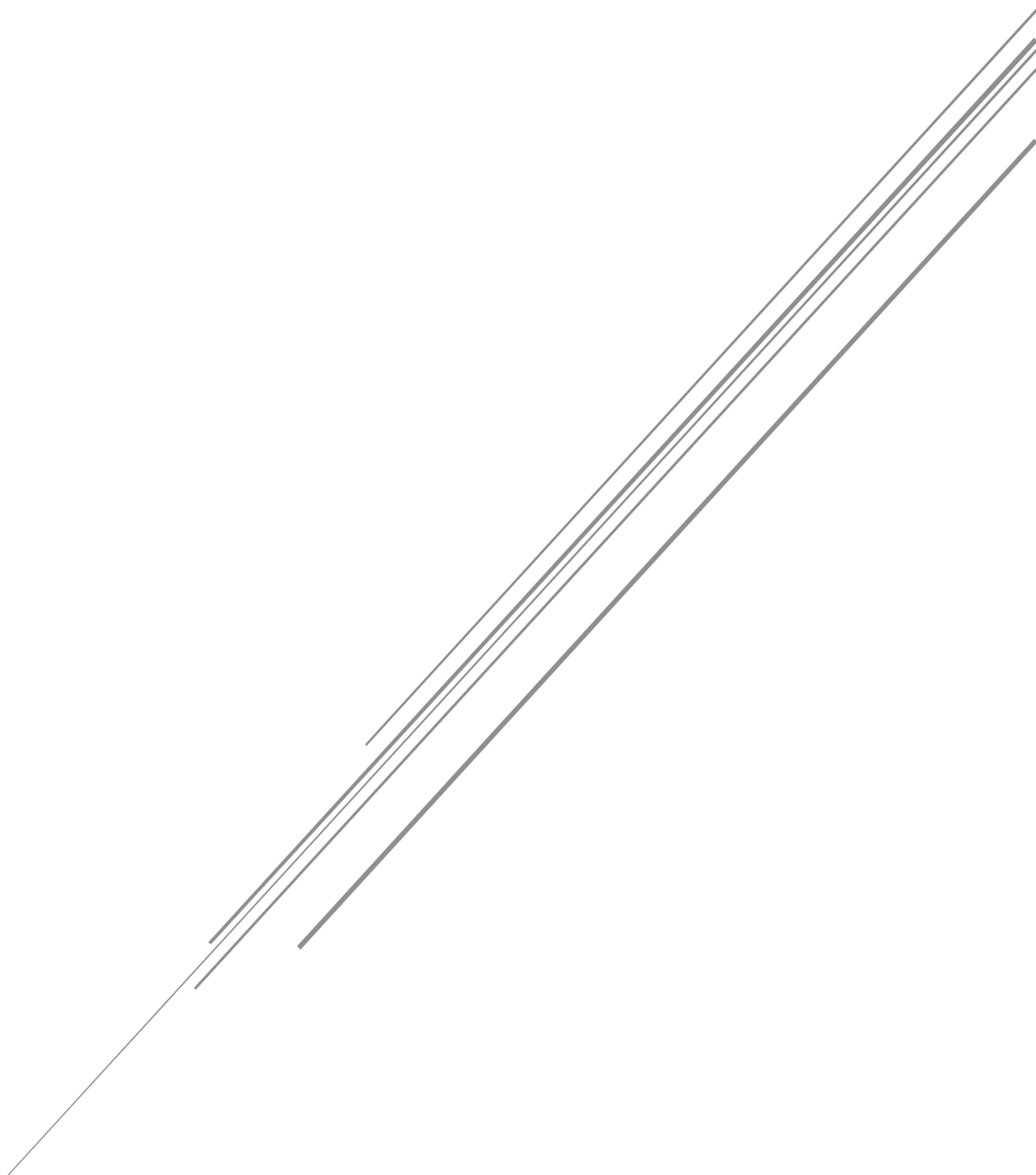


GUÍA BUENAS PRÁCTICAS TIC



CEIP EL OTERO

Contenido

INTRODUCCIÓN	2
DECÁLOGO DE BUENAS PRÁCTICAS.....	2
PELIGROS DE INTERNET	2
Netiqueta.....	2
Phishing.....	3
Cyberbullying.....	3
Contenidos inapropiados:.....	3
Oversharing.....	4
Phubbing.....	4
Retos virales.....	4
Grooming	5
La dictadura del like	5
Sexting.....	5

INTRODUCCIÓN

En el momento actual se hace un uso cada vez más asiduo de las TIC y a los niños se les entregan los dispositivos sin darles unas instrucciones concretas sobre su buen uso.

Una vez que entramos en internet tenemos a nuestro alcance toda clase de contenidos. Los menores pueden estar sobreexpuestos a contenidos para los que no están preparados.

Internet es una red global sin límites. Los adultos debemos establecer los límites para los menores, informando, educando y dando instrucciones sobre el buen uso. Los menores cada vez utilizan más tiempo, y a edades más tempranas las tablets, ordenadores y teléfonos móviles. Las herramientas digitales pueden poner a los menores en gran peligro. Deben de ser conscientes de los peligros que entraña y cómo actuar en cada caso. Es por esto en el centro hemos decidido establecer un plan de trabajo para que sean conscientes desde primero de infantil de los peligros del mal uso de las tecnologías.

DECÁLOGO DE BUENAS PRÁCTICAS

1. Conoce tu dispositivo.
2. Conéctate a redes seguras.
3. Defiende tu privacidad.
4. Respeta a los demás.
5. Guarda tus contraseñas.
6. Entra en páginas web seguras.
7. Identifica información falsa.
8. Usa el control parental.
9. Pide ayuda cuando lo necesites.
10. Respeta los derechos de autor.

PELIGROS DE INTERNET

Netiqueta

¿Qué es? Es el conjunto de normas sociales que se usan a través de internet. Estas normas son propuestas y aceptadas por los usuarios de la red dentro de cada contexto de uso. Son normas similares a las que seguimos en nuestras interacciones sociales cara a cara.

¿Cómo actuar? Al igual que cuando hablamos con alguien mostramos respeto, interés por lo que nos dicen, turno de palabra, etc. debemos hacer lo mismo cuando nos comunicamos a través de internet.

Phishing

¿Qué es? Consiste en intentar conseguir información de una persona de forma fraudulenta a través de Internet. La información suele estar relacionada con contraseñas y códigos de tarjetas de crédito y de bancos.

¿Cómo prevenirlo? Antes de introducir contraseñas o códigos debemos de estar seguros de que es una página segura.

¿Cómo actuar? En caso de que recibamos correos sospechosos, con faltas de ortografía, con recomendaciones, premios que has ganado o que no estemos seguros de que provienen de donde dicen que provienen tenemos que denunciarlo y nunca contestar.

Cyberbullying

¿Qué es? Se trata de infligir daño a otra persona a través de las redes sociales mediante insultos, amenazas, secuestro de cuentas, suplantación de identidad. También lo puede hacer un grupo de personas que se ríen de otra.

¿Cómo prevenirlo? Educación en contra de este tipo de situaciones y a favor de la gestión de la privacidad y el derecho y respeto de las identidades digitales.

¿Cómo actuar? La víctima no debe contestar a las provocaciones, bloquear o silenciar al acosador, denunciar la situación y en todo este proceso debe tener el apoyo de la familia para sentirse fuerte frente a los insultos, amenazas, etc.

Contenidos inapropiados:

¿Qué es? Se trata de documentos escritos, vídeos o imágenes que contengan temáticas no apropiadas que nuestros alumnos y alumnas deben de evitar: violencia, juegos de azar, sexualidad y malos hábitos de salud.

¿Cómo prevenirlo? La mejor manera de prevenirlo es explicarles los contenidos que pueden encontrar en la red y que deben de evitar. También las familias deben de ser conscientes de la importancia de instalar controles parentales en los dispositivos.

¿Cómo actuar? En caso de que veamos a un menor expuesto a contenidos inapropiados, debemos hablar con ellos, no culpabilizarlos, pero que comprendan la gravedad de la situación y, en casos extremos, denunciar a la policía.



Oversharing

¿Qué es? Es la exposición en redes sociales que afecta a nuestra reputación e identidad digital. En cada publicación que se hace se incluye gran cantidad de información sobre nosotros, en algunos casos sin darnos cuenta.

¿Cómo prevenirlo? Se debe reflexionar sobre un contenido antes de compartirlo, sobre la importancia de no dar más información de la que sea estrictamente necesario. Cuantos más datos exponemos, mayor es el riesgo presente y futuro. Antes de enviar o publicar algo relacionado con nosotros, debemos de preguntarnos:

¿Con quién lo vamos a compartir? ¿Incluye más información de la que queremos compartir? ¿Incluye información personal? ¿Puede causarnos problemas?

¿Cómo actuar? Mostrar una publicación y extraer de ella información para que vean cómo se comparte más de lo que parece. Poner un ejemplo de cómo en cada interacción que hacemos en la red, sea a través de mensajes, publicaciones, web o apps que usamos, deja un rastro digital que, en algunos casos es imposible eliminar y seguirán apareciendo durante años.

Phubbing

¿Qué es? Viene del inglés phone y snubbing que significa ignorar a alguien por usar el teléfono. Puede ser por una adicción al teléfono, pero también puede ser una forma de ocultar nuestra timidez o por imitar a los demás.

¿Cómo prevenirlo? Se tienen que establecer unas normas claras de uso y un horario para impedir el uso del móvil ignorando a las personas.

¿Cómo actuar? Los adultos deben de ser un ejemplo para saber desconectar cuando se está con otras personas.

Retos virales

¿Qué es? Son propuestas de retos que se llevan a cabo, se graban y se comparten a través de las redes sociales para que se hagan virales. Al peligro hacia la identidad digital hay que añadirle que, en muchos casos son retos que conllevan gran peligro para la integridad física de las personas.

¿Cómo prevenirlo? Se debe supervisar el uso de los dispositivos, el tipo de contenidos que buscan y que publican, si cambia su círculo de contactos en redes sociales, si siguen a algún influencer etc. y si tienen, de repente, algún comportamiento extraño, piden algún objeto inusual o permiso para hacer algo fuera de lo normal.

¿Cómo actuar? Se debe establecer una comunicación muy fluida para que sientan la confianza de explicar por qué han participado en esta clase de retos y trabajar mucho su autoestima, porque se suele buscar encajar en el grupo.

Grooming

¿Qué es? Es un engaño deliberado a un menor por parte de un adulto para cometer un abuso sexual. A través de las redes sociales el adulto se crea un perfil aparentando tener la misma edad y gustos que el menor para ganarse su confianza y que acceda a enviar fotos de contenido sexual o incluso quedar en una cita.

¿Cómo prevenirlo? Se debe establecer la norma básica de que no deben mantener conversaciones con extraños a través de internet y si alguien que no conocen se pone en contacto con ellos de alguna manera que lo informen a un adulto.

¿Cómo actuar? Un menor que ha sufrido grooming es una víctima que necesita apoyo y seguridad para contar lo que ha pasado y poder denunciar los hechos.

La dictadura del like

¿Qué es? Es una forma de valorar positivamente algo que un amigo ha colgado en una red social, puede ser texto o imágenes. Cuantos más “like” tenga una persona quiere decir que tiene más seguidores y más reconocimiento. Cada vez es más importante para determinar la aceptación y sociabilidad de una persona y alguien que tenga pocos puede llegar a pensar que no es aceptado, lo que incide en su autoestima. Pueden llegar a situaciones de riesgo para conseguir los “like” e incluso a amenazar.

¿Cómo prevenirlo? Trabajar la autoestima es fundamental, para que no dependa de los “like” que se sientan bien consigo mismos. Es también necesario supervisar todo el contenido que suben a las redes sociales.

¿Cómo actuar? Quitar importancia al número de “like” y aportarles confianza.

Sexting

¿Qué es? Es el envío de contenido sexual a través de Internet, ya sea de la persona que lo envía como de otra persona al que le hace una foto.

¿Cómo prevenirlo? Educar en contra de difundir públicamente cualquier tipo de imagen nuestra, especialmente si tiene contenido sexual y a favor del disfrute saludable de Internet y redes sociales.

¿Cómo actuar? En relación con quien envía el contenido: se debe de tratar de parar la cadena de envíos del contenido, contactando con el responsable de la web para que lo retire, cuanto más se difunda más posibilidades hay de que haya cyberbullying, grooming, geolocalización y riesgos físicos. En relación con quien recibe el contenido: educar hacia no visionar este tipo de contenido, denunciarlo y no difundirlo; si se conoce a la persona implicada informarle.