Guía de buenas prácticas TIC para las familias

Junta de Castilla y León

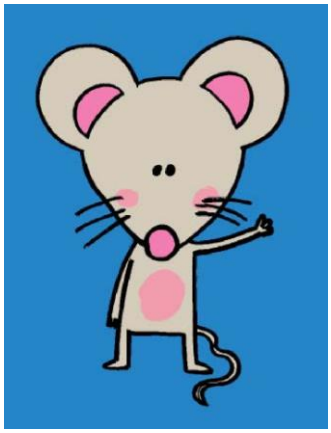
LAS VENTAJAS DE LA ESCUELA DIGITAL

Gracias a la interacción entre nuevos medios y métodos de aprendizaje, se logra que el alumnado desarrolle capacidades imprescindibles en el Siglo XXI:

- ***Aprender por sí mismo*** (autoaprendizaje) y aprender por descubrimiento de forma continuada en el tiempo.

- ***Trabajar en equipo*** y cooperativamente, de forma creciente, autónoma y planificada.

Red XXI es la adaptación del trabajo escolar a los cambios en nuestra sociedad, para mejorar la calidad de la enseñanza y aumentar el éxito escolar.



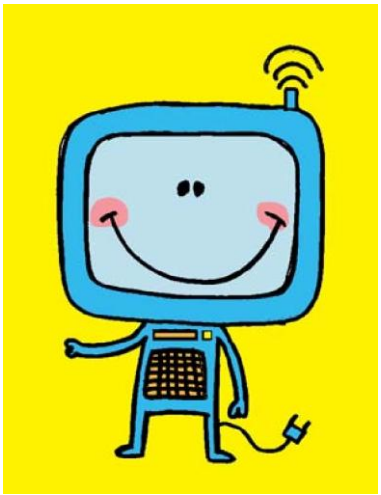
- ***Buscar, evaluar, procesar e interpretar información,*** comunicarla y transformarla en conocimiento significativo.

- ***Hacer un uso responsable de las tecnologías,*** conociendo las buenas prácticas y los potenciales peligros, regulando satisfactoriamente su relación con ellas y sus hábitos de usuario.

- ***Comunicarse y expresarse*** con distintas intencionalidades y en diferentes situaciones, aprovechando todas las posibilidades que proporcionan las Tecnologías de la Información y la Comunicación, para desarrollar su creatividad y mejorar sus habilidades sociales.

- ***Aprovecharse de la actualización permanente de los contenidos,*** y personalizar su proceso de aprendizaje, adaptándolo a sus intereses, capacidades y necesidades.

¿CUÁNDO Y CUÁNTO USAR EL ORDENADOR?



Una de las primeras contribuciones de las familias es ayudar a sus hijos e hijas a planificar convenientemente los tiempos de uso del ordenador: ***establecer y hacer cumplir un horario*** (con cierta flexibilidad, pero con criterios claros)

- Las posibilidades de consulta de información, ocio o relaciones sociales con las TIC son casi ilimitadas. Pero hay que ***evaluar el tiempo de uso acumulado*** o la proporción entre ese tiempo y el rendimiento obtenido.

- Hay que evitar usos obsesivos.

Las familias juegan un papel fundamental en la regulación del tiempo de uso (marcando horarios para tareas escolares, y delimitando también un tiempo para el ocio o las relaciones sociales on-line), procurando también espacios y tiempos para la interacción personal presencial. En casos extremos se puede llegar a generar un problema de aislamiento.

La labor de las madres y padres ante el desarrollo de las tareas escolares cobra nuevos matices: los adultos no necesitan ser usuarios expertos de las tecnologías de la información y la comunicación, pero deben mostrar sensibilidad ante las ventajas de su uso. Además, hay un amplio campo de apoyos que pueden y deben prestar.

LA INFORMACIÓN PROCEDENTE DE INTERNET

• Algunas tareas escolares pasan por la ***búsqueda de información en Internet:*** hay que "filtrarla" y evaluar su calidad.

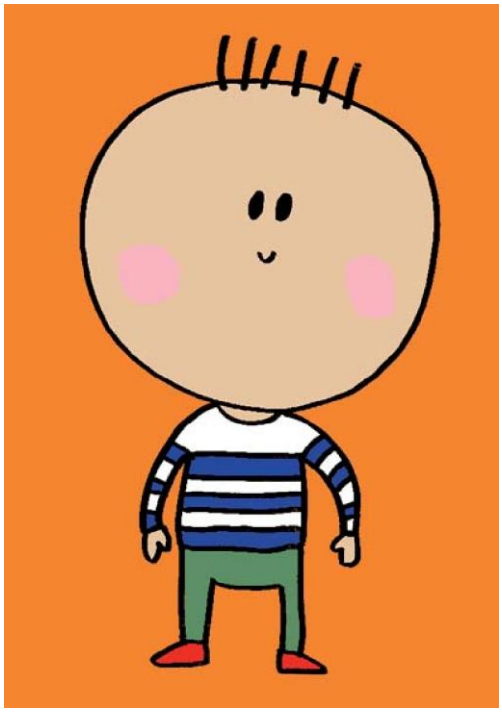
En todo caso, los padres deben ser sensibles ante una nueva realidad: uno de los retos escolares del presente consiste, precisamente, en la habilidad de encontrar, evaluar, manipular y comunicar información procedente de un medio tan heterogéneo como Internet.

• Es conveniente sacar el máximo partido posible a los motores de búsqueda de contenidos, evaluando quién ofrece una información (particulares, organizaciones, entidades educativas, centros oficiales…), ***o contrastando varias fuentes sobre un mismo campo.***

• Una buena práctica es utilizar los motores de búsqueda avanzados (que únicamente muestran las páginas web que cumplan determinadas características, como fecha de publicación, tipo de archivo, etc.)

• Las familias pueden ayudar a evitar uno de los defectos más frecuentes en los contenidos procedentes de Internet: el plagio de trabajos ya realizados (aunque sean de libre distribución).

PROTECCIÓN DE LA INTIMIDAD



Las plataformas sociales (como Tuenti, Facebook, Skype, Messenger…) están diseñadas para interconectar personas, compartiendo información, contactando en tiempo real (chat, videoconferencia, audioconferencia…) o facilitando la posibilidad de ponerse en conexión con otros usuarios (si aceptan establecer esta relación).

Es posible que usuarios que sólo se conocen por coincidir en este tipo de plataformas acaben estableciendo un contacto en la vida real. También puede suceder que un usuario acabe poniéndose en contacto con los contactos de otro al que ha aceptado en su lista de amistades virtuales (a esto se le denomina ***difusión viral*** de la red social). Además, ofrecen un conjunto de herramientas, como intercambio de archivos de cualquier tipo, búsqueda de personas, formación de colectivos o afiliados a un grupo, etc., integradas en una misma página o plataforma web.

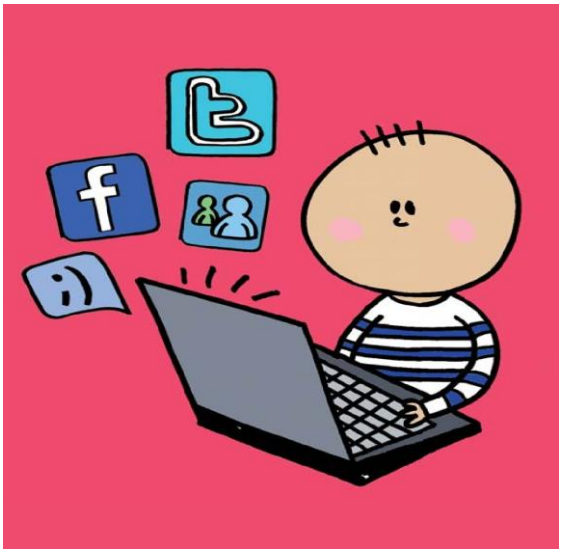
Las familias deben aceptar con normalidad ***estas nuevas vías de comunicación social, que, bien empleadas, pueden ser beneficiosas y enriquecedoras.*** No deben angustiarse por la sensación de falta de control sobre el uso de las redes sociales, sino adoptar algunas normas básicas, consensuadas con sus hijas e hijos, como preguntar periódicamente por los contactos aceptados, e informarse si se producen comunicaciones o solicitudes extrañas. Por regla general, un diálogo natural e inteligente respecto al uso de las redes –sin excluir hablar de sus peligros- es más eficaz que una posición de rechazo frontal. Las redes sociales son uno de los cauces más frecuentes de socialización, y bien usadas son beneficiosas para el menor (desarrollan la empatía, habilidades comunicativas, solidaridad, etc.)

El uso de redes sociales ***puede generar algunos problemas que podemos evitar:*** en ocasiones, los usuarios de la red no son conscientes de que los datos que indican en su perfil (edad y fecha de cumpleaños, gustos, aficiones, etc.) van a estar a la vista de cualquier persona, e incluso constituyen un bien codiciado por agencias de márketing o personas que pueden aprovecharlos para usos no lícitos.

Algunas recomendaciones a la hora de participar en una red social son:

- Asegurarse que la plataforma tenga una política de protección de datos y que ésta sea siempre visible (no sólo en el momento de darse de alta) y que se pueda imprimir o descargar.
- En caso de que se desee saber qué datos personales han sido almacenados (y, en su caso, borrarlos, modificarlos o actualizarlos), se puede solicitar ejercitar los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO). Si la plataforma no responde a esa petición puede recurrir a denunciar la situación a la Agencia Española de Protección de Datos (www.agpd.es)
- También es denunciable ante la AEPD la recepción de publicidad o información no deseada, que pudiera tener su origen en los datos proporcionados a redes sociales sin autorización del usuario.

Es preciso considerar que muchos de los materiales (fotos y vídeos, fundamentalmente) alojados en una plataforma social tienen una alta posibilidad de resultar accesibles desde distintas páginas web por millones de usuarios. Un usuario autorizado a acceder a nuestras imágenes o vídeos puede (con distintas intenciones) acabar difundiéndolo. Por eso, las redes sociales que se usen deben tener formas de denunciar la difusión de contenidos inadecuados.



Podremos exigir a sus administradores la eliminación de un contenido personal, un comentario o un texto que se esté difundiendo sin nuestra autorización.
En caso de la difusión no consentida de datos de menores, es posible recurrir ante las distintas instituciones para la defensa del menor, así como de los Cuerpos y Fuerzas de Seguridad del Estado.

Un criterio básico en el uso de la red social es no facilitar en el perfil público datos personales que no comunicaríamos a un desconocido, como domicilio, teléfono, lugar de estudio, profesión de los padres, datos sociológicos, económicos, ideas y creencias políticas, religiosas o de cualquier tipo, fotos, información sobre gustos y aficiones, etc.

Es necesario concienciar a nuestras hijas e hijos de las ventajas de las redes sociales, pero también de los posibles riesgos que generan:

- No deben usarse redes sociales que no se conozca y ofrezcan garantías. No debe aceptarse nunca una invitación de una red que no se conozca, aunque provenga (aparentemente) de un usuario conocido. Es fácil informarse en Internet sobre cada una de las redes sociales, antes de afiliarse a ella.
- No debe indicarse en el perfil una edad que no corresponda con la real, porque puede provocar que adultos desconocidos entren en contacto con el menor. Tampoco puede suplantarse una identidad.
- El perfil creado debe configurarse para que sólo puedan verlo las personas a quien autorice el menor, no dejándolo en modalidad pública.

• Nunca debe admitirse a personas que no se conozca (aunque aparentemente sean amigos de amigos a los que ya se han admitido).

• Hay que asegurarse, en todos los casos, que el perfil de la persona con la que voluntariamente contactamos corresponda con quien aparenta ser. Es fácil recurrir a todo tipo de engaños: fotos falsas, perfiles falsos, empleo de nombres falsos –incluyendo suplantación-, etc.

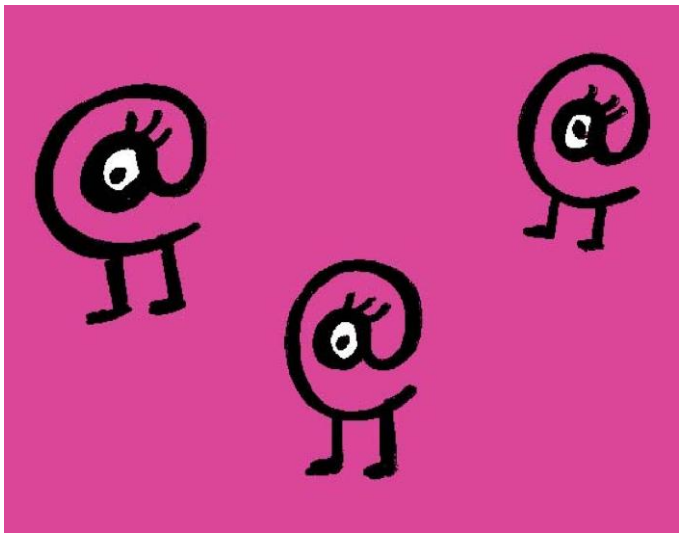
• Al igual que en la vida real, en la red no deben nunca emplearse insultos, amenazas, comentarios hirientes, etc. Internet es un espacio público. Muchos casos de ciberacoso comienzan por incidentes surgidos en el uso de redes sociales.

• No deben aceptarse archivos adjuntos de ningún tipo si no se conoce y autoriza a quien los remite. También es importante ignorar recomendaciones como la de visitar páginas web desconocidas, y aceptar juegos u otros programas (que, entre otros peligros, pueden vulnerar los derechos de propiedad intelectual). Deben rechazarse las páginas en la se solicite registrarse, dar el número de la cuenta corriente, etc., sin la presencia de un adulto responsable.

• Ante cualquier contacto no deseado, comentario inadecuado o extraño, incitación a una cita presencial sospechosa, petición de fotos u otro material, solicitud de información personal, o cualquier injuria u ofensa, el menor o los adultos responsables deben bloquear a la persona de la que provienen, denunciarlo a la red social, y evitar responder a provocaciones.

CIBERACOSO Y GROOMING O ACOSO SEXUAL

Se puede hablar de ciberacoso para referirse a actuaciones como vejaciones, insultos o chantaje mediante tecnologías de la información y la comunicación.



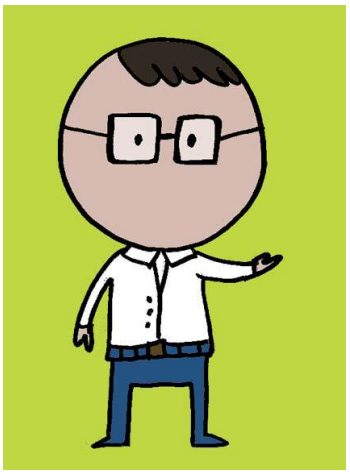
Una de las formas más frecuentes es el ***ciberbullying,*** que consiste en difundir información con objeto de causar daño mediante correo electrónico, redes sociales, teléfonos móviles, etc., incluyendo la publicación de fotografías o vídeos en las páginas web de difusión de contenidos. El acosador y el acosado (que en muchas ocasiones no sabe cómo actuar) suelen ser compañeros de centro educativo, grupo social o vecindario, coincidiendo físicamente en la vida real con frecuencia, y teniendo edades similares. Es frecuente que situaciones de acoso en la vida real, o incidentes de convivencia, sean los desencadenantes de ciberbullying.

Si las familias sospechan o detectan que esta situación se está produciendo, se debe actuar:

• Evitar que el menor siga manteniendo cualquier contacto o relación con el acosador.

• Pedir que la información generada vejatoria sea retirada del servidor de contenidos de Internet en la que se encuentra, y posteriormente de los índices de los contenidos de buscadores en los que aparezca.

• Denunciar la situación a las Fuerzas y Cuerpos de Seguridad del Estado. Es conveniente aportar pruebas gráficas del material vejatorio o calumnioso (correos, comentarios en foros, fotos, etc.) que el acosador haya generado.



Se habla de ***grooming*** para referirse a un acoso realizado por un adulto con pretensión de mantener un control emocional o un chantaje respecto a un menor, para provocar posteriormente situaciones de abuso. El contenido de dicho acoso explícita o implícitamente tiene un contenido sexual.

En todo el proceso el menor se ve poco a poco violentado, actuando contra su voluntad, sintiéndose aislado e incapaz de confiar lo sucedido a los padres o adultos responsables.

Este tipo de situaciones deben ser denunciadas. La Policía tiene una Brigada de Investigación Tecnológica (htTp://www.policia.es/bit/in-dex.htm), encargada de este tipo de labores, como la persecución de amenazas, injurias y calumnias por correo electrónico, SMS, foros, web, etc., protección al menor en el uso de las nuevas tecnologías, pornografía infantil, piratería digital, estafas en Internet, virus, sustracción de datos, suplantación de seguridad, etc.

Un consejo práctico es que los padres visiten también esas mismas redes sociales. Esta práctica permitirá conocer las posibilidades y amenazas que las mismas tienen, y proporcionará una cercanía y empatía con los menores bajo su protección.

CONTENIDOS NO DESEABLES Y PROTECCIÓN DE LA NAVEGACIÓN INFANTIL

Muchas páginas de Internet presentan contenidos no deseables para los menores (desde pornografía a incitación a la violencia, etc.) Evitar que un menor acceda a ellas no siempre es fácil. Por eso es conveniente, en la medida de lo posible, estar alerta cuando los menores naveguen libremente por Internet, aunque sea en busca de información académica.

Si la situación de ciberbullying se mantiene a lo largo del tiempo: es algo más que un episodio aislado (que, por sí mismo, puede ser constitutivo de delito)

• Muchos de los buscadores de páginas web tienen opciones de filtrado, que evitan la mayoría del contenido inapropiado. Por ejemplo, Google puede configurar su búsqueda (parte superior derecha de la pantalla). Esto permite habilitar en su modo estricto el Filtro Safe-Search, que evita páginas con contenido sexual explícito. Yahoo puede editar y activar el Filtro Adulto (menú Opciones / Preferencias). En todo caso, estas opciones no son infalibles.

• Hay algunos programas que bloquean o filtran el acceso a con-tenidos no deseados, como el programa gratuito Naomi Family Safe Internet, o K9 Web Protection (en inglés)

• Hay determinados programas de monitorización y registro de uso del ordenador (algunos ejemplos son AB-PC Control, PC TimeWatch, etc)

• También hay configuraciones que permiten que el ordenador sólo pueda usarse en una determinada franja horaria. Windows, por ejemplo (Inicio/Panel de control) permite establecer las restricciones al uso del ordenador mediante la opción “Control parental”.

• Los programas de filtrado de salida ayudan a proteger los datos que el usuario de un ordenador sube a Internet (por ejemplo datos personales, etc.)

En todo caso, es conveniente que los adultos revisen el historial de navegación del menor con cierta frecuencia, comprobando qué páginas ha visitado, y para qué.