PROTECCIÓN DE DATOS

Protocolo de Actuación

Presentado al ETCP el 19/04/2023, aprobado en el claustro de profesores con fecha de ---------, oído en el Consejo Escolar con fecha de---------.

IES MAR DE ALBORÁN

ÍNDICE

PROTOCOLO DE PROTECCIÓN DE DATOS
IES MAR DE ALBORÁN

PREÁMBULO

La protección de los datos personales se ha convertido en un derecho fundamental en la sociedad actual. Hemos de tener en cuenta la cantidad de datos que se manejan en todos los organismos, empresas, en internet, redes sociales, etc. Por este motivo y como medida de protección al honor y la intimidad personal y familiar de las personas, se hizo necesario legislar a este respecto. Nuestro centro educativo, como tratante de datos, debe por lo tanto cumplir con la legislación vigente en esta materia. Se crea así este protocolo de Tratamiento de Datos del IES Mar de Alborán, para dejar constancia de la recogida de datos, la finalidad y el uso, informando de todo ello a toda la comunidad educativa de nuestro centro.

1. MARCO LEGAL: PRINCIPIOS DE PROTECCIÓN DE DATOS

La legislación que regula la protección de datos es **el Reglamento General de Protección de Datos (RGPD)** que es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y que comenzó a aplicarse el 25 de mayo de 2018 y la **Ley Orgánica 3/2018, de 5 de diciembre**, de **Protección de Datos Personales y garantía de los derechos digitales** que adapta el ordenamiento jurídico español al Reglamento General de Protección de Datos.

El **Real Decreto-ley 14/2019, de 31 de octubre**, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones regula varios aspectos meramente puntuales respecto del tratamiento de datos personales por parte de las Administraciones Públicas y sus contratistas al amparo de la habilitación contenida en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018.

En ambos documentos se hace referencia a una serie de **principios de protección de datos**, que son los siguientes:

1. *Exactitud de los Datos*: debiendo ser actualizados y/o modificados en caso de que nos fuesen correctos por la persona a la que pertenecen los datos.
2. *Deber de confidencialidad*: los datos y el tratamiento de los datos, es confidencial por parte de todo el personal del centro, no pudiéndose hacer un uso de los mismos fuera del ámbito educativo y con la finalidad para la que se deben emplear.
3. *Tratamiento basado en el consentimiento del afectado*: en el caso de los centros educativos hay una recogida de datos necesaria legalmente. En otra serie de elementos, como el uso de imagen o realización de actividades fuera del centro, es necesario recabar el consentimiento expreso de los interesados.

4. *Consentimiento de los menores de edad*: en este caso el consentimiento expreso del menor se debe recabar cuando superen la edad de catorce años. En menores de catorce años el consentimiento expreso depende de sus responsables legales.
5. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos*. En los centros públicos tratamos una serie de datos con una finalidad educativa, administrativa y/o de orientación. El tratamiento de estos datos es confidencial y siempre en cumplimiento de la misión para la que fueron recabados.
6. *Categorías especiales de datos*: existen una serie de datos sensibles como son aquellos que tienen que ver con la ideología, religión, orientación sexual o estado de salud que no pueden ser usados o recabados con la finalidad de discriminar o identificar a las personas por estos motivos. En nuestro centro educativo no se recaba ningún dato sensible, a no ser que sea entregado por consentimiento expreso por los afectados.
7. *Trasparencia e información al afectado*: el responsable del tratamiento de los datos tiene el deber de informar y facilitar la información que haya sido obtenida directamente del afectado, así como tiene el deber de informar del tratamiento que se hacen de los datos.

2. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

La Consejería de Educación dispone de un registro de actividades de tratamiento, en cumplimiento de lo establecido en el artículo 30 del Reglamento General de Protección de Datos, que abarca de forma global las competencias de la Consejería en las que se tratan datos de carácter personal de la comunidad educativa, personal no docente y ciudadanía en general.

Debemos identificar los tratamientos que realizamos en nuestro trabajo así como su finalidad, nivel de seguridad, responsable y las medidas de seguridad que deben aplicarse en función de su nivel. Cabe destacar entre los tratamientos, tres de especial relevancia para los centros y servicios educativos:

- **Videovigilancia,** cuya finalidad es la vigilancia y seguridad en el interior de las sedes administrativas, centros y servicios educativos dependientes de la Consejería de Educación.
- **Control del horario y seguimiento del personal,** cuya finalidad es el control de presencia en el interior de las sedes administrativas, centros y servicios educativos dependientes de la Consejería de Educación para la gestión del cumplimiento de la jornada y horarios. En el IES Mar de Alborán se utilizarán la geolocalización habilitada y asegurada por la plataforma de Séneca y el sistema de control de presencia mediante QR a través del control de presencia de Séneca.
- **Contenido audiovisual de las actividades** de los centros y servicios educativos, con la finalidad de realizar promoción y difusión en los sitios web de los centros y servicios educativos de las actividades culturales, recreativas, deportivas y sociales en las que participa el propio centro.

Los centros y servicios educativos que traten datos contenidos en alguno de estos tres supuestos deberán además rellenar los cuestionarios pertinentes para que exista constancia de ese tratamiento.

2.1. Videovigilancia

La Consejería de Educación dispone de un registro de actividades de tratamiento, en el cual se incluye como uno de los tratamientos la 'Videovigilancia', cuya finalidad es la vigilancia y seguridad en el interior de las sedes administrativas, centros y servicios

educativos dependientes de la Consejería de Educación. Los centros educativos que deseen instalar sistemas de videovigilancia deberán:

- Rellenar y mantener actualizado en Séneca el cuestionario que a tal efecto está disponible (apartado 'Centro' / 'Cuestionarios' / 'Seguridad y protección de datos' / 'Sistemas de videovigilancia').
- Informar a las personas cuyas imágenes se capten. Para ello se utilizará un distintivo como el que se encuentra en 'Documentos' / 'Centro' / 'Cuestionarios' / 'Distintivo de videovigilancia'. El distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos se debe colocar en todos ellos al objeto de que la información sea visible con independencia de por dónde se acceda. Adicionalmente, se dispondrá de copias, o la posibilidad de imprimirlas, del impreso informativo ubicado en ('Documentos' / 'Centro' / 'Cuestionarios' / 'Impreso informativo de videovigilancia') y también disponible aquí. Videovigilancia
- La Consejería de Educación dispone de un registro de actividades de tratamiento, en el cual se incluye como uno de los tratamientos la 'Videovigilancia', cuya finalidad es la vigilancia y seguridad en el interior de las sedes administrativas, centros y servicios educativos dependientes de la Consejería de Educación. Los centros educativos que deseen instalar sistemas de videovigilancia deberán
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado. De forma general, estas medidas incluirán el control de acceso de modo que sólo el personal autorizado pueda acceder a las imágenes. Para más información, debe consultarse la Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AGPD ('Documentos' / 'Centro' / 'Cuestionarios' / 'Guía de Videovigilancia').
- Garantizar la cancelación de las imágenes captadas. El plazo de cancelación de las imágenes será de un mes desde su captación. Transcurrido dicho plazo las imágenes deberán ser canceladas, lo que implica el bloqueo de las mismas
- Por otra parte, sí serían aplicables los siguientes derechos:
  a. El derecho de acceso, si bien éste reviste características singulares, ya que requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros. Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.
  b. El derecho a la limitación del tratamiento, que se aplicaría en su otra vertiente, es decir, se solicite al responsable que se conserven las imágenes cuando:
     - El tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso.
     - El responsable ya no necesite los datos para los fines del tratamiento pero el interesado si los necesite para la formulación, ejercicio o defensa de reclamaciones.

- Comunicación de imágenes a terceros.- En el ámbito que nos ocupa este tipo de comunicaciones sin consentimiento de los interesados ocurren con mayor frecuencia en los siguientes casos:

- Cuando la comunicación de imágenes tengan por destinatarios los Jueces o Tribunales.
- Cuando las Fuerzas y Cuerpos de Seguridad soliciten las grabaciones en aquellos supuestos que son necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2.2. Publicación de contenido audiovisual

La Consejería de Educación dispone de un registro de actividades de tratamiento, en el cual se incluye como uno de los tratamientos el 'Contenido audiovisual de las actividades de los centros y servicios educativo'. Dicho tratamiento habilita el tratamiento de imágenes del alumnado, padres, madres y/o tutores de alumnos y personal del centro por parte de los centros docentes con la finalidad de la promoción y difusión en los sitios web de los centros y servicios educativos de las actividades culturales, recreativas, deportivas y sociales en las que participa el propio centro.

Para el cumplimiento de la normativa en materia de protección de datos de carácter personal en la toma de fotografías y/o vídeo o cualquier contenido audiovisual, como su publicación en Internet requieren cumplir con el derecho de información, la solicitud del consentimiento que debe ser inequívoco y prestado mediante una clara acción afirmativa y así como un conjunto de medidas que garanticen la protección de los mismos. En consecuencia, los centros educativos que deseen publicar contenido audiovisual de la comunidad educativa deberán:

- Rellenar y mantener actualizado en Séneca el formulario que a tal efecto está disponible (apartado 'Centro' / 'Cuestionarios' / 'Seguridad y protección de datos' / 'Publicación contenido audiovisual').

- Asegurar que la finalidad de la publicación es apropiada mediante la evaluación previa del tipo de foto, la pertinencia de su publicación y su objetivo.

- Informar y solicitar consentimiento a las personas cuyas imágenes se tomen y publiquen. La captura de contenido audiovisual (fotografías, vídeo, etc.) como su publicación (Internet) requieren el conocimiento y consentimiento del afectado. En caso de fotografiar a un alumno menor de 14 años, se debe informar y recabar el consentimiento de sus padres o tutores.

- Para ello es necesario cumplir con estos derechos en los formularios de matriculación, contratación, etc. o en formularios ad-hoc previos al evento, mediante un impreso que muestre la cláusula informativa del tratamiento, solicite el consentimiento e indique si la validez es puntual, anual o abarca la totalidad temporal del vínculo del afectado con el centro docente.

- Garantizar la atención a los derechos reconocidos en los plazos previstos. Tiene especial consideración cuando el afectado solicita la oposición o cancelación del uso

de las fotografías se debe proceder al borrado de las imágenes o al pixelado de la imagen del afectado en caso de ser una foto de grupo.

2.3. Cesión de datos

La comunicación a otras entidades u organismos de los datos de carácter personal que tratamos en los centros y servicios educativos es una acción que debe ser supervisada con extremo detalle. Una comunicación no conocida y consentida, expresa o implícitamente, por la persona a la que identifican los datos constituye una cesión no permitida y por lo tanto una infracción de la normativa de protección de datos de carácter personal.

Debido a la importancia y riesgo que supone la comunicación de datos, se estima necesario que ante la solicitud de datos por parte de un organismo o entidad, previamente a su comunicación, se realice una consulta a la cuenta se@maralboran.es. Recibida la consulta,

- la solicitud de comunicación se registra,
- se valora si es legalmente viable en función del cumplimiento de la LOPD y
- se responde al solicitante informando sobre su viabilidad de forma clara y detallada.

2.4. Publicación de datos de carácter personal

La publicación de datos de carácter personal requiere que previamente se cumpla con las siguientes pautas de actuación para asegurar un tratamiento adecuado de los datos de carácter personal en los términos requeridos por la normativa en materia de protección de datos de carácter personal:

- Tratar los datos únicamente para la finalidad para la que se han recabado: los datos se recaban de los ciudadanos para una o varias finalidades. En el caso de datos de carácter personal, además, esa finalidad es la única informada y consentida por el ciudadano, por lo que es necesario que conozca y apruebe si se va a tratar para otro fin (ejemplo: una publicación en Internet).
- Tratar los datos únicamente en los sistemas informáticos previstos a tal efecto que están autorizados por la Consejería.
- Publicar datos personales en Internet es una cesión de datos de carácter personal; por tanto solo se deben publicar datos personales en Internet tras informar y solicitar consentimiento a los afectados.
- Verificar que los datos que se publican son estrictamente los mínimos necesarios.

3. TRATAMIENTO DE DATOS PERSONALES

3.1 Responsable del tratamiento de datos (DTD –Delegado de tratamiento de datos-)

En el IES Mar de Alborán, en cumplimiento de lo establecido en los artículos 34 y 35 de la Ley Orgánica 3/2018, tenemos la figura del Delegado de Tratamiento de Datos que recae en la figura del Vicedirector del centro ya que posee los conocimientos de derecho y formación en Protección de Datos mínimos requeridos para atender cualquier requerimiento o reclamación de algún demandante, salvo que otra persona acreditada solicite desempeñar esta función. El **Equipo Directivo** tiene la obligación de dar a conocer este protocolo de Protección y Tratamiento de Datos, pero **no es el responsable del mal uso por parte de cualquier miembro** de la

comunidad educativa. Cualquier miembro de la comunidad educativa que trate los datos del centro debe tener en cuenta el principio del secreto y el permiso para el uso de los datos para según qué actividades o en el uso de plataformas, siendo la responsabilidad del mal uso la persona que los trate de forma irresponsable. Debe tenerse en cuenta además que los datos tratados en el centro tienen una finalidad educativa, no pudiéndose usar con otra finalidad sin que se tenga un consentimiento expreso por parte de los afectados y/o afectadas, a los que ha de informarse previamente de la finalidad de su uso.

3.2. Tipología de datos

En el IES Mar de Alborán los datos tratados son todos de carácter personal. Se recaban nombre y apellidos del alumnado, familiares y del personal, número de teléfono, correos electrónicos, profesión, estudios, domicilio e incluso en algún momento el número de cuenta bancaria.

En cuanto a los datos sensibles (especialmente datos médicos del alumnado) siempre son entregados por sus propietarios de forma explícita en el momento de matriculación, ya que este procedimiento administrativo se lleva a cabo mediante el sobre electrónico de matrícula gestionado por la Junta de Andalucía a través de la Secretaría virtual de los centros docentes de Málaga. Todos los datos personales mencionados anteriormente son recabados a través de un método que garantiza la seguridad y confidencialidad de los mismos. Posteriormente, en el Portal de Séneca, considerando los diferentes perfiles creados para su uso, solo el tutor o tutora y miembros del Equipo Directivo tienen acceso a la ficha del alumno y a los datos extremadamente sensibles sobre su situación familiar y médica.

Ante todos los datos recogidos y a todo el personal que tenga acceso a él, le corresponde la obligación del secreto, así como la prohibición de su uso para otros fines que no sean los estrictamente relacionados con la docencia y la vida del centro educativo.

3.3. Procedimiento de recogida de datos

La recogida de datos por parte del IES Mar de Alborán se realiza con el alumnado, las familias y el personal del centro. La recogida de datos del alumnado y las familias se realiza a través de las matrículas y en las reuniones que se estimen oportunas a lo largo del curso con el profesorado del centro con fines educativos. Los datos que se recaban son todos de carácter personal, debiendo ser exactos, y en caso contrario, modificados en cuanto se produzca un cambio. Estos datos recogidos son por una obligación legal de los centros educativos, pues ha de mantenerse un contacto con las familias del alumnado, así como recabar información del alumnado o sus familias con fines educativos o de orientación.

La matrícula electrónica llevada a cabo por nuestro centro incluye una autorización sobre la recogida de datos y el uso de la imagen del alumno o alumna exclusivamente con fines educativos. Las familias pueden dar su conformidad o disconformidad a la hora de cumplimentar estos documentos de la matrícula. El profesorado con perfil de tutor/a y dirección puede consultar esta información acerca de su alumnado en el portal de Séneca (Documentos/Alumnado/gestión de autorizaciones/firma). En el apartado "títulos" aparecerán todas las autorizaciones registradas por el centro y la Delegación, entre ellas se encuentran los Programas Específicos, autorizaciones sobre el uso del correo electrónico, autorizaciones sobre el uso de la imagen del alumno/a y autorizaciones sobre el uso del móvil en clase por parte del alumnado como una herramienta didáctica siempre y cuando el profesorado lo estipule así en su aula. Por otro lado, en el apartado "Mostrar las autorizaciones con estado" → "Autorizado/Firmado; No autorizado/No firmado; Pendiente" el profesorado con perfil de tutor/a y

direccción podrá asegurarse del estado de las autorizaciones antes de emprender la publicación de datos del alumnado. Para facilitar la consulta del alumnado que no ha autorizado se pondrá en las unidades compartidas de Drive un listado con esta información en la siguiente ruta: Documento del profesorado/protección de datos/Listado de alumnado No autoriza.

No obstante, a lo largo del curso se pueden recabar datos y/o autorizaciones expresas para actividades complementarias que se desarrollen fuera del centro, para el uso de la imagen del alumnado o para eventos que se organicen por el centro fuera o dentro del mismo, así como los trámites administrativos derivados de la práctica docente y del funcionamiento del centro (entrevistas con las familias, compromisos educativos, informes de evaluación, etc.).

El profesorado recabará y tratará datos del alumnado durante todo el curso con la finalidad evaluadora y para la práctica docente (exámenes, pruebas, trabajos, informes, audiciones, presentaciones, obras teatrales, etc.).

La recogida de datos del personal se lleva a cabo por parte del centro y a través de la Administración (Delegación Territorial, Consejería de Educación…), que son los que establecen una relación del personal con el centro, de ahí su necesidad. En caso de pertenecer a la plantilla de forma estable no es necesario recabar ninguna información (salvo que se produzcan cambios en los datos ya existentes) y en el caso del personal que se incorpora cada curso, se pide los datos que nos pide la administración educativa a principio de curso.

3.4. Publicación de datos del alumnado

En este caso deberíamos diferenciar entre los datos que se recaban en la matrícula y pertenecen al expediente del alumnado y los datos recabados por el profesorado a lo largo del proceso de enseñanza-aprendizaje y con una finalidad evaluadora del mismo.

En el primer supuesto, los datos son accesibles desde la aplicación Séneca y también de forma física en los archivos de administración, debidamente custodiados. Los datos físicos pueden ser consultados, pero nunca sustraídos del centro, debiendo ser devueltos una vez consultados a su archivo correspondiente.

En los datos recabados como fruto del proceso educativo a lo largo del curso, los datos serán custodiados por el profesorado correspondiente. En caso de ser en formato físico deberá ser guardado en el centro durante todo el curso y **hasta al menos junio del curso siguiente**, salvo que haya un proceso de reclamación u otro tipo de procedimientos que requiera que se guarden estos datos durante un periodo de tiempo superior, al menos mientras dure los posibles procedimientos.

El profesorado y el centro podrá publicar datos (trabajos, informes, imágenes, vídeos, audiciones…) del alumnado en la web del centro o en las redes sociales del mismo, siempre con finalidad educativa y que cuente **con el consentimiento expreso de los o las afectadas**. En el

caso de menores de 14 años siempre con el consentimiento de los tutores o tutoras legales, y en el caso de los mayores de 14 años con el consentimiento expreso del afectado o afectada. No podrán publicarse datos que comprometan la integridad y el honor del alumnado y que no tengan una finalidad educativa.

El profesorado y el centro podrán publicar datos del alumnado en el caso de participar en concursos o certámenes, siempre que haya recogido expresamente los consentimientos pertinentes.

El profesorado y el centro podrán recabar cualquier información del alumnado con fines educativos, siempre que no implique su publicación, para lo cual se requerirá el consentimiento expreso. Es de gran importancia el deber de secreto en todos los datos tratados en el centro, así como la información del personal del centro, las familias o el alumnado en general.

3.4. **Calificaciones**

Las calificaciones del alumnado son datos personales que no pueden hacerse públicas en ningún momento. Un alumno o alumna puede negarse a que el profesorado diga públicamente sus calificaciones ante terceros.

Las calificaciones serán entregadas de forma personal al alumnado y sus familias o responsables legales. En el caso de los boletines de notas sólo se podrán entregar a las familias o responsables legales del alumnado y se podrán publicar en las áreas privadas de iPasen para cada familia, no pudiéndose **en ningún momento publicar las calificaciones en tablones de anuncio situados en espacios comunes o en cualquier medio digital, que no respete la privacidad de los datos publicados**.

En el caso de hacerse públicas las calificaciones del alumnado deberá hacerse de forma que no sea identificable el alumnado por terceros.

3.4.1. Criterios para publicar las notas de los alumnos

La Agencia Española de Protección de Datos (AEPD), en un reciente Informe de fecha 21/05/2019, considera lícita la publicación de las calificaciones de los estudiantes, sin necesidad de contar con su consentimiento expreso. Señala cómo el legislador ha reconocido en ello la existencia de un interés público y un interés legítimo por parte de los alumnos del grupo por lo que su publicación está amparada en el Reglamento General de Protección de Datos (RGPD).

Siendo lícita la publicación de las notas, la Agencia estima que deberán respetarse en todo caso los principios recogidos en el RGPD de modo que esta publicación suponga la menor injerencia posible en los derechos y libertades de los interesados para lo cual deberán tenerse en cuenta los siguientes criterios:

a) Excluir la posibilidad de conocimiento generalizado de las calificaciones (NO publicación en internet).
b) Utilizar como medio preferente la publicación a través del Cuaderno de Séneca, Moodle, en el aula virtual con acceso limitado a profesores y compañeros de grupo o cualquiera otra herramienta en un medio que hay suscrito un convenio con la Junta de Andalucía que, este caso, se convierte en garante de la seguridad de los datos.
c) Si no fuera posible, se pueden utilizar los tablones de anuncios del centro, siempre que no se encuentren en las zonas comunes, se garantice que el acceso queda restringido a los interesados y se adopten las medidas necesarias para evitar su público conocimiento por quienes carecen de interés en el mismo.
d) Los datos a publicar deberán limitarse al nombre y apellidos del alumno y la calificación obtenida. Sólo en caso de que hubiera alumnos con los mismos nombres

y apellidos deberá publicarse para ellos cuatro cifras aleatorias de su DNI o equivalente, siguiendo estos criterios: https://www.aepd.es/media/docs/orientaciones-da7.pdf

e) La publicación de calificaciones provisionales sólo se mantendrá mientras transcurre el plazo para presentar reclamaciones.
f) La publicación de las calificaciones definitivas lo será durante el tiempo imprescindible que garantice su conocimiento para todos los interesados.

3.5. Acceso a la información del alumnado

El acceso a la información del alumnado está en el sistema de Séneca y de forma física en el despacho de Administración del centro, en archivos debidamente custodiados. El profesorado y el personal administrativo tienen acceso directo a esta información del alumnado. En el caso de ser requerida por las familias, al ser propietarias de la información del alumnado, pueden tener acceso a la misma y deberá darse información de cómo se tratan, gestionan y qué finalidad tiene la recogida de todos los datos en caso de que lo requieran.

En el caso de que la administración o cualquier organismo público requieran información del alumnado o las familias, el centro deberá facilitarla siempre que sea legítimo su uso.

3.6. Comunicaciones de datos del alumnado

Los datos del alumnado no pueden ser comunicados a terceros, a no ser que sea requerido legalmente al centro. Siempre que se comuniquen datos del alumnado por el centro (sin requerimiento legal de la administración) deberá de contarse con el consentimiento expreso de las familias y/o del afectado o afectado en caso necesario.

3.7. Actividades de tratamiento de la información

A continuación, se recogen las actividades de tratamiento de la información que se llevan a cabo en el IES Mar de Alborán, determinando responsable, finalidad, categoría de los datos, interesados/as, destinatarios/as, plazo de supresión y medidas de seguridad. Estas actividades entran todas dentro del carácter administrativo de los centros educativos y la recogida de datos siempre es de datos personales, nunca se requieren datos sensibles, salvo que sean proporcionados por los interesados de forma expresa.

TRATAMIENTO	***RECOGIDA DE DATOS NUEVAS INCORPORACIONES DEL PERSONAL***
RESPONSABLE	Equipo directivo, Administrativas del centro
FINES DE LOS DATOS	Identificación del personal, forma de contacto
CATEGORÍA DE LOS DATOS	Personal
INTERESADOS	Administración
DESTINATARIOS/AS	Administración Educativa
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia debidamente en archivadores bajo llave.
OBSERVACIONES	

TRATAMIENTO	***REGISTRO DE ASITENCIA DEL PERSONAL DEL CENTRO***
RESPONSABLE	Equipo directivo
FINES DE LOS DATOS	Control de asistencia diaria mediante Geolocalización o código QR a través de Séneca o iSéneca. Justificante de ausencias.
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Administración Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.

MEDIDAS DE SEGUIRAD	Lo custodia JE y las administrativas..
OBSERVACIONES	

TRATAMIENTO	***Matrículas/expedientes/documentos administrativos/becas del alumnado***
RESPONSABLE	Equipo directivo y Administrativas del centro.
FINES DE LOS DATOS	Recabar datos académicos y personales del alumnado.
CATEGORÍA DE LOS DATOS	Personal
INTERESADOS	Administración Educativa, Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia debidamente en archivadores bajo llave.
OBSERVACIONES	

TRATAMIENTO	***REGISTROS DEL ALUMNADO (Asistencia, Entrada y Salida del centro, uso del baño)***
RESPONSABLE	Equipo directivo
FINES DE LOS DATOS	Llevar un registro de las distinta actividades del alumnado
CATEGORÍA DE LOS DATOS	Personal (Nombre y apellidos)
INTERESADOS	JE, Coordinador/a de Convivencia, Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia en JE.
OBSERVACIONES	

TRATAMIENTO	***Exámenes, trabajo, audiciones, vídeos o cualquier otro documento de evaluación***
RESPONSABLE	Profesorado
FINES DE LOS DATOS	Recabar información para el proceso de evaluación del alumnado
CATEGORÍA DE LOS DATOS	Personal (Nombre y apellidos)
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Disponibilidad para cualquier interesado/a que requiera de dicha información
OBSERVACIONES	

TRATAMIENTO	***Documentos e informes docentes (Actas de evaluación, partes de conducta, entrevistas con familia o alumnado, compromisos educativos…)***
RESPONSABLE	Profesorado y Equipo Directivo
FINES DE LOS DATOS	Recabar datos académicos del alumnado y su evolución
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia en JE
OBSERVACIONES	

TRATAMIENTO	***Autorizaciones para la realización de actividades extraescolares o complementarias dentro o fuera del centro***
RESPONSABLE	Jefes/as de los departamentos, Coordinador/a de la actividad complementaria
FINES DE LOS DATOS	Recabar el consentimiento expreso para la realización de dichas actividades.
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Lo custodia el Coordinador/a de la actividad, Jefe/a del Dpto. Se recomienda su custodia en Séneca o iSéneca en el apartado de “autorizaciones/firma”
OBSERVACIONES	

TRATAMIENTO	***Autorización del uso de la imagen***
RESPONSABLE	Tutoras/es, Equipo Directivo
FINES DE LOS DATOS	Recabar el consentimiento expreso para el uso de la imagen del alumnado en la web y redes sociales del centro con fines educativos

CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia se realiza en Séneca e iSéneca ("Autorizaciones/firma")
OBSERVACIONES	

TRATAMIENTO	***Correos electrónicos, Gsuite –Classroom/Moodle-***
RESPONSABLE	Profesorado y Equipo Directivo
FINES DE LOS DATOS	Recabar datos académicos del alumnado y su evolución y establecer comunicación
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	GSuite y Moodle cumplen con la normativa de protección de datos. No obstante, otras aplicaciones que no están dentro del convenio de la Junta de Andalucía no poseen la cobertura en relación a la protección de datos.
OBSERVACIONES	

TRATAMIENTO	***Programaciones didácticas y otros documentos que se requiere para la docencia***
RESPONSABLE	Departamentos Didácticos y Equipo Directivo
FINES DE LOS DATOS	Organizar y planificar la labor docente y dejar constancia de las mismas.
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia en archivadores bajo llave (Secretaría y/o JE). Las programaciones didácticas están dentro de Séneca y en una carpeta de las Unidades compartidas en nuestro Drive de Google.
OBSERVACIONES	

TRATAMIENTO	***Videovigilancia***
RESPONSABLE	Equipo Directivo (Preferentemente la Dirección del centro y, durante su ausencia, la Vicedirección del centro junto el/la JE)
FINES DE LOS DATOS	Mantener el orden en el centro, obtención de pruebas para objetivar la aplicación de medidas disciplinarias.
CATEGORÍA DE LOS DATOS	Personales
INTERESADOS	Comunidad Educativa
DESTINATARIOS/AS	
PLAZO DE SUPRESIÓN	Cuando desaparezca la finalidad legítima del tratamiento de datos o se ejercite el derecho de supresión.
MEDIDAS DE SEGUIRAD	Se custodia en el despecho de la Dirección del centro.
OBSERVACIONES	

4. TRATAMIENTO DE LOS DATOS EN INTERNET

4.1 **Utilización de plataformas educativas**

En el IES Mar de Alborán usamos dos plataformas esencialmente. Una es Séneca, así como su homóloga Moodle, proporcionadas por la Junta de Andalucía y que cumple con todos los requisitos, y la otra es GSUITE, la plataforma de Google para los centros Educativos, la cual también cumple con todos los estándares de tratamiento de datos, estando en el listado de sitios web que cumplen con todos los requisitos. Asimismo, el profesorado tiene la posibilidad de trabajar con Microsoft para trabajar los documentos incluidos en el paquete ofimático Microsoft 365 (Outlook, Microsoft Office, OneDrive, Word y Power Point) dado que Microsoft actualmente está dentro del convenio firmado por la Junta de Andalucía.

Fuera de estas aplicaciones, se pueden usar plataformas o aplicaciones web que no requieran de datos personales del alumnado o familias, y siempre que se usen deberá informarse al responsable del tratamiento de datos para la verificación de la política de protección de datos de dichas aplicaciones o plataformas educativas.

4.2. Publicación de datos en la web y redes sociales del centro.

El centro cuenta con una página web, maralboran.eu, en la que se publica con regularidad información del centro para las familias y el alumnado y también se publicitan y publican las actividades que se realizan por parte del centro, tanto dentro como fuera del mismo. Para ello se pide en la matrícula el consentimiento en el uso de la imagen por parte de las familias y a los mayores de 14 años también se le solicitará antes de publicar cualquier imagen, vídeo o dato personal que le pertenezca para tener el consentimiento expreso. También contamos con varios blogs educativos, cuenta de Instagram, Facebook y Twitter, en las que publicamos la misma información. Todas las publicaciones tienen un carácter divulgativo e informativo de la actividad docente del centro, cumpliendo con la finalidad para la que se recaba la información y se publica. Asimismo, nuestra página web tiene alojadas algunas bahías en donde se encuentran las páginas web particulares de cada departamento, gestionada por el Jefe/a del Departamento en cuestión. En ella, se publica información didáctica que guarda relación con los contenidos epistemológicos de cada módulo, materia o área, además de imágenes relacionadas con actividades complementarias de esos departamentos en cuestión.

Nuestra página web continuamente se está actualizando para ofrecer el mejor servicio informativo a toda la comunidad educativa, de forma que cualquier miembro puede estar puntualmente informado sea cual sea su necesidad.

4.3. Ciberseguridad

A nivel de seguridad llevamos ya varios años con un sistema basado en un servidor que carga los diferentes perfiles del profesorado. Asimismo, los ordenadores del profesorado en despechos y aulas están congelados. Estos ordenadores están configurados mediante la memoria flash, tratándose de un dispositivo de almacenamiento informático que puede guardar datos durante cortos periodos de tiempo, lo que hace más seguros nuestros ordenadores ante virus ajenos. De otro lado, el perfil del profesorado contempla una clave acceso y el material que guarda en su perfil es privado, teniendo la garantía de que se cumplen los requisitos de privacidad para guardar documentos de evaluación. Si bien es cierto que la política de contraseñas para los perfiles de dominio es mejorable.

Este apartado es de gran importancia debido a la gran cantidad de datos que se manejan en internet. Para ello se hacen necesarias herramientas para verificar claves o la seguridad de las páginas que se usen o consulten, para lo que añadimos las siguientes como opciones:

4.3.1. Herramientas

– Verificar las claves; https://password.kaspersky.com/es/
– Verificar si una página web (o enlace) es segura: https://safeweb.norton.com/ o http://www.urlvoid.com/

– Verificar si un fichero tiene virus: https://www.virustotal.com
– Productos y recomendaciones de Sw de seguridad: https://satinfo.es/
– Antivirus gratuitos: McAfee, Norton, Kaspersky, Avast. Todos cuentan con versiones gratuitas para PC y móvil, especialmente para los portátiles facilitados por la Junta de Andalucía.
• AVG Anti-Virus Free http://www.avg.com/es-es/free-antivirus-download
• Avast Free Antivirus http://www.avast.com/es-es/index
• Microsoft Essentials http://www.microsoft.com/security_essentials/
• Ad-Aware de lavasoft (http://www.lavasoft.com/) incluye antivirus y antiespías en un solo paquete.

4.3.2. Consultas

1. Consejos sobre pantallas (app); www.contraste.info
2. Instituto Nacional de Ciberseguridad (INCIBE): www.incibe.es
3. Oficina de Seguridad del Internauta: www.osi.es
4. Bulos que corren por Internet: https://maldita.es/
5. Línea de ayuda: 017

4.3.3. Recomendaciones de medidas de ciberseguridad

1. Uso de contraseñas seguras.
2. Actualización de las aplicaciones.
3. Cierre de las aplicaciones cuando no se usen.
4. Descarga de aplicaciones originales.
5. Uso de un antivirus de confianza.
6. Verificar las apps a descargar y los sitios web a usar.
7. En las redes sociales tener cuidado con lo que publicamos.
8. Cifrar la información crítica.
9. En los ordenadores tener varios usuarios.
10. No abrir correos sospechosos o spams.
11. Usar el sentido común.
12. En el uso de espacios de almacenamiento en la nube, borrar la información innecesaria y guardar de forma segura aquellos datos que estimemos importante.
13. Establecer contraseñas en los archivos sensibles.

4.3.4. Uso de aplicaciones, plataformas virtuales de aprendizaje y sistemas de mensajería instantáneas

Los centros educativos deben observar la debida diligencia con los tratamientos de datos personales, incluyendo los que se producen como consecuencia de la llegada de las tecnologías a las aulas, velando por que se reúnan las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos.

Normas internas:

- Los usuarios deben tener especial cuidado al publicar imágenes y vídeos mediante apps y herramientas en la nube para no poner en riesgo la intimidad de otras personas.

- Se recomienda leer la información sobre el servicio (política de privacidad y condiciones de uso) antes de empezar a utilizarlo.
- Al utilizar redes sociales se recomienda configurar las opciones de privacidad en el perfil de usuario para permitir el acceso a la información publicada a un grupo conocido y previamente definido de usuarios.
- Al facilitar datos en cualquier ámbito (en cualquier tipo de aplicación, en el registro de usuarios, en los contenidos) debe evitarse incorporar datos del domicilio de los menores y otros datos personales que puedan poner en peligro su seguridad.
- Debe recomendarse no atender la demanda que puedan tener las aplicaciones para recabar datos personales, que pueda llevar al tratamiento de datos excesivos.
- Al utilizar sistemas de almacenamiento de documentos en nube tipo Dropbox, iCloud o Google Drive, se debe evitar incluir datos personales sensibles, tales como datos relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, etc.
- Cuando exista en el centro una plataforma educativa que permita la interacción entre alumnos/as, y entre estos/as y los profesores, se aconseja que se prime su utilización para este fin, sin establecer mecanismos de comunicación adicionales.

En relación con la base de legitimación, cuando el centro emplea plataformas educativas puestas a su disposición por la Administración para fines docentes u orientadores del alumnado, no debe solicitarse el consentimiento de los interesados, pues el tratamiento se basa en el cumplimiento de una misión realizada en interés público o de una obligación legal, como es el ejercicio de la función educativa. En caso de otros fines, es preciso el consentimiento.

5. TRATAMIENTO DE LAS IMÁGENES DEL ALUMNADO

En el caso de grabación y/o uso de imágenes del alumnado, antes de su publicación en la web o redes sociales del centro deberá contarse con el consentimiento expreso de las familias y/o del alumnado en cuestión. Este consentimiento figura como autorización al uso de imagen del alumnado en la matrícula electrónica de inscripción al centro. **No obstante, el profesorado debe conocer qué alumnos/as no tienen la autorización de sus tutores/as legales– en caso de ser menores de 14 años-.** El uso de imágenes siempre será con **fines educativos**, y **no podrá usarse en redes sociales o blogs del profesorado o de las familias sin el consentimiento expreso de los afectados y afectadas**. Las imágenes publicadas en la web o redes sociales del centro permanecerán en las mismas salvo que las familias o el alumnado en cuestión requieran su eliminación.

5.1. Grabación de imágenes durante actividades extraescolares y/o complementarias

Durante las actividades extraescolares y/o complementarias podrán ser tomadas imágenes o vídeos por parte del profesorado, siempre que la finalidad sea educativa y que no sean publicadas sin el consentimiento expreso del alumnado o sus familias.

5.2. Grabación y difusión de imágenes en eventos organizados y celebrados en el centro

Durante los eventos organizados y celebrados en el centro podrán ser tomadas imágenes o vídeos por parte del profesorado y las familias, siempre que la finalidad sea educativa y que no sean publicadas sin el consentimiento expreso del alumnado o sus

familias. **No obstante, empresas externas al centro no podrán tener acceso a estas imágenes.**

5.3. Grabación de imágenes de actividades desarrolladas fuera del centro

Durante las actividades extraescolares y/o complementarias realizadas fuera del centro podrán ser tomadas imágenes o vídeos por parte del profesorado, siempre que la finalidad sea educativa y que no sean publicadas sin el consentimiento expreso del alumnado o sus familias.

6. DERECHOS EN MATERIA DE PROTECCIÓN

6.1. Derecho de acceso

Los y las propietarias de los datos tendrán siempre acceso a los mismos presentando previamente la documentación identificativa, especificando el motivo por el que desea tener acceso a los mismos mediante una solicitud.

6.2. Derecho de rectificación

El centro está obligado a facilitar a los propietarios de los datos la rectificación de los datos personales inexactos o la modificación de los mismos. Para ello deberán rellenar un formulario específico y presentarlo en la secretaría del centro, o enviarlo por correo al correo se@maralborán.es.

6.3. Derecho de cancelación

El centro está obligado a facilitar el derecho de supresión de los datos personales cuando estos no sean necesarios, cuando se retire el consentimiento, cuando el interesado/a se oponga al tratamiento de los datos, cuando los datos personales hayan sido tratados de forma ilícita o cuando deban suprimirse en cumplimiento de una obligación legal. El interesado o interesada deberá indicar con claridad qué datos desean que se eliminen y el motivo por el que lo solicita. En estos casos los datos en formato físico podrán ser entregados al interesado o interesada con acuse de recibo, y firmando un compromiso de eliminación de los datos digitalizados, siempre que sea potestad del centro educativo su eliminación.

6.4. Derecho de oposición

Los interesados o interesadas pueden oponerse en cualquier momento a proporcionar datos personales o sensibles que no consideren necesarios. En caso de no proporcionar ciertos datos necesarios para la labor docente o el funcionamiento del centro, se le hará saber las consecuencias de no proporcionar dichos datos.

Salvo en los casos que se acrediten motivos legítimos imperiosos para el tratamiento de dichos datos, el o la responsable del tratamiento de datos dejará de utilizar dichos datos. El interesado o interesada deberá rellenar un formulario para ejercer su derecho de oposición en el tratamiento de los datos, especificando los datos que no quiere que se usen en el centro.

7. BRECHAS DE SEGURIDAD DE DATOS PERSONALES

Aunque el RGPD se refiere a estos incidentes como violaciones de seguridad, el término que comúnmente se utiliza es el de **brechas de seguridad de datos personales**. El

artículo 4.12 del RGPD las define como "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".

Todo el personal del centro, en primer lugar, tiene la obligación de cumplir con los protocolos o las medidas de seguridad establecidas por el responsable del tratamiento, (que deberían ser comunicadas a los centros y estar disponibles, por ejemplo, en la web del responsable), tanto para prevenir incidentes de seguridad, como para gestionar las posibles brechas que se detecten.

En caso de surgir un incidente de seguridad, cuando el centro no sea el responsable del tratamiento deberá informar de ello con la mayor diligencia al Delegado/a de Protección de Datos, quien deberá encargarse de valorar su gravedad, si se han visto comprometidos datos personales, de dar las instrucciones adecuadas para paliar los efectos del incidente y para evitar en lo posible mayores daños en el ámbito de la privacidad de los interesados. El Delegado/a de Protección de Datos ofrecerá un modelo de Incidente de Brecha de Seguridad de Datos para describir el incidente.

Por todo ello, el Delegado de Protección de Datos facilitará al personal docente y no docente cuyos datos figuren en la página web del centro un modelo específico para el consentimiento informado en el que podrán dar o no su consentimiento.

Entre otros, pueden citarse a modo orientativo los siguientes ejemplos de riesgos de seguridad o incidentes, ya se produzcan de forma intencionada o no intencionada:

- Pérdida, robo o depósito en localización insegura de documentación en formato papel que contenga datos personales.
- Destrucción incorrecta de datos personales en formato papel o eliminación incompleta de archivos con datos personales en carpetas o dispositivos.
- Ciberataque mediante malware (software malicioso): es un tipo de software que tiene como objetivo infiltrarse, dañar o causar un malfuncionamiento a un ordenador o conjunto de ellos en red, sin el consentimiento de su propietario.
- Ciberataque mediante phishing o suplantación de identidad: es una de las técnicas más usadas para obtener información suplantando a una entidad legítima como puede ser un banco, una red social, una entidad pública, un centro docente o cultural.
- Ciberataque mediante DoS ó DDoS: Se entiende como denegación de servicio (DoS) al conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Este tipo de ataques satura o colapsa un servidor y no permite que sus legítimos usuarios puedan utilizar los servicios prestados por él. En la denegación distribuida (DDoS), el incidente se causa utilizando múltiples puntos de ataque simultáneamente.
- Correo electrónico o postal perdido o abierto por personas distintas a sus destinatarios.
- Dispositivo electrónico (CD, DVD, USB, Ordenador, Móvil, Tablet…) perdido o robado que almacene datos personales.
- Publicación indebida de datos personales en cualquier medio.
- Datos personales mostrados o facilitados a una persona incorrecta.
- Revelación verbal no autorizada de datos personales.

8. PROTOCOLO DE BUENAS PRÁCTICAS

Salvando todas aquellas actuaciones que hasta a la fecha respetaban la normativa vigente en protección de datos, cabe destacar un conjunto de medidas que pueden ayudar a mejorar el tratamiento de los datos que hacemos en el centro. Por ello, a continuación se enumera una serie de medidas de mejoras que pueden contribuir a la creación de un protocolo de buenas prácticas en nuestro centro:

a) Solicitud de consentimiento informado a los docentes que aparecen en la página web mediante un anexo que podrá descargar desde las unidades compartidas de nuestro Drive.
b) Se recogen las actividades de tratamiento de la información que se llevan a cabo en el IES Mar de Alborán, determinando responsable, finalidad, categoría de los datos, interesados/as, destinatarios/as, plazo de supresión y medidas de seguridad. Estas actividades entran todas dentro del carácter administrativo de los centros educativos y la recogida de datos siempre es de datos personales, nunca se requieren datos sensibles, salvo que sean proporcionados por los interesados de forma expresa
c) Nombramiento oficial de la figura del Delegado de Protección de Datos.
d) Se ofrecen recomendaciones de seguridad en el apartado de ciberseguridad.
e) Antes de publicar cualquier imagen o vídeo en internet que contenga imágenes de nuestro alumnado tendremos que consultar en Séneca si han dado su consentimiento expreso.
f) Colocar icono de cámaras de seguridad en cada módulo.
g) No se debe publicar en zonas comunes del centro datos personales del alumnado junto con sus calificaciones.
h) La publicación de listados de admitidos o excluidos, alumnado seleccionado para un programa o plan del centro, o casos similares podrán publicarse en zonas comunes pero no en internet. Asimismo, los datos sensibles han de publicarse parcialmente para proteger las privacidad de los mismos (DNI, pasaporte, etc…) tal como se indica en el apartado correspondiente.
i) Las calificaciones del alumnado de las Pruebas Libres de la ESO se publican prioritariamente en la página de Formación Permanente de la Junta de Andalucía de forma individualizada. Los admitidos podrán acceder mediante su clave iANDE. De tener que hacerse la consulta de forma física por cualquier incidente digital, podrá publicarse un “LISTADO PUBLICABLE” que Séneca ofrece a tal efecto en donde se omite información sensible.
j) Se deben utilizar aplicaciones autorizadas por la Junta de Andalucía en el tratamiento de datos: Moodle, Séneca, iSéneca, GSuite de Google y Microsoft. Idoceo y Aditio no están autorizados por la Junta de Andalucía pese a que cumplen con los requisitos de la AEPD.
k) Si guardamos información en carpetas privadas con datos personales del alumnado debe estar debidamente cifrada con código de acceso.
l) La información altamente sensible como la situación familiar del alumnado, o datos del alumnado con NEAE puede distribuirse al profesorado de forma que no puedan editarla, ni publicarla. Es solo información de consulta y lectura. Podrá publicarse en las unidades compartidas de Drive siempre que el permiso concedido sea únicamente el de lectura.

m) El alumnado puede negarse a que se digan públicamente sus notas o a que aparezcan proyectadas públicamente ante la clase. Se recomienda pedir consentimiento expreso antes de su proyección pública en el aula.
n) Se recuerda que la transgresión de la privacidad de datos de un miembro de la comunidad educativa no es responsabilidad de la dirección del centro. El centro tiene la obligación de informar a la comunidad educativa y velar por su cumplimiento.
o) Se han confeccionado diferentes documentos para garantizar el derecho de todos los miembros de la comunidad educativa al acceso, cancelación, oposición y rectificación de los datos personales.