Guía de Uso
Responsable TICs
CEIP TARTESSOS
Curso 21/22

ÍNDICE

- 1. Introducción y justificación ¿Por qué esta guía?**
- 2. Objetivos**
- 3. Principios sobre el buen uso de las TIC**
- 4. Prácticas para un uso responsable de las TIC**
- 5. Normas de uso de las tecnologías en el centro**
- 6. Sanciones**
- 7. Medios, recursos humanos y materiales en caso de detección de conductas de acoso en red**
- 8. Bibliografía**

1. Introducción y justificación ¿Por qué esta guía?

Vivimos en una sociedad cada vez más conectada en la que Internet y las redes sociales adquieren mayor protagonismo, con una tecnología cada vez más asequible y que sigue evolucionando: cualquier persona accede a Internet gracias a los móviles, tablets, ordenadores, etc. También hay que señalar que la edad a la que se adquiere el primer dispositivo móvil con acceso a Internet continúa bajando. A pesar de lo extendidas que están, se echan en falta recursos que faciliten el conocimiento para un uso responsable y seguro, que debe primar cuando hablamos de personas menores de edad.

Las Tecnologías de la Información y la Comunicación (TIC) constituyen un elemento clave de nuestro modelo educativo. Nos hemos esforzado mucho por implantar un modelo educativo que tuviera presente el uso de estas herramientas, tanto en el aula como fuera de ella. En este camino 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 ha realizado un profundo trabajo con alumnado y profesorado con el fin de que se consiga un uso responsable y educativo de estas nuevas tecnologías.

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 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.

2. Objetivos.

- Asegurar que los/as alumnos/as del centro se benefician de las ventajas del uso de las TICs en la educación de forma efectiva y segura.
- Formar e informar sobre métodos de autoprotección y protección de otros en la red.
- Evitar el mal uso de las TICs de forma intencionada o por desinformación.
- Ofrecer un marco ético y proponer buenas prácticas para así favorecer un uso correcto de las tecnologías digitales en el entorno educativo.
- Ser un recurso para dar a conocer, sensibilizar, implicar y facilitar un uso responsable de las TICs.

3. 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 derramar comida o líquidos sobre ellos.

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 TICs 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. 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. 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.

K. Cuidar el ordenador, tablet, móvil..., evitando riesgos físicos, como derramar comida o bebida sobre ellos, ponerlos en focos de calor, que sufran golpes, y mantener limpios todos los componentes.

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.

4. Prácticas para un uso responsable de las TIC.

A continuación, te proponemos 7 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. 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 descargar aplicaciones siempre de web oficiales y utilizar antivirus para proteger los dispositivos del centro de posibles amenazas.

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. Por tanto, hay que acordar con ellos unos horarios y unas finalidades para las que se conectarán en cada clase y en los momentos de ocio. 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 dar 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 redes sociales como Facebook o páginas de Internet 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 letras y números.

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

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 el centro quisiera. 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 ordenadores. Aprender a no hacer clic en enlaces sospechosos previene el acceso a páginas web con amenazas capaces de infectar los ordenadores. 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.

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.

5. Normas de uso de las tecnologías en el centro

- 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.
- El centro promoverá el uso de herramientas para aplicaciones, páginas... que necesiten registro por parte de los/as alumnos/as a través de Google Suite.
- 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.
- 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 hay que 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 TICs
- El centro podrá comprobar los archivos guardados, descargados, histórico de la 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.
- 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.
- Comunicaciones del profesorado con el alumnado, en caso de disponer de un correo electrónico éste se utilizará exclusivamente para la actividad educativa. Las familias serán conocedoras del correo que usan los estudiantes para la actividad escolar y así poder supervisarlos.
- Las alumnas y alumnos harán comunicaciones mediante correo electrónico o redes sociales 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:
 - o Mostrar respeto por uno mismo y todas las personas de la comunidad escolar.
 - o Proteger la propia identidad y la de otras personas.
 - o Respetar y proteger la propiedad intelectual.
- Se podrán emplear servicios en la nube para entregar las actividades.
- Cualquier persona de la comunidad educativa que se percate de un uso inadecuado de las comunicaciones deberá comunicarlo inmediatamente para tomar las medidas oportunas.

NORMAS DE USO DE LAS REDES SOCIALES EN EL CENTRO EDUCATIVO.

- 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 padre/madre (menores).
- 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 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, equipo directivo y profesorado intentarán hacer uso de las redes sociales como medio para difundir sus actividades habituales.
- Mediante el uso de cuentas personales se facilitará al profesorado enlaces a documentos (textos, videos, infografías...) que faciliten su formación.
- Tanto las imágenes como la música que se publiquen en las redes sociales del centro cumplirán la normativa respecto a los derechos de autor.
- Todas las familias y trabajadores del centro firmarán un documento en el que firmen su consentimiento o su negativa a aparecer en publicaciones del centro.
- Se animará a participar en estos canales de comunicación a las personas más reticentes planificando actividades que potencien su uso para reducir en la medida de lo posible la brecha digital.

- No se permite 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.

NORMAS DE USO DE LOS DISPOSITIVOS MÓVILES/TABLETS y ORDENADORES EN EL CENTRO

El uso de dispositivos móviles/tablets y ordenadores en el centro será permitido exclusivamente con fines educativos. El uso de dispositivos móviles/tablets y ordenadores en el centro se hará siempre bajo la supervisión de un/a profesor/a. Cuando se requiera el uso de dispositivos por parte del alumnado el/la profesor/a responsable se asegurará de que todos los/las alumnos/as disponen de estos recursos. Se utilizarán sólo las aplicaciones o páginas que exclusivamente pida el profesorado, y sólo se utilizarán en ese momento. El profesorado también se encargará de realizar una lista con las aplicaciones o páginas que se pueden utilizar y otras que no. La conexión se realizará siempre a través de la Wifi del colegio. El profesorado dinamizará la creación y utilización de herramientas y aplicaciones digitales a las que el alumnado accederá mediante el uso de los diferentes dispositivos. Se tendrá en cuenta el horario de préstamo que dispone el centro para cada uno de los dispositivos y clases. En caso de utilización de dispositivos en horario no establecido para dicha clase habrá que solicitarlo con “suficiente antelación” al Equipo Directivo o coordinador TDE.

6. Sanciones

- 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

Leves:

- Uso del dispositivo sin permiso: se requisará el dispositivo durante ese día/clase.

Graves:

- Utilizar el dispositivo para realizar fotografías/vídeos/audios sin el consentimiento del afectado.
- Acceder a páginas no apropiadas.
- Acceso a redes sociales sin autorización del docente.
- Acceso a aplicaciones no autorizadas por el docente.

Se le retirará el dispositivo, impidiendo su uso en el centro, durante el tiempo considerado por el Equipo docente. Se tendrá en cuenta lo dispuesto en el ROF.

7. Medios, recursos humanos y materiales en caso de detección de conductas de acoso en 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:

-Ciberbullying: acoso entre alumnos/as

-Ciberbaiting: 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 de manera permanente.

Se tendrán en cuenta los protocolos para prevenir, detectar, mediar y resolver los conflictos que establece legislación vigente.

Teléfonos de ayuda contra el acoso y el Bulling:

Ministerio de Educación: 900018018

Grupo de Protección al Menor en el uso de las NNTT: 915822358

SOS Bullying: 640489332

Acoso Escolar y maltrato infantil en Andalucía: 900851818

Comunicación de cualquier actividad ilegal a través del uso de las Redes Sociales

8. Bibliografía

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 enredas 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
Guía de privacidad y seguridad en internet.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Privacidad_y_Seguridad_en_Internet.pdf 12 ANEXO I Formulario de