

Curso 2023/24



GUÍA SOBRE EL USO RESPONSABLE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ÍNDICE

1. PRESENTACIÓN
2. PRINCIPIOS SOBRE EL BUEN USO DE LAS TIC
3. PRÁCTICAS PARA USO RESPONSABLE DE LAS TIC
4. NORMAS DE USO DE LOS DISPOSITIVOS PORTÁTILES DEL CENTRO
5. CONDUCTAS CONTRA LA CONVIVENCIA EN EL USO DE LAS TECNOLOGÍAS
6. DETECCIÓN DE CONDUCTAS DE POSIBLE ACOSO EN LA RED
7. BIBLIOGRAFÍA Y DOCUMENTOS DE REFERENCIA
8. ANEXOS
 - Guía para el profesorado sobre protección de datos en el ámbito educativo y código de conducta elaborado por la Junta de Andalucía para el uso de las TIC
 - Modelo de préstamo de ordenadores portátil para el profesorado
 - Modelo de préstamo de ordenadores portátiles para el alumnado
 - Compromiso de uso extraordinario de teléfonos móviles en el viaje de estudios.

1. PRESENTACIÓN.

Las Tecnologías de la Información y la Comunicación (TIC) constituyen un elemento clave de nuestro modelo educativo. Muchos han sido los esfuerzos por implantar un modelo educativo que tuviera presente el uso de estas herramientas, tanto en el aula como fuera de ella.

La Consejería de Desarrollo Educativo y Formación Profesional ha dado en los últimos años un paso decisivo en metodología educativa y formación del profesorado antes de integrar múltiple equipamiento TIC en nuestros centros.

Pero en este ascenso hacia la enseñanza digital no nos podemos olvidar de garantizar la salud física, mental y emocional de nuestro alumnado en su interacción con la red y los dispositivos electrónicos. Por ello, se han realizado distintas iniciativas que han permitido recopilar suficiente documentación que se concreta en esta Guía para el uso responsable y educativo de las TIC. Se pretende que esta guía sea un documento vivo que se actualice con suficiente periodicidad en función de los constantes cambios que las tecnologías de la comunicación nos ofrecen, así como las novedades en materia informativa, formativa y normativa que se vaya publicando.

Esta Guía es un instrumento de referencia práctico, dirigido a padres, madres, alumnos, profesionales de la enseñanza y, en general, a cualquier persona relacionada con la educación. Trata de centrarse tanto en las repercusiones positivas como negativas del uso de las TIC y establece algunas recomendaciones para un uso autónomo, pero a la vez responsable, de las mismas. Pretende, también, prevenir conflictos a corto o largo plazo, así como indicar determinadas actuaciones que deben tenerse en cuenta cuando el problema ya se ha desarrollado.

Se ofrece una síntesis organizada de la abundante información dispersa en la web y en la bibliografía especializada.

2. PRINCIPIOS SOBRE EL BUEN USO DE LAS TIC.

ALUMNADO

Los alumnos y alumnas deben saber y tener presentes los siguientes principios:

- A. Controlar el tiempo que se conectan, ya sea al ordenador, a la tablet, al móvil o a cualquier otro dispositivo similar.
- B. Cuidar su correcta posición corporal al usar cualquiera de estos dispositivos, sentándose correctamente.
- C. Ser prudentes y no concertar encuentros con personas que no conocen y que les proponen quedar a solas.
- D. Tener respeto a otros usuarios, evitando las burlas, difamaciones, humillaciones y agresiones.
- E. No suplantar la identidad de nadie en la red.**
- F. Aprender a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.**
- G. Saber que tienen derecho a la privacidad de su información personal y a que no sea difundida sin su consentimiento por la red. Hay que tener cuidado con los datos que se comparten tanto en chat, redes sociales o por email (imágenes, datos, perfiles, números de teléfono...), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.**
- H. De la misma manera, entender que no se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.**
- I. Saber que tienen el deber de pedir ayuda a una persona mayor cuando algo no les guste o lo consideren peligroso para chicos o chicas de su edad, incluso si no les afecta personalmente, para ver conjuntamente con el adulto si hay que denunciarlo a las autoridades competentes.
- J. Cuidar el mantenimiento de los dispositivos que utilizan, evitando golpearlos, exponerlos a contacto con líquidos, usarlos bruscamente o con fuerza inapropiada.

FAMILIA

Es muy importante la contribución de las familias en los siguientes principios:

- A. Estar al día en todo lo relativo a internet y nuevas tecnologías, ya que cuanto más información se tenga sobre estas realidades mejor podrán ayudar y acompañar a sus hijos o hijas en el buen uso de ellas.
- B. Acordar unas normas de uso claras, estableciendo y haciendo cumplir un horario. Es importante que los menores tengan claro lo que pueden y no pueden hacer y sepan sus consecuencias. Se debe marcar un tiempo para tareas escolares y un tiempo para el ocio.

- C. Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las webs tienen la misma credibilidad, que es importante filtrar y evaluar su calidad.
- D. Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”, de modo que sus tareas no se conviertan en plagios de trabajos ya realizados.
- E. Fomentar el diálogo sobre hábitos de utilización de las TIC y sus riesgos. Es importante que el menor sienta que cuando le suceda algo extraño o le incomode, puede decírselo a sus padres sin sentirse culpable.
- F. Utilizar filtros de control de acceso a la red y programas de control parental, con los que se evitará que los menores accedan a páginas de contenido inapropiado y proporcionarán herramientas de regulación del tiempo de uso de los dispositivos digitales.
- G. Tener el ordenador en una zona de uso común, ya que facilitará tanto la supervisión del tiempo de utilización como las situaciones que puedan resultar incómodas para el menor, así como la revisión de las webs que visita, por ejemplo, consultando el historial de navegación. Buscar una ubicación en la que la luz sea la adecuada, evitando reflejos.
- H. Cuidar la postura respecto al ordenador, que debe seguir estas pautas:
 - Los ojos deben estar situados enfrente, y a una distancia mínima del doble de la diagonal de la pantalla.
 - La espalda recta, y reposada la zona lumbar contra el respaldo de la silla.
 - El ángulo de rodillas y codo ha de ser de 90°.
 - Es conveniente acostumbrar al menor a levantar la vista de la pantalla cada 15 o 20 minutos, fijándola en un punto alejado, y a no permanecer en la misma postura durante más de una hora.
- I. Enseñarles en qué consiste la privacidad, que los datos personales son información sensible y que pueden ser utilizados en su contra.
- J. Advertir del derecho a la privacidad de la información personal del alumnado y a que no sea difundida sin su consentimiento por la red. Hay que tener cuidado con los datos que se comparten tanto en chat, redes sociales o por email (imágenes, datos, perfiles, números de teléfonos.), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.
- K. Explicarles que en las redes hay que respetar a los demás, que detrás de cada apodo hay una persona y que siempre hay que ser educado.
- L. Cuidar el ordenador, tablet, smartphone..., evitando riesgos físicos, manteniéndolos limpios y evitando que sufran golpes o exposiciones a calor.

PROFESIONALES DE LA ENSEÑANZA

- A. Controlar el tiempo que se conectan a internet en clase.
- B. Colaborar en el mantenimiento de todos los dispositivos tecnológicos del aula.
- C. Fomentar la utilización de una posición correcta para el cuerpo frente al ordenador, siguiendo estas pautas:

- Los ojos deben estar situados enfrente, y a una distancia mínima del doble de la diagonal de la pantalla.
 - La espalda recta, y reposada la zona lumbar contra el respaldo de la silla.
 - El ángulo de rodillas y codo ha de ser de 90°.
 - Es conveniente acostumbrar al menor a levantar la vista de la pantalla cada 15 o 20 minutos, fijándola en un punto alejado, y a no permanecer en la misma postura durante más de una hora.
- D. Fomentar el respeto a otros usuarios, evitando las burlas, difamaciones y agresiones.
- E. Enseñar a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.
- F. Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las webs tienen la misma credibilidad, que es importante filtrar y evaluar su calidad.
- G. Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”, para evitar plagios de trabajos ya realizados.
- H. Advertir del derecho a la privacidad de la información personal del alumnado y a que no sea difundida sin su consentimiento por la red. Hay que tener cuidado con los datos que se comparten tanto en chat, redes sociales o por email (imágenes, datos, perfiles, números de teléfonos.), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.
- I. De la misma manera, explicar que no se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.

3. PRÁCTICAS PARA USO RESPONSABLE DE LAS TIC.

A continuación, se ofrecen algunas buenas prácticas para el uso responsable y seguro de internet en los colegios con el fin de ayudar a que los alumnos utilicen internet sin asumir riesgos innecesarios.

1. Mantener actualizados los equipos del colegio

Una forma de evitar amenazas es mantener actualizados los sistemas operativos y las aplicaciones instaladas en dispositivos windows. Esta cuestión debe ser autorizada por la dirección del centro o la coordinación TDE. Hay que ser precavidos porque existen webs que simulan ofrecer programas populares, pero en realidad son versiones con algún tipo de malware o código malicioso que se activa cuando el usuario lo instala en su equipo. Por ello, es recomendable que en los dispositivos bajo Windows se lleven a cabo las descargas de aplicaciones siempre de web oficiales y utilizar antivirus para proteger los dispositivos del centro de posibles amenazas.

En el caso de los dispositivos portátiles “educaandos o chromebooks”, facilitados por la Consejería de Educación, no es necesario realizar ninguna operación, ya que se actualizan automáticamente y poseen aplicaciones preinstaladas en el caso de los primeros.

2. Aprender a tener un horario de uso de internet

Internet ha cambiado la forma en la que aprenden los niños y muchos proyectos educativos innovadores aprovechan los avances tecnológicos y de la Red. Los alumnos necesitan tener un

horario de uso de internet en el colegio, puesto que no es lo mismo utilizar la red para aprender, programar o investigar información que distraerse en las redes sociales o con algún juego.

Se fomentará el uso de internet como herramienta complementaria y de uso progresivo en función de los niveles educativos.

Asimismo, todos los ordenadores tienen que estar situados en un sitio visible y con contraseñas de acceso para que los adultos puedan comprobar que los menores cumplen con las normas que hemos establecido previamente.

3. No facilitar datos personales a desconocidos

Muchas webs suelen llamar la atención con concursos, ofertas o anuncios con el objetivo de conseguir datos personales de los usuarios (nombre y apellidos, dirección, correo electrónico o teléfono) mediante formularios o acceso con redes sociales. Tenemos que enseñar a los alumnos a no proporcionar datos personales a webs desconocidas para evitar el uso fraudulento de sus datos o que sean víctimas de situaciones de acoso.

Es fundamental que los estudiantes conozcan los riesgos de aceptar invitaciones de desconocidos o de publicar información comprometida. Una vez que compartimos algo en internet su difusión es muy rápida y eliminar el contenido por completo puede resultar muy difícil. Las cuentas en redes sociales solo deben ser visibles para sus amigos, nunca para “los amigos de tus amigos” ni, por supuesto, abiertas a todo el público.

4. Asegurar las cuentas en los dispositivos y en las redes sociales

Es imprescindible enseñarles a utilizar una contraseña para proteger el ordenador o el dispositivo desde el que acceden a internet, bloquearlo en los descansos y cerrar las cuentas de correo, nubes y demás entornos con usuario y contraseña al finalizar las sesiones. Las contraseñas que utilicen tienen que ser complejas (no muy utilizadas por otros usuarios), con una longitud de al menos 8 caracteres y resultado de una combinación de letras y números.

Según la guía de uso responsable del INCIBE (Instituto Nacional de Ciberseguridad), una buena práctica es usar reglas nemotécnicas como las iniciales de una frase, expresión o título de canción, película...

Ejemplo: “En un lugar de la Mancha” >> EuldIM, se puede añadir un carácter especial y si la usamos para varias aplicaciones, por ejemplo, correo electrónico >>> EuldIM#2mail

5. Enseñar un uso responsable del correo electrónico

El correo electrónico es una de las herramientas más útiles y utilizadas por los adultos como una forma de comunicación. Por este motivo, hay que tener especial precaución y enseñar a los alumnos a emplear el correo de forma responsable.

Una práctica común es tener una dirección de correo electrónico para comunicarse con familiares y amigos y otra dirección para darse de alta en las redes sociales y otras páginas como foros o juegos. De esta forma es más fácil identificar correos no deseados (spam) o que contengan virus.

En el caso del alumnado de primaria, especialmente en segundo y tercer ciclo, disponen de cuentas de Google educativas oficiales, proporcionadas por la Consejería de Educación, del tipo xxxxxx@g.educaand.es. Dichas cuentas tienen como usuario y contraseña el usuario de Pasen del alumnado. El alumnado y sus familias como responsables, deben custodiar privadamente dichas credenciales de acceso.

6. Hablar con claridad sobre los contenidos de la Red

En internet, dado que toda la información está a un golpe de clic, los niños y adolescentes pueden tener acceso a contenidos violentos, imágenes desagradables o lenguaje obsceno. Se han diseñado numerosos programas para vigilar la actividad en internet de los alumnos y filtrar los contenidos a los que acceden, pero muchas veces las herramientas no son tan efectivas como sería deseable.

Para evitar estos contenidos lo mejor es hablar regularmente con los niños de su actividad en Internet y las consecuencias que pueden tener el mal uso de internet, tanto para ellos mismos y su imagen como para los dispositivos.

Aprender a no hacer clic en enlaces sospechosos previene el acceso a páginas web con amenazas capaces de infectar los dispositivos. Los enlaces sospechosos podemos encontrarlos un mensaje de un foro, en un correo electrónico o incluso en los primeros resultados de Google. Lo importante es analizar si son ofrecidos en alguna situación sospechosa, provienen de un remitente desconocido o remiten a una web poco confiable.

Una buena medida puede ser la supervisión del historial de navegación de los menores por parte de los adultos.

7. Informar sobre los derechos de propiedad intelectual.

Cada vez es más frecuente que los profesores pidamos trabajos a nuestros alumnos que requieran buscar información en internet. Los estudiantes deben tener formación sobre los derechos de propiedad intelectual y saber que no se pueden utilizar libremente imágenes, textos u otros contenidos con derechos reservados sin citar la fuente.

8. Normas de uso de las tecnologías en el centro

- El uso de los dispositivos móviles (smartphone) en los centros lo regula la Instrucción 4 de diciembre de 2023 de la Viceconsejería de Desarrollo Educativo y Formación Profesional. Al mismo tiempo el Reglamento de Organización y Funcionamiento y el Plan de Convivencia del colegio establecen las condiciones de uso de los dispositivos en horario lectivo, complementario y extraescolar, así como las correcciones en caso de incumplimiento.
- Los recursos informáticos tienen como "finalidad servir de apoyo a la docencia" y por tanto deben emplearse para el trabajo y el estudio, no con otros fines. La dirección del centro tomará las medidas oportunas ante eventos o actividades especiales con la oportuna comunicación a las familias y en su caso previa la oportuna justificación por escrito.
- El centro promoverá el uso de herramientas para aplicaciones o espacios de uso educativo, en el caso de necesitar registro por parte de los/as alumnos/as, se comunicará previamente a los tutores legales para que lo realicen con las credenciales de la Google Suite educativa: xxxx@q.educaand.es.
- Debemos ser responsables y cuidadosos/as con los dispositivos que se tienen en el centro, tanto el profesorado como el alumnado y, por tanto, no se modificarán los programas existentes. Si hubiera que hacerlo o instalar nuevas aplicaciones, programas... debe ser consultado a la figura de la coordinación TDE. Ver punto 4 de este documento.

- El profesorado del centro informará a los alumnos y alumnas sobre el uso adecuado de las herramientas o apps usadas.
- Sólo se podrán utilizar dispositivos autorizados por el centro.
- El profesorado del centro supervisará las actividades que precisan el uso de Internet.
- Respecto a la seguridad: no se debe compartir con nadie ningún dato: contraseñas, claves, acceso.
- Aunque no se puede garantizar que los/as alumnos/as no vayan a encontrar algún contenido inapropiado en la web, el centro analizará las páginas web, herramientas o apps utilizadas para la docencia, minimizando este riesgo en lo posible.
- El centro proporcionará formación sobre los peligros de la red, cómo evitarlos y promover un uso seguro de las TIC (Tecnologías de la Información y Comunicación) y las TAC (Tecnologías del Aprendizaje y Conocimiento).
- El centro podrá comprobar los archivos guardados, descargados, historial del navegador web y cualquier otro elemento como resultado del uso de Internet.
- Cualquier persona de la comunidad educativa que encuentre material inapropiado en los dispositivos del centro, o durante una actividad, deberá comunicarlo inmediatamente para corregirlo.
- El centro pedirá autorización a las familias para la publicación, con fines educativos, de imágenes de los estudiantes. Esto se realizará de forma general, al formalizar la matrícula de cada curso y de forma específica para aquellas actividades singulares que lo precisen.
- El centro no se responsabiliza de los materiales compartidos por terceros, ni del contenido accesible desde los vínculos que divulguen.
- Con objeto de respetar el buen uso de las redes, el centro educativo se reserva el derecho de eliminar cualquier aportación que contravenga los principios aquí expuestos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales en su artículo 7, establece que la edad para otorgar consentimiento en la utilización de los datos personales se establece en **14 años**. Para los menores de esta edad el otorgamiento (responsabilidad) recae en los tutores legales.

- Los alumnos y alumnas no pueden sacar fotos ni videos de otros alumnos o alumnas ni del personal docente o no docente, ni hacerlos circular, publicarlos o difundirlos por ningún medio a no ser que cuente con el permiso de la persona (mayores de edad) o de los tutores legales (menores). Esta cuestión es extensible a toda la jornada escolar, lectiva, complementaria y extraescolar.
- Familias, alumnos/as y trabajadores/as del centro harán uso de las redes sociales teniendo en cuenta la normativa de convivencia del centro. Siempre publicando y comentado en ellas con máximo respeto y cuidado hacia todas las personas que integran la comunidad educativa.
- Tanto los/as alumnos/as como trabajadores/as y familias tienen la responsabilidad de poner en conocimiento de la dirección del centro cualquier publicación que observen en las redes sociales que pueda perjudicar la imagen del centro o la de las personas que lo integran.
- Además de utilizar los canales oficiales de comunicación, el equipo directivo y profesorado que coordine los planes y programas oficiales del centro podrán hacer uso de la web y las

redes sociales oficialmente establecidas como medio para difundir sus actividades habituales.

- Mediante el uso de cuentas de Office 365 o Google Suite (xxx@G.educaand.es) se facilitará al profesorado acceso a espacios privados y compartidos documentos (carpetas de contenidos, documentos, calendarios, videos, infografías...) que faciliten su formación y trabajo diario.
- Tanto las imágenes como la música que se publiquen en las redes sociales del centro cumplirán la normativa respecto a los derechos de autor.
- Se animará a participar en el uso responsable de las tecnologías educativas a los trabajadores o alumnado de nueva incorporación planificando actividades que potencien su uso para reducir en la medida de lo posible la brecha digital.
- No se permitirá la participación del alumnado en chats o espacios de características similares, excepto cuando se trate de una actividad de contenido educativo que cuente con la aprobación de un docente.

COMUNICACIONES

Comunicaciones del profesorado con el alumnado: podrá usarse el correo de gmail de las cuentas educativas de Google Suite. Para ello al principio de cada curso escolar el/la tutor/a del aula facilitará al alumnado y sus familias las credenciales de acceso para el seguimiento y supervisión por parte de los tutores legales.

El alumnado podrá comunicaciones entre sí mediante dicho correo electrónico exclusivamente con fines educativos.

El centro proporcionará al alumnado un conjunto de normas de conducta, protección y autoprotección para tener unas comunicaciones efectivas y seguras en la red.

Los estudiantes podrán en práctica las siguientes normas:

- Mostrar respeto por uno mismo y todas las personas de la comunidad escolar.
- Proteger la propia identidad y la de otras personas.
- Respetar y proteger la propiedad intelectual.

Se podrán emplear servicios en la nube para organizar los documentos y o entregar las actividades, como Google Drive

Cualquier persona de la comunidad educativa que se percate de un uso inadecuado de las comunicaciones deberá comunicarlo inmediatamente para tomar las medidas oportunas.

4. NORMAS DE USO DE LOS DISPOSITIVOS PORTÁTILES DEL CENTRO

Para el alumnado será de aplicación lo dispuesto en los puntos anteriores de esta guía además de los acuerdos y normas establecidas por el profesorado sobre el uso de los dispositivos portátiles, la protección de datos personales y la guarda y custodia de credenciales de acceso. Así mismo, se atenderá a lo dispuesto en el Plan de Convivencia del Centro y al punto 5 de la presente guía.

En el anexo de esta guía se incluye el compromiso para la firma de los tutores legales sobre el uso excepcional de teléfonos móviles en el viaje de estudios. Dicho uso será voluntario y previa solicitud.

En cuanto al profesorado y personal no docente se tendrá en cuenta la “Guía de protección de datos y uso de las TIC”, elaborada por la red TDE_Almería, basada en los materiales publicados por la Agencia Española de Protección de datos y en la Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía. Esta guía para el profesorado se incluye como **anexo** al presente documento.

ORGANIZACIÓN DE LOS DISPOSITIVOS PORTÁTILES DEL CENTRO

Los ordenadores portátiles recibidos de la Consejería de la Consejería de Desarrollo Educativo y Formación profesional actualmente se estructuran en los siguientes grupos:

- A. Portátiles para el uso del profesorado: 40 unidades.
 - B. Portátiles para el uso del alumnado en el aula y/o préstamo para alumnado en riesgo de brecha digital: 50 unidades
 - C. Chromebooks para el trabajo con el alumnado del tercer ciclo de primaria: 50 unidades
-
- Dispositivo tipo A: Este material estará custodiado en el almacén principal del centro. Cada inicio de curso la dirección del centro distribuirá dichos dispositivos según los criterios acordados: equipo directivo, tutores/as, coordinación TDE, responsables de planes y programas, especialistas ordenados por antigüedad y/o necesidad de uso. Para la recogida de este material se firmará el documento de préstamo al profesorado recogido en el ROF y anexo a la presente guía.
 - Dispositivo tipo B: Este material será de uso del alumnado, se contemplan dos opciones, por un lado para préstamo en el hogar para el alumnado con brecha digital. A tal fin la dirección del centro requerirá a las tutorías un listado justificado con los casos que pudieran existir, para ello se seguirá el procedimiento recogido en el ROF y las familias en el acto de entrega firmarán un doble documento de recogida y compromiso, dicho documento se presenta como anexo a esta guía.
Por otro lado, el resto de dispositivo no prestado a los hogares se distribuirá para uso de las diferentes unidades y ciclos educativos por orden de prioridad. En el cuadro indicaco más abajo se refleja dicha distribución.
 - Dispositivo tipo C: Estos dispositivos se dotan para uso del alumnado del tercer ciclo de primaria. Para ello, se dispondrá de 30 aparatos en uno de los muebles de carga del tercer ciclo.

Organización de dispositivo por muebles de carga y/o unidades/ciclos:

Actualmente el centro cuenta con 5 armarios de carga para ordenadores portátiles distribuidos según el siguiente cuadro:

Ciclo educativo	Planta	Dependencia	Uso	Dispositivos
Orientación y apoyo	Baja	Aulas de PT	alumnado	2
Orientación y apoyo	Baja	Aula de AL	alumnado	1
Conserjería	Princip	Conserjería	música	1
Biblioteca	Princip	Biblioteca	alumnado	1
Esp. Música	Princip	Aula música	Prof/alumnado	1
Esp. EF	2	5ºC	Prof	1
Ciclo 1 Armario	Baja	Aula peq grupo1	alumnado	8
Ciclo 2 Armario	1ª	Aula de apoyo	Alumnado	13
Ciclo 3 Armario 1	2ª	Aula de apoyo	Desuso	Ultraportátiles y tablets
Ciclo 3 Armario 2	2ª	Aula de apoyo	Alumnado	13 Portátiles
Ciclo 3 Armario 3	2ª	Aula de apoyo	Alumnado	30 Chromebook

Uso y carga de dispositivos por planta y custodia de llaves de armarios:

Al inicio de curso, una vez nombradas las coordinaciones de cada ciclo educativo, en las primeras semanas de curso, se establecerá el horario de uso de los dispositivos, especialmente para el tercer ciclo de primaria.

La custodia de llaves de dichos armarios la ostentará la coordinación de cada ciclo educativo, debiendo ubicarse en un lugar del aula del coordinador/a, conocido por todos los profesores de dicho ciclo. La dirección del centro y la coordinación TDE dispondrán de una copia de cada uno de los armarios.

En cuanto a la carga de los aparatos, en cada planta existe un armario con carga programada nocturna, por lo que si se conectan adecuadamente tras su uso los dispositivos deben estar en perfecta carga. En caso de detectar alguna anomalía deberá comunicarse a la coordinación TDE. En el ciclo 3 se disponen de dos armarios, uno en desuso y el otro que debe conectarse a la corriente con frecuencia oportuna para disponer de aparatos en carga.

*** Aunque el alumnado del tercer ciclo puede colaborar en la recogida y entrega de dispositivos en sus armarios de carga, dicha actuación debe ser supervisada y comprobada su eficacia por el profesorado que en dicha actuación disponga de la docencia con el nivel educativo en cuestión.*

5. CONDUCTAS CONTRA LA CONVIVENCIA EN EL USO DE LAS TECNOLOGÍAS.

El mal uso de Internet o incumplimiento de la normativa puede conllevar sanciones e incluso la retirada del acceso a Internet de forma temporal o definitiva.

El centro podrá informar a las autoridades competentes de cualquier actividad ilegal detectada o situaciones que afecten a la integridad

Conductas contrarias a la convivencia:

- Mal uso del dispositivo por descuido no intencionado y sin rotura del mismo: Amonestación verbal y comunicación a la dirección del centro.

- Mal uso del dispositivo por descuido no intencionado con rotura del mismo: Los tutores legales correrán con los gastos de reparación.
- Realizar actividades, acceso a aplicaciones o webs no indicadas en ese momento por el profesorado: Amonestación verbal y comunicación a la dirección del centro.

Conductas gravemente perjudiciales para la convivencia:

- Utilizar el dispositivo para realizar fotografías/vídeos/audios sin el consentimiento del afectado.
- Reiteración de las conductas contrarias anteriormente descritas.
- Acceder a páginas no apropiadas.
- Uso del dispositivo cuando no lo ha autorizado el docente.
- Acceso a redes sociales sin autorización del docente.
- Acceso a aplicaciones no autorizadas por el docente.

La dirección del centro aplicará las correcciones oportunas recogidas en el Plan de Convivencia del centro, pudiendo encontrarse entre las mismas la realización futura de actividades académicas similares que no requieran el uso de dispositivos portátiles.

6. DETECCIÓN DE CONDUCTAS DE POSIBLE ACOSO EN LA RED.

Definición de acoso en red: Conducta hostil de uno o varios hacia otra persona, de forma sistemática, afectando a todos los niveles de la vida del acosado e incluso a su círculo más próximo. Se produce cuando hay un desequilibrio de poder entre acosador y acosado.

Tipos de ciberacoso:

- cyberbullying: acoso entre alumnos/as
- cyberbaiting: acoso de alumnos a un profesor/a
- grooming: acoso de un adulto a un menor

El profesorado y las familias, pilares fundamentales por ser los más próximos al alumnado, mantendrán una actitud dialogante, de empatía con los/as alumnos/as y de reproche hacia el ciberacoso. De tal modo que se favorezca la denuncia temprana de estas situaciones.

Se realizarán acciones tutoriales con el alumnado implicado y las familias de forma independiente y no conjunta.

A través de acciones como el “Plan Director” el centro podrá colaborar con la Guardia Civil para realizar formaciones de prevención del ciberacoso y el uso seguro de las tecnologías de la información, incluido las redes sociales. Esta formación se enfoca hacia las familias, a través de la AMPA del centro, y directamente al alumnado, especialmente del tercer ciclo de primaria.

En caso de que el centro tenga información sobre un caso grave de posible ciberacoso, se podrá informar a las autoridades competentes para recabar ayuda en su tratamiento y tomar las medidas oportunas.

CONTACTO DE INSTITUCIONES PARA LA AYUDA

Listado de las instituciones públicas y privadas que gestionan las peticiones de ayuda en caso de ciberacoso:

- Instituto Nacional de Ciberseguridad de España (INCIBE): <https://www.incibe.es/>
- Fundación ANAR Tfno. 900-20-20-10
- AlertCops App
- Tú decides en Internet Tfno. 901-23-31-44. Correo: canaljuven@agpd.es Whatsapp 616-172-204
- Guardia Civil. Tlf: 062. Correo: colabora@guardiacivil.org

Grupo de delitos telemáticos <https://www.guardiacivil.es/es/servicios/denuncias/index.html>

- Policía Nacional. Brigada de investigación tecnológica (UIT) <https://www.policia.es/es/denuncias.php#>

7. BIBLIOGRAFÍA Y DOCUMENTOS DE REFERENCIA.

- Marco Común de Competencia Digital Docente INTEF. Ministerio de Educación Cultura y Deporte
- Seguridad y uso responsable de las TIC. Guía para centros educativos.
- Tú decides en Internet <http://www.tudecideseninternet.es>, perteneciente a la AEPD
- Guíales en Internet <http://www.tudecideseninternet.es/agpd1/images/guias/guia-formadores.compressed.pdf>
- Enséñales a ser legales en Internet. http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf
- No te enredes en Internet <http://www.tudecideseninternet.es/agpd1/images/guias/guia-menor.compressed.pdf> y Sé legal en Internet http://www.tudecideseninternet.es/agpd1/images/guias/Guia_menores2016.pdf
- Instituto Nacional de Ciberseguridad de España (INCIBE). Guía de privacidad y seguridad en Internet http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Privacidad_y_Seguridad_en_Internet.pdf
- Guía "Privacidad y seguridad en i

- Agencia Española de Protección de Datos: Guía para Centros Educativos.

- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.

- Red TDE Almería: Guía para la protección de datos en el ámbito educativo y uso responsable de las TIC para los profesionales de la Junta de Andalucía.

ANEXOS

Protección de Datos en el Ámbito educativo

Uso de las TIC para profesionales públicos de la Junta de Andalucía.



Junta de Andalucía

Delegación Territorial de Desarrollo Educativo y FP en Almería

Normativa

Normativa



EL RGPD

(Reglamento General de Protección de Datos)

2016



La LOPDGDD

(Ley Orgánica de Protección de Datos y
Garantía de Derechos Digitales)

2018

Última actualización

09/05/2023

Conceptos Clave

Conceptos clave

Datos de carácter personal

Dato Genético

Dato Biométrico

Datos especialmente sensibles

Responsable y encargado del tratamiento de datos

Persona Delegada del tratamiento de datos

Tratamiento de datos

Toda información sobre una persona física identificada o identificable.

**Datos de
carácter
personal**

El nombre y apellidos del alumnado, de sus familiares, su dirección, número de teléfono o su correo electrónico, imágenes o, por ejemplo, la profesión los estudios o el lugar donde trabajan los familiares, o su número de cuenta bancaria.



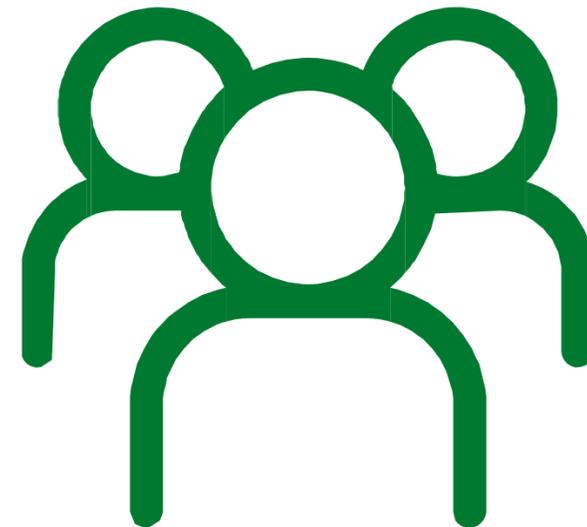
Persona dentificable

Persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

DE QUIÉN SON LOS DATOS DE CARÁCTER PERSONAL

**Datos de
carácter
personal**

De la persona física titular de los datos: alumnado, familias, profesorado o personal de administración y servicios.



Dato Genético

Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.



Dato Biométrico

Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.



**Datos
especialmente
sencibles**

Circunstancias o información de las personas sobre su esfera más íntima y personal.

- Ideología,
- Afiliación sindical,
- Religión y creencias
- Origen racial, a la salud y a la vida sexual
- Sobre la comisión de infracciones penales o administrativas
- Datos biométricos y genéticos



RESPONSABLE

La persona física o jurídica pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal

**Responsable y
encargado del
tratamiento de
datos**

Centros Públicos

Consejería de la Comunidad Autónoma competente en materia educativa, salvo para los centros de Ceuta y Melilla o los centros en el exterior titularidad del estado dependientes del Ministerio de Educación

Centros Privados/Concertados

Los propios centros.

ENCARGADO

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento



Las empresas que sean contratadas por el centro o la Administración educativa para prestar los servicios de comedor, servicio médico, transporte escolar o el de seguridad tienen la consideración de encargados del tratamiento de datos personales.

El equipo directivo del centro, los profesores, o el personal de administración y servicios del centro educativo no son encargados del tratamiento.



**Persona
Delegada del
tratamiento
de datos**

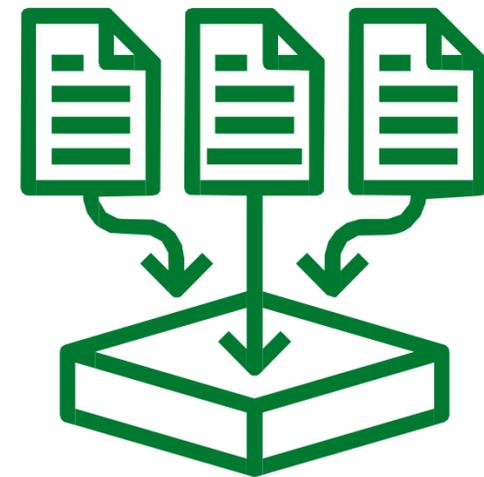
art. 34.1. b) LOPD GDD establece que deberán designar esta figura “los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas”.

Regulación de las funciones del delegado de protección de datos

Artículo 39 RGPD. Funciones del delegado de protección de datos

Tratamiento de datos

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un **tratamiento de datos**, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.



Derechos / Cautelas



Tratamiento de datos

- El derecho de **ACCESO** permite a los titulares de los datos personales conocer y obtener gratuitamente información sobre si sus datos de carácter personal están siendo objeto de tratamiento, con qué finalidad, qué tipo de datos tiene el responsable del tratamiento, su origen, si no proceden de los interesados, y los destinatarios de los datos.
- El derecho de **RECTIFICACIÓN** permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.
- El derecho de **SUPRESIÓN** permite que se supriman los datos que resulten ser inadecuados o excesivos. La revocación del consentimiento da lugar a la cancelación de los datos cuando su tratamiento esté basado en él, pero sin efecto retroactivo.
- El derecho de **OPOSICIÓN** es el derecho del interesado a que, por motivos relacionados con su situación personal, no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.
- El derecho de **LIMITACIÓN AL TRATAMIENTO** es el “marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro” según las condiciones establecidas en el artículo 18 del RGPD.
- El derecho de **PORTABILIDAD**, el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.



Tratamiento de datos



El profesorado y resto del personal que acceda a los datos personales del alumnado o de sus familias está sometido al deber de guardar **secreto.**

(art. 5 LOPDGDD.)

Todas las personas que presten sus servicios en los centros y Administraciones educativas docentes, personal administrativo o de servicios auxiliares, en relación con los datos de carácter personal a los que accedan, incluso una vez finaliza la relación con el responsable o con el encargado de tratamiento.

En la práctica

¿Puede el profesorado recoger datos personales directamente del alumnado?

Solo pueden recabar:

- Datos de carácter personal, como grabaciones de imágenes o sonido con la finalidad de **evaluar** sus conocimientos u otros datos relacionados con la realización de dichos ejercicios, o los resultados de su evaluación.
- Datos del alumnado y de sus familias para el desempeño de la **función docente y orientadora**.



A tener en cuenta.

- Como medio de acreditación de la identidad del/la estudiante, contenido o del ejercicio realizado..
- Garantizar el derecho de revisión o reclamación.
- Se conservará durante el periodo imprescindible.

Publicación de contenido audiovisual por los CENTROS

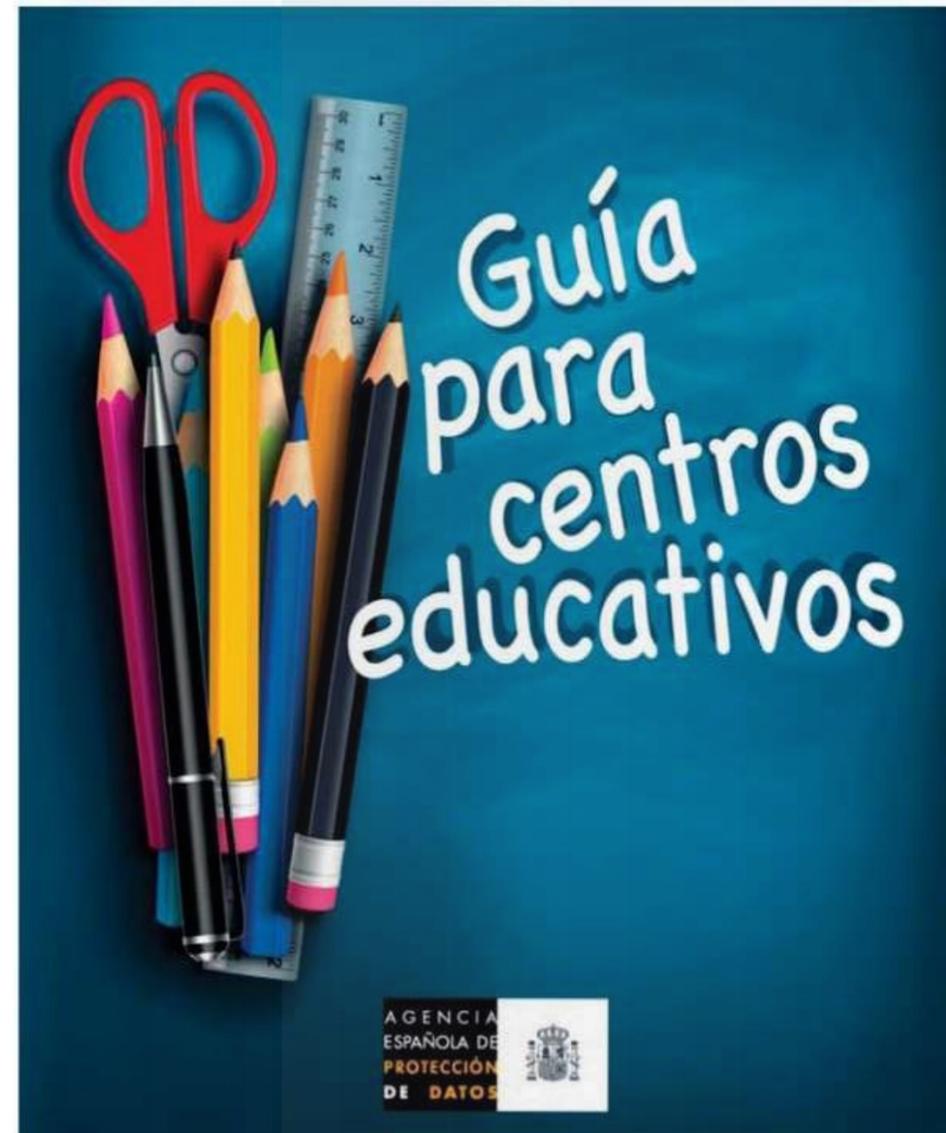
- Rellenar y mantener actualizado en Séneca el formulario que a tal efecto está disponible:

(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 o alumna menor de 14 años, se debe informar y recabar el consentimiento de sus padres o tutores.



Preguntas y respuestas



[Acceso al documento](#)

Ejemplos



¿Se pueden hacer públicas las calificaciones escolares?

Las calificaciones de los alumnos se han de facilitar a los propios alumnos y a sus padres.

En el caso de comunicar las calificaciones a través de plataformas educativas, éstas sólo deberán estar accesibles para los propios alumnos, sus padres o tutores, sin que puedan tener acceso a las mismas personas distintas.

No obstante, sí sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, mostrando su calificación frente a la media de sus compañeros.



¿Pueden los profesores facilitar las calificaciones oralmente en clase?

Como se ha indicado, no existe una regulación respecto de la forma de comunicar las calificaciones. Aunque sería preferible que las calificaciones se notificasen en la forma indicada en el punto anterior, sería posible enunciarlas oralmente, evitando comentarios adicionales que pudieran afectar personalmente al alumno.

Ejemplos



¿Puede publicarse en la web del centro información relativa a los alumnos, como fotografías o vídeos?

Sí, siempre que se disponga del consentimiento de los alumnos o de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los alumnos, por ejemplo, pixelando las imágenes.



¿Y un profesor puede publicar en su blog las actas del departamento o los exámenes de los alumnos o sus fotografías?

El blog de un profesor es un medio de información y comunicación al margen de la función docente que desarrolla en los centros educativos. De su contenido será responsable el profesor que deberá observar la normativa de protección de datos en cuanto que incluya información de carácter personal.

Por tanto, salvo que se contase con el consentimiento de los afectados, o de sus padres o tutores, no se podrían publicar en el blog de un profesor datos de carácter personal que permitan identificar a los alumnos.

Al igual que con los blogs de los centros educativos, se podría publicar la información previa disociación o anonimización de los datos de los alumnos de manera que no se les pudiese llegar a identificar.

Código de conducta uso TIC

Normativa



Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.

Cumplimiento - Principios de uso

“ Los profesionales están obligados al conocimiento y cumplimiento del presente Código de Conducta en cualquier modalidad de prestación de servicios, tanto presencial como de teletrabajo.”

Los profesionales deberán respetar los siguientes principios:

- Servicio y proximidad a la ciudadanía.
- Responsabilidad, profesionalidad y cualificación profesional.
- Seguridad.
- **Protección de datos personales**, tanto de la ciudadanía como de los profesionales.
- Eficacia en el desempeño de las funciones y eficiencia en la utilización de los recursos públicos.
- Accesibilidad de las tecnologías y contenidos, especialmente en la relación con la ciudadanía.

Uso del equipamiento TIC del puesto de trabajo.

Los profesionales:

- Utilizarán para el desempeño de sus funciones el equipamiento TIC y las redes de comunicación cuyo acceso les haya sido facilitado.
- La puesta a disposición del equipamiento TIC **no implica cesión de su propiedad**, sino exclusivamente cesión de su uso.
- Realizarán un uso del equipamiento TIC **compatible con el desempeño de sus funciones**.
- **No permitirán ni facilitarán el uso del equipamiento TIC a terceros** que no estén debidamente autorizados.
- **Cuidarán y conservarán en buen estado** el equipamiento TIC.
- **No alterarán el equipamiento TIC ni realizarán reparaciones ni actuaciones técnicas** de mantenimiento o mejora del mismo.
- **No alterarán el software** que esté instalado en el equipamiento TIC ni instalarán nuevo software, aunque éste sea de libre uso o gratuito.
- Seguirán los protocolos y mecanismos establecidos en su Consejería o Agencia para incidencias, solicitudes de dispositivos, permisos, equipamiento TIC y software.
- Utilizarán los mecanismos de bloqueo que se hayan establecido en caso de desatención temporal del equipamiento TIC.

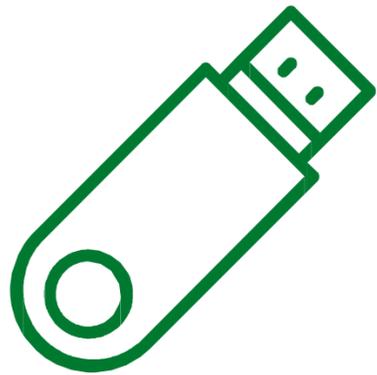


Uso de aplicaciones y sistemas



- Utilizarán exclusivamente las aplicaciones y sistemas que para el desempeño de sus funciones les haya habilitado la Administración de la Junta de Andalucía. Estas aplicaciones y sistemas podrán pertenecer a otras Administraciones Públicas u otras entidades.
- Atenderán a las guías, instrucciones y manuales establecidos para el uso de las aplicaciones y sistemas.
- Atenderán a los protocolos y mecanismos establecidos para gestionar incidencias y solicitudes de permisos.
- Deberán cerrar las sesiones al finalizar el uso de la aplicación. Se recomienda utilizar las funcionalidades dispuestas para ello en la misma («desconexión», «cerrar sesión», «salir» o similar) y no simplemente «cerrando» la ventana de trabajo.

Almacenamiento y formato de la información



- Almacenarán la información que precisen o generen en el desempeño de sus funciones en los sistemas de información, en las herramientas corporativas [...], de modo que esté disponible para todas las personas que pudieran necesitarla, [...].
- Con carácter general, evitarán almacenar información en dispositivos de almacenamiento extraíble (discos duros portátiles, memorias USB, etc). El uso admisible de estos dispositivos es exclusivamente el de instrumento de transporte de ficheros aplicando las medidas de seguridad establecidas para ello.
- No utilizarán cuentas particulares en servicios externos de almacenamiento en la nube como herramienta en el desarrollo de sus funciones.
- Utilizarán preferentemente formatos de ficheros basados en estándares abiertos de forma que se satisfaga el principio de neutralidad tecnológica y se facilite la interoperabilidad y la reutilización de la información.
- Velarán por la accesibilidad de los documentos y contenidos que generen y que vayan a ser publicados en los sitios web de la Junta de Andalucía.

Uso de Internet

- Accederán a Internet como herramienta de servicio, productividad y conocimiento, con las directrices, medios y habilitación que, en su caso, les haya establecido la Administración de la Junta de Andalucía.
- El uso de Internet por los profesionales tendrá una finalidad adecuada a su ámbito profesional, sin que en ningún caso pueda ir en detrimento de la realización de sus funciones, la seguridad o el rendimiento de la red.
- No accederán a direcciones de Internet que tengan un contenido que no sea ético o que resulte ofensivo, ilegal o atentatorio contra la dignidad humana.
- La Administración de la Junta de Andalucía podrá restringir total o parcialmente el acceso a determinados contenidos en Internet por motivos legales, de seguridad, de eficiencia en el uso de los recursos u otros que se determinen.
- Los profesionales tendrán en consideración que la navegación que realicen por Internet podrá ser monitorizada y registrada en su totalidad, en especial direcciones de acceso, tiempo de conexión, contenidos accedidos y ficheros descargados.
- Los profesionales no visitarán páginas no fiables o sospechosas para evitar posibles incidentes de seguridad, en especial, las que se consideren susceptibles de contener código dañino o malicioso.
- Los profesionales atenderán a las recomendaciones que reciban en materia de uso de navegadores y configuración de los mismos.
- Los profesionales no intentarán alterar o eludir las restricciones y controles de navegación que estén implantados.



Uso del correo-e

- Utilizarán la cuenta de correo electrónico corporativo que tengan asignada como herramienta de servicio, productividad y comunicación, con las directrices, medios y habilitación que, en su caso, les haya establecido la Administración de la Junta de Andalucía. El acceso a dicha cuenta de correo se efectuará mediante una credencial personal e intransferible.
- Utilizarán el correo electrónico corporativo exclusivamente para propósitos profesionales y no lo facilitarán como medio de contacto o registro para otros propósitos.
- Tendrán en consideración que los mensajes enviados o recibidos a través del correo electrónico corporativo pueden tener la condición de información pública en virtud del artículo 2.a) de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, y estar sometidos a lo dispuesto en la normativa en materia de transparencia.
- Accederán a las cuentas de correo electrónico que tengan asignadas, con la frecuencia suficiente para evitar demoras en el desempeño de sus funciones. En caso de ausencia por un periodo determinado, los profesionales deberán tomar medidas para habilitar la respuesta automática a los mensajes recibidos, de manera que no queden desatendidos.
- No usarán una cuenta de correo electrónico no corporativa para la remisión de mensajes en el desempeño de sus funciones, ni facilitarán la misma con el objeto de recibir este tipo de mensajes.
- No accederán a cuentas de correo que no les hayan sido asignadas, y se abstendrán de interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otras personas.



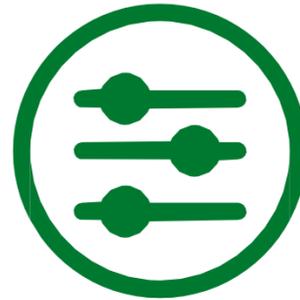
Uso del correo-e



- Observarán especial cuidado en el envío de mensajes con múltiples destinatarios, debiendo valorar la conveniencia de usar el campo de «copia oculta» para no revelar indebidamente datos personales.
 - Comprobarán, previamente al envío de cualquier mensaje, la pertinencia de todos sus destinatarios, a fin de evitar problemas de pérdida de confidencialidad y revelación de información.
 - No accederán a mensajes de correo electrónico sospechosos de tener propósito dañino o malicioso. En caso de sospechar que un determinado mensaje sea de esta naturaleza se utilizarán los mecanismos de notificación de incidentes de seguridad establecidos.
-
- Revisarán el correo electrónico clasificado automáticamente como «No deseado» (SPAM) por si incluyera mensajes incorrectamente clasificados como tales.
 - No utilizarán las cuentas de correo electrónico para almacenar de forma permanente información relevante o necesaria para el desempeño de sus funciones.
 - Prestarán especial cuidado en el acceso al correo electrónico desde dispositivos ajenos a su entorno normal de trabajo, en cuyo caso se evitará la descarga de información y el guardado de credenciales de acceso en el navegador, asegurándose de cerrar la correspondiente sesión de trabajo.
 - En el caso de resultar necesario el envío de ficheros que superen el tamaño límite establecido en el sistema de correo electrónico, los profesionales utilizarán las herramientas corporativas existentes para el intercambio de ficheros.

Además, se regulan...

- Herramientas de colaboración.
- Redes Sociales
- Política de seguridad
- Contraseñas
- Uso de certificados electrónicos



- Notificación de incidencias
- Conductas prohibidas
- Herramientas de colaboración.
- Fin del desempeño de las funciones
- Realización de comprobaciones y exigencia de responsabilidades.

ANEXO XI. DOCUMENTO DE RECOGIDA DE EQUIPAMIENTO PARA EL ALUMNADO

La persona abajo firmante, como madre / padre / tutor/a legal del alumno _____ **recibe** en funcionamiento el siguiente equipamiento: PC Portátil número de serie- _____, en calidad de **préstamo**.

Se compromete a:

1. La devolución del equipamiento en la fecha establecida, en el centro de origen, como se especifica al final de este documento.
2. Comunicar cualquier incidencia a la persona encargada de la coordinación #TDE para su gestión.
3. Si la incidencia es por pérdida o sustracción del dispositivo deberá notificarse de inmediato a la persona que ejerza las funciones de dirección en su centro educativo.
4. En general, hacer un uso correcto del equipamiento; en caso contrario, cualquier deterioro deberá ser reparado a su cargo, debiendo reintegrar un equipo nuevo en caso de un desperfecto que lo haga inutilizable.
5. No realizar ninguna modificación de hardware o software en el dispositivo (incluido Sistema Operativo).
6. Reintegrar el equipo limpio de contenidos propios.
7. Utilizar el dispositivo únicamente para fines educativos.
8. No conectar el dispositivo a redes abiertas o que no sean de confianza.
9. No almacenar datos de carácter personal. En caso de ser necesario, la información deberá estar encriptada.
10. No usar la opción "guardar contraseñas" de los navegadores para las credenciales de acceso a aplicaciones educativas de uso por el centro, como por ejemplo Moodle Centros.
11. Adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso por parte de personas no autorizadas.

Este equipamiento **será devuelto** según el protocolo que el centro elabore para ello, procediéndose a registrar la devolución y el estado del equipo, teniendo como plazo máximo el 30 de junio o hasta que se produzca un traslado de centro durante este curso escolar.

En Huércal de Almería, a _____ de _____ de 20__

Fdo.: _____

ANEXO XII. DOCUMENTO DE RECOGIDA DE EQUIPAMIENTO PARA EL ALUMNADO

La persona abajo firmante, como madre / padre / tutor/a legal del alumno _____ **recibe** en funcionamiento el siguiente equipamiento: PC Portátil número de serie- _____, en calidad de **préstamo**.

Se compromete a:

1. La devolución del equipamiento en la fecha establecida, en el centro de origen, como se especifica al final de este documento.
2. Comunicar cualquier incidencia a la persona encargada de la coordinación #TDE para su gestión.
3. Si la incidencia es por pérdida o sustracción del dispositivo deberá notificarse de inmediato a la persona que ejerza las funciones de dirección en su centro educativo.
4. En general, hacer un uso correcto del equipamiento; en caso contrario, cualquier deterioro deberá ser reparado a su cargo, debiendo reintegrar un equipo nuevo en caso de un desperfecto que lo haga inutilizable.
5. No realizar ninguna modificación de hardware o software en el dispositivo (incluido Sistema Operativo).
6. Reintegrar el equipo limpio de contenidos propios.
7. Utilizar el dispositivo únicamente para fines educativos.
8. No conectar el dispositivo a redes abiertas o que no sean de confianza.
9. No almacenar datos de carácter personal. En caso de ser necesario, la información deberá estar encriptada.
10. No usar la opción "guardar contraseñas" de los navegadores para las credenciales de acceso a aplicaciones educativas de uso por el centro, como por ejemplo Moodle Centros.
11. Adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso por parte de personas no autorizadas.

Este equipamiento **será devuelto** según el protocolo que el centro elabore para ello, procediéndose a registrar la devolución y el estado del equipo, teniendo como plazo máximo el 30 de junio o hasta que se produzca un traslado de centro durante este curso escolar.

En Huércal de Almería, a _____ de _____ de 20____

Fdo.: _____

DOCUMENTO DE PRÉSTAMO DE EQUIPAMIENTO TECNOLÓGICO AL PROFESORADO

D./Dña. _____ recibe en perfectas condiciones y en funcionamiento el equipo _____ marca _____ y número de serie: _____ en calidad de préstamo para el ejercicio docente.

Se compromete a:

- La devolución del mismo, según la necesidad establecida por la dirección del centro, hasta que el profesorado termine su vinculación con el centro y con un plazo máximo hasta el 30 de junio.
- La persona que recibe el préstamo debe comunicar cualquier incidencia al coordinador TDE para su gestión.
- Si la incidencia es por pérdida o sustracción del dispositivo, deberá notificarse de inmediato a la persona que ejerce la dirección del centro, presentando la denuncia de tal hecho.
- En general, hacer un uso correcto del equipamiento; en caso contrario cualquier deterioro deberá ser reparado a su cargo, debiendo reintegrar un equipo nuevo en caso de un desperfecto que lo haga inutilizable.
- No realizar ninguna modificación de hardware o software en el dispositivo (incluido el sistema operativo).
- Reintegrar el equipo limpio de contenidos propios.
- Utilizar el dispositivo únicamente para fines profesionales.
- No conectar el dispositivo a redes abiertas o que no sean de confianza.
- No almacenar datos de carácter personal. En caso de ser necesario, la información deberá estar encriptada.
- Adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso por parte de personas no autorizadas.
- Para la retirada del equipo el profesorado solicitante aportará una funda, bolso o mochila para su protección ya que la caja del equipo queda custodiada en el centro.

En Huércal de Almería, a _____ de _____ de 20____

El maestro/a solicitante

Fdo.: _____



COMPROMISO DEL TUTOR/A LEGAL PARA EL USO EXTRAORDINARIO DE DISPOSITIVOS MÓVILES EN EL VIAJE DE ESTUDIOS POR PARTE DE ALUMNADO MENOR

Normativa vigente en protección de datos:

Artículo 18 de la Constitución Española, se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El RDPD, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Instrucciones de 4 de diciembre de 2023, sobre regulación de uso de móviles en los centros educativos.

Fecha: _____

Yo, _____, como padre, madre o tutor legal del alumno/a:

del curso _____ me comprometo, en representación de mi hijo/a menor de edad a:

1. Que haga un uso adecuado, utilizando el móvil únicamente cuando los docentes le den permiso y sólo para realizar llamadas por teléfono.
2. No hacer un uso ofensivo contra cualquier persona, no realizar imágenes, audios y vídeos de menores.

Firma del Padre/Madre o tutor/a legal.

