

GUÍA DE BUENAS PRÁCTICAS

(ALUMNADO)

Índice.-

1. Justificación.....	2
2. Cuestiones básicas de funcionamiento.....	2
3. Principios sobre el buen uso de las TIC	2
4. Uso de ordenadores del centro.....	3
4.1. Aula de usos múltiples	3
5. Préstamos.....	4
6. Dispositivos propios del alumnado.	4
7. Internet y redes sociales	5
8. Redes propias del centro.....	6
a. Web del centro	6
b. Seguimiento educativo	7
c. Entorno de aprendizaje	7

1. Justificación.

En la sociedad actual, la utilización de las nuevas tecnologías resulta fundamental para el desarrollo tanto personal como profesional, por lo que resulta necesaria su integración dentro del proceso de enseñanza-aprendizaje del alumnado en el aula. Por este motivo, resulta necesario establecer una guía de buenas prácticas, que permita el uso responsable de los dispositivos digitales, ya que el desconocimiento de las mismas, puede resultar sumamente perjudicial para el alumnado.

De esta forma, la guía de buenas prácticas busca informar al alumnado sobre los riesgos derivados de una mala utilización tanto de los dispositivos digitales proporcionados por el propio Centro, como por los dispositivos personales que puedan utilizar en un momento dado.

2. Cuestiones básicas de funcionamiento.

a) En primer lugar, indicar que el único propósito de la utilización de los dispositivos en el Centro, será de tipo educativo, buscando en todo momento mejorar el aprendizaje significativo del alumnado.

b) En relación con los dispositivos utilizados en el propio centro, o aquellos entregados en concepto de préstamo, será necesario aplicar en todo momento las indicaciones de la presente guía de buenas prácticas, así como el conjunto de normas establecidas para la utilización de los mismos.

c) La información obtenida por medio de los distintos dispositivos (como tablets, móviles, ordenadores portátiles, etc...), no podrá ser publicada ni distribuida por ningún medio (correo electrónico, mensajería instantánea, redes sociales, etc...) salvo autorización expresa de las personas a las que les afecte.

d) Cuando cualquier miembro de la comunidad educativa, como profesores o alumnado, lleven un dispositivo personal al Centro, será bajo su exclusiva responsabilidad.

3. Principios sobre el buen uso de las TIC

El alumnado debe conocer y tener presentes los siguientes principios:

a) Autocontrolar el tiempo que están conectados a Internet, ya sea mediante ordenador, tablet, móvil o cualquier otro dispositivo.

b) Cuidar su correcta posición corporal al usar cualquiera de los dispositivos, sentándose correctamente.

c) Tener respeto a otros usuarios, desechando totalmente las burlas, difamaciones, humillaciones y agresiones.

d) No suplantar la identidad de nadie en la red.

e) Aprender a navegar por Internet de forma segura, accediendo sólo a contenidos educativos.

f) 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 correo electrónico (imágenes, datos, perfiles, números de teléfono...), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.

g) 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.

h) Cuidar los dispositivos que utilizan, evitando caídas o el derrame de alimentos o líquidos sobre ellos.

i) No creas todo lo que lees. Ten actitud crítica y reflexiva.

j) Elabora tus propios materiales: no copies, selecciona la información, organiza tus ideas y reescribe el contenido.

k) En la elaboración de materiales ten en cuenta siempre las licencias que los protegen.

4. Uso de ordenadores del centro.

Se asignará un ordenador completo a cada alumno, para uso individual, en perfectas o razonables condiciones para su uso.

El alumno se responsabilizará del uso y cuidado del ordenador que se le haya asignado.

En caso de avería o incidencia, lo notificará inmediatamente al profesor que corresponda para ser resuelta a la mayor brevedad posible.

Se usará el ordenador con un objetivo didáctico y pedagógico.

Queda prohibido cualquier uso o manipulación no autorizada del equipo informático asignado.

Los portátiles se mantendrán limpios, sin escrituras ni ralladuras.

Es responsabilidad del alumnado tomar las medidas de seguridad necesarias para no perder la información almacenada.

No está permitido el almacenamiento de material ilegal, ofensivo, o no educativo.

4.1. Aula de usos múltiples

En el aula de usos múltiples, situada en la primera planta del centro, se encuentran a disposición del alumnado una serie de ordenadores de sobremesa para que puedan ser utilizados de manera puntual y siempre con fines educativos (completar trabajos, enviar correos, acceder a la plataforma, etc).

El alumnado no podrá, en ningún caso, hacer uso personal de ellos, ni descargar y ejecutar programas que no estuvieran instalados previamente.

5. Préstamos

Con el objeto de reducir la brecha digital entre el alumnado del IESO, el centro ha puesto en marcha un servicio de préstamos de material informático.

El alumnado beneficiario del préstamo, firmará el documento “CERTIFICADO DE PRÉSTAMO TEMPORAL DE RECURSO TECNOLÓGICO” anexo al Protocolo de Gestión de Recursos y tendrá que cumplir con las siguientes observaciones:

a) Devolver el equipamiento en la fecha establecida, en el centro de origen. Este equipamiento será devuelto según el protocolo establecido, procediéndose a registrar la devolución y el estado del equipo, teniendo como plazo máximo el 20 de junio o hasta que termine su vinculación con el centro durante este curso escolar.

b) Comunicar cualquier incidencia a la persona encargada de la coordinación de transformación digital para su gestión.

c) 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.

d) 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.

e) No realizar ninguna modificación de hardware o software en el dispositivo (incluido Sistema Operativo).

f) Reintegrar el equipo limpio de contenidos propios.

g) Utilizar el dispositivo únicamente para fines educativos y de formación.

h) No conectar el dispositivo a redes abiertas o que no sean de confianza.

i) No almacenar datos de carácter personal.

j) No usar la opción "guardar contraseñas" de los navegadores para las credenciales de acceso a aplicaciones corporativas, como por ejemplo el correo corporativo.

k) Usar la navegación privada.

l) Adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso por parte de personas no autorizadas.

6. Dispositivos propios del alumnado.

El uso de los dispositivos propios como los smartphones por parte del alumnado en el interior del centro educativo no es, en principio, necesario para el desarrollo de la actividad académica, por lo que deben permanecer en todo momento desconectados y guardados.

Excepcionalmente, un profesor/a puede permitir la utilización de los smartphones del alumnado únicamente con fines educativos. En tal caso, el alumnado se atenderá a las indicaciones del profesor/a.

En ningún caso el Instituto se responsabiliza de la pérdida, hurto o deterioro de los smartphones del alumnado, correspondiendo a cada alumno/a su guarda y custodia.

7. Internet y redes sociales

El Centro Criptológico Nacional – CCN CERT nos ofrece una serie de consejos que podríamos considerar como “buenas prácticas” cuando navegamos en internet y accedemos a las diferentes redes sociales:

- a) Cuida tus perfiles en redes sociales, aportan más información de la que piensas y conforman tu identidad digital. Procura siempre proteger y cuidar todos los documentos de identificación personal para evitar la ciberdelincuencia.
- b) Controla el contenido que publicas en redes sociales. Personas y empresas encuentran cosas sobre ti, lo analizan y sacan un juicio sobre ti en base a ellas. Si tú puedes buscar a (casi) cualquier persona por Internet, cualquier persona te puede buscar a ti.
- c) Publicar demasiada información personal tuya o de otros en redes sociales supone un riesgo. Cuanto más sensible es la información y los contenidos publicados, mayores probabilidades hay de sufrir un robo de identidad, caer en fraudes online, ser víctima de un ciberacoso y un largo etcétera.
- d) Evita publicar información sobre tu domicilio. Ten cuidado de no exponer tus documentos de información personal, número de teléfono, tarjetas bancarias. Hay que tener especial cuidado con la información que se comparte sobre menores.
- e) En Internet viene muy bien aplicar un principio básico: ser prevenido ante lo desconocido. Hacer clic en cualquier enlace, archivo adjunto o mensaje de fuentes desconocidas (incluso de conocidas) nos puede poner en grave riesgo.
- f) Tener precaución a la hora de conectarse en redes WiFi públicas. No accedas al banco cuando te conectes a través de una Wifi pública.
- g) Protege el acceso a las cuentas haciendo uso de contraseñas largas y diferentes para cada servicio.
- h) Controla si está activada o no la geolocalización de tus perfiles y contenidos en redes sociales. No es bueno dejarla activada por defecto, mejor comprobarlo y compartir la ubicación sólo cuando a ti te convenga; se trata de hacer un uso inteligente de esta funcionalidad para evitar riesgos.
- i) Comprueba siempre cómo tienes la configuración de privacidad tanto de tus perfiles en las redes sociales como en los contenidos que compartes. Nunca es buena idea dejar la configuración de privacidad por defecto; activar la revisión del etiquetado en publicaciones puede evitar más de una sorpresa.
- j) El respeto debe ser una máxima. No hay que difundir información privada sobre otras personas sin su consentimiento ni etiquetar a nadie que no quiera. Lo que no te gustaría que te hicieran a ti, no lo hagas.

A continuación, te damos algunos consejos prácticos sobre el uso de determinadas herramientas:

a. Búsquedas WEB.

- Introduce consultas sencillas.
- Piensa en cómo estará escrita la página que estás buscando. Utiliza las palabras con mayor probabilidad de aparición en la página.
- Selecciona palabras descriptivas. Cuanto más específica sea la palabra, mayor será la probabilidad de que encuentres resultados relevantes.
- Utiliza comillas para buscar frases exactas.
- Limita tu búsqueda a un periodo de tiempo concreto.

b. Contraseñas.

- Utiliza una clave diferente para cada servicio.
- Haz que tus contraseñas sean siempre robustas.
- No compartas tus claves con nadie, ni las apuntes.
- Cambia periódicamente tus contraseñas.
- Asegúrate de usar conexiones https cuando inicies sesión.
- Evita las WIFIs públicas cuando tengas que usar o acceder a información sensible.

c. Correo electrónico.

- Usa el asunto adecuado: escribe una frase informativa.
- No utilices letra mayúscula.
- No abuses de los signos de exclamación.
- Si tienes que enviar un archivo adjunto, asegúrate de haberlo subido completamente antes de enviar el correo
- Diferencia entre correo profesional y personal: son dos estilos muy diferentes.
- Elige a los destinatarios adecuados. Utiliza la opción CCO para que las direcciones de correo no sean visibles al resto de destinatarios.
- Revisa tus mensajes antes de enviarlos.

8. Redes propias del centro

a. Web del centro

El IESO Peña Escrita tiene su página web en la siguiente dirección: <http://ies-penaescrita.centros.castillalamancha.es/>

En ella podrás encontrar información importante sobre el instituto: datos de contacto, documentos destacados y novedades del portal de Educación.

b. Seguimiento educativo

Dentro de la plataforma Educamos CLM, tenemos el seguimiento educativo, que es el entorno que permite la comunicación entre los centros educativos y las familias, tutores legales y alumnado.

c. Entorno de aprendizaje

Se accede también dentro de la plataforma Educamos CLM. Dentro del mismo tendremos a acceso a las Aulas Virtuales. En ellas encontrarás los materiales y tareas del curso.