en ocasiones, sacrificar algunas prestaciones o servicios.



10. El menor no debe contactar ni seguir en redes sociales a quien no conoce en la vida real. Y menos acudir a una cita. El *grooming* se produce cuando un adulto se hace pasar por menor, para chantajearle y abusar sexualmente de él.

- Debemos evitar: No usar herramientas tipo chat con el alumnado, a menos de que estén asociadas a cuentas corporativas o intranet cerradas.
- Es preferible: Recordar a los menores el peligro que supone entablar conversaciones con desconocidos y proporcionarles información personal que pudieran usar en nuestra contra. Enseñarles explícitamente a reconocer señales de alerta ante peticiones inapropiadas o extrañas de desconocidos y a comunicárselo automáticamente a su profesorado o familiares.