GUÍA DE BUENAS PRÁCTICAS Y USO RESPONSABLE DE DISPOSITIVOS DIGITALES

1. JUSTIFICACIÓN

El uso de las nuevas tecnologías en el proceso de enseñanza-aprendizaje de adultos, y más específicamente en las modalidades de "semipresencial" y "distancia", es algo imprescindible e ineludible. Las posibilidades que se generan con el uso de las nuevas tecnologías permiten que las actuaciones con los diferentes miembros de la comunidad educativa (profesorado, alumnado y administración educativa) sean acordes a los procesos de digitalización que se imponen en el momento actual.

Los dispositivos personales incrementan de forma notable el acceso a la información, así como la comunicación, colaboración y coordinación entre la comunidad educativa.

Por lo tanto, desde el IPEP Córdoba pretendemos fomentar un uso responsable tanto de los dispositivos del centro como de los personales, y se procurará un ambiente que promueva e incentive actuaciones en las que las tecnologías emergentes estén presentes, fomentando la adquisición y desarrollo de las habilidades necesarias en este ámbito con el objetivo de prepararse debidamente ante las nuevas formas de intervención que los medios tecnológicos permiten.

Ante todos estos planteamientos, se hace necesario, el desarrollo de una guía que establezca cómo debemos utilizar estos dispositivos ya incorporados o que se incorporarán a la dinámica de trabajo del IPEP.

2. CUESTIONES BÁSICAS DE FUNCIONAMIENTO

a) El único propósito del uso de dispositivos del centro o personales en los distintos lugares de trabajo es educativo.

b) Con respecto a los equipos que hay en el centro y a aquellos objeto de préstamo al alumnado, se seguirán las indicaciones de esta guía, así como las normas que se establezcan para su uso

c) Toda la información obtenida por medio de los dispositivos móviles (fotos, videos, audios, textos) no podrá exceder el ámbito de lo estrictamente educativo ni ser publicada o difundida por ningún medio (redes sociales, correo electrónico, mensajería instantánea, o cualquier otro que suponga publicación o difusión) salvo que se autorice expresamente por parte de aquellos a quienes la información les afecte directamente.

d) Cuando se habla de dispositivo personal se hace referencia a tablets, smartphones, teléfonos móviles, ordenadores portátiles, y todos aquellos dispositivos tecnológicos que puedan ser utilizados en el proceso de enseñanza-aprendizaje.

e) Cuando un miembro de la comunidad educativa lleva su dispositivo personal a los distintos lugares de trabajo es bajo su exclusiva responsabilidad y, por tanto, es responsable de su mantenimiento y protección.

f) La formación en la utilización de las nuevas tecnologías es fundamental para un uso adecuado y eficaz de los dispositivos asociados a ellas. Por lo tanto, es necesario facilitar la información adecuada y realizar actividades de formación periódicas que permitan un uso ágil, práctico y actualizado de dichos dispositivos.

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 leas. 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

a. Aula TIC

1. Se asignará un ordenador completo a cada alumno, para uso individual o compartido, en perfectas o razonables condiciones para su uso.
2. El alumno se responsabilizará del uso y cuidado del ordenador que se le haya asignado (CPU, monitor, ratón, teclado) y se sentará siempre en el puesto que se le asigne, salvo en caso de avería, en que se le podrá asignar temporalmente un nuevo equipo.
3. En caso de avería o incidencia, lo notificará inmediatamente al profesor que corresponda para ser resuelta a la mayor brevedad posible.
4. Se usará el ordenador con un objetivo didáctico y pedagógico.
5. Queda prohibido cualquier uso o manipulación no autorizada del equipo informático asignado.
6. Se mantendrán limpios, sin escrituras ni ralladuras, los teclados, ratones y monitores.
7. Es responsabilidad del alumnado tomar las medidas de seguridad necesarias para no perder la información almacenada.
8. No está permitido el almacenamiento de material ilegal, ofensivo, o no educativo.

b. Biblioteca

En la Biblioteca, situada en la primera planta del centro, se encuantran 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.

Para poder utilizar estos equipos, los alumnos deben utilizar su propio ratón, que deberán traer de casa, o pedir uno a los conserjes del centro.

5. PRÉSTAMOS

Con el objeto de reducir la brecha digital entre el alumnado del IPEP Córdoba, el centro ha puesto en marcha un servicio de préstamos de material informático que puede incluir equipos portátiles, tablets, ratones, etc.
El alumnado beneficiario del préstamo, firmará el documento de "Compromiso de Préstamo de Recursos T.I.C." 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 25 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 TDE 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. BYOD – DISPOSITIVOS PROPIOS DEL ALUMNADO

El concepto BYOD ("Bring your own device", es decir, "Trae tu propio dispositivo") se está imponiendo cada vez con más fuerza, debido a la extensión de uso de los smartphones, a la obsolescencia del material informático de los institutos y a las consideraciones sanitarias como consecuencia de la pandemia por el COVID-19.
El uso de los dispositivos propios por parte del alumnado en el interior del centro educativo debe ajustarse a las siguientes consideraciones.

a) Smartphones

   Los smartphones no son, en principio, dispositivos necesarios 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 atendrá 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.

b) Tablets y Ordenadores portátiles

Dadas las especiales características del IPEP y la enseñanza de adultos, el profesorado puede permitir la utilización de estos dispositivos con fines educativos, fundamentalmente para acceder a la plataforma Moodle y al Aula Virtual de cada materia o ámbito. En tal caso, el alumnado se atendrá a las indicaciones del profesor/a.

Para favorecer dicho uso, el centro dispone de una red de acceso a internet para el alumnado.

En ningún caso el Instituto se responsabilizará de la pérdida, hurto o deterioro de este tipo de dispositivos, correspondiendo a cada alumno/a su guarda y custodia.

7. INTERNET Y REDES SOCIALES

Como ya hemos indicado en apartados anteriores, el IPEP de Córdoba cuenta con acceso gratuito a internet a través de la red del alumnado, facilitando así el uso de dispositivos propios. No obstante, deberíamos tener en consideración algunas cuestiones relacionadas con el uso de internet y las redes sociales, cuestiones que sería aconsejable que observaramos no sólo en el centro, sino en cualquier otro lugar (domicilio, redes públicas, etc.).

El Centro Criptológico Nacional – CCN CERT nos ofrece una serie de consejos que podríamos considerar como “buenas prácticas” en internet y las 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) Ten cuidado a la hora de conectarse en redes WiFi públicas.
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 IPEP Córdoba tiene su página web en la siguiente dirección:
https://blogsaverroes.juntadeandalucia.es/ipepcordoba/
En ella podrás encontrar información importante sobre la enseñanza de adultos, normativa, calendario con las fechas más importantes y enlaces a la página de Educación Permanente de la Junta de Anadalucía, a la Secretaría Virtual, a la Plataforma **Moodle** y a **iPasen**.
También encontrarás tutoriales sobre cómo acceder al Aula Virtual o cómo darte de alta en iPasen, por ejemplo.

b. (i)Pasen

Pasen (o **iPasen** – la app –) es el módulo de Séneca que permite la comunicación entre los centros educativos y las familias, tutores legales y alumnado, ofreciendo una serie de funcionalidades como son la consulta de:

- Datos del centro educativo
- Horario escolar
- Calendario escolar
- Faltas de asistencia
- Calificaciones

Para darte de alta o aprender a utilizar Pasen (o iPasen) puedes consultar el siguiente enlace de nuestra web: **https://blogsaverroes.juntadeandalucia.es/ipepcordoba/tutorial-de-pasen/**

c. Moodle

Las Plataformas Moodle (Presencial o Semipresencial/Distancia) son el lugar donde se encuentran las aulas virtuales de cada materia o ámbito. En ellas encontrarás los materiales y tareas del curso. También encontrarás:

- Actividades evaluables
- Observaciones
- Tablón de anuncios
- Agenda personal
- Mensajería interna
- Recepción de avisos por notificaciones
- Punto de encuentro.

Para más información acerca de Moodle, primer acceso y configuración, consulta el siguiente enlace: **https://blogsaverroes.juntadeandalucia.es/ipepcordoba/tutorial-de-pasen/**

9. PROTECCIÓN DE DATOS

La protección de datos en los centros educativos es una cuestión de vital importancia. Aquí tienes algunas recomendaciones importantes para actuar conforme a la legislación vigente.

a) Los datos del alumnado y del profesorado que constan en el centro son:
   - Identificativos: nombre y apellidos, DNI, domicilio, email, etc.
   - Condiciones personales: discapacidad, enfermedades, intolerancias, tratamientos, informes psicopedagógicos…
   - Escolarización: curso, grupo, estudios previos, calificaciones, asignaturas…

   Ninguno de estos datos podrá usarse para fines diferentes al educativo (función docente y orientadora).

b) Publicación de datos de carácter personal

   No se publicará ningún dato de carácter personal en ningún lugar público, físico o virtual, excepto en los siguientes casos:
   - Listas de admitidos: solo en los tablones de anuncios del centro y en sitios web de acceso restringido (como Moodle o Séneca). Estas listas solo recogerán el resultado final del baremo, no resultados parciales que puedan responder a datos o información sensible.
   - Beneficiarios de becas: en las mismas condiciones. Y si la beca está asociada a una situación de discapacidad o similar, solo se puede publicar el número identificador de la solicitud.

   La publicación de *cualquier* otro dato de cualquier miembro de la comunidad educativa, ya sea en sitios web, en redes sociales o en cualquier otro espacio físico o virtual, deberá contar necesariamente con el consentimiento del afectado.
   Ten presente que la mera transmisión de un nombre, una fotografía o cualquier otro dato personal mediante cualquier medio telemático como Whatsapp o Telegram constituye por sí misma una violación de la legislación vigente. Este tipo de datos (y cualquier otro) solo pueden tratarse en webs de acceso restringido como Moodle o Séneca.

c) Almacenamiento de datos de carácter personal

   Los datos de carácter personal deben almacenarse en lugares debidamente protegidos. Si hablamos de datos digitales, los únicos lugares habilitados para ello son los propios servidores de la Consejería de

Educación y Deporte (es decir, Moodle, Séneca y Pasen), o aquellos pertenecientes a terceros con los que la Consejería haya firmado un acuerdo de colaboración.
Esto significa que no deberías almacenar datos de carácter personal del alumnado en ningún otro lugar, como, por ejemplo, en archivos almacenados en un pendrive, en archivos en la nube o incluso archivos en el disco duro de tu ordenador: cualquier robo o extravío de esa información podría hacer que circulara por la red y tú serías la persona responsable de ello por no haberlos alojado en los lugares adecuados.

d) Captación de imágenes

Es habitual que, durante ciertos eventos como excursiones, talleres, conferencias o celebraciones, se recojan fotografías y vídeos del alumnado y el profesorado.
La toma de imágenes, si la actividad tiene fines educativos, no requiere consentimiento, pero su publicación en cualquier medio físico o virtual, sí. Por lo tanto, el consejo más sensato es recabar siempre el consentimiento de los afectados.

e) Datos sobre resultados académicos

Los resultados académicos también son datos sensibles según la legislación vigente, por lo que no se deben publicar en ningún lugar de acceso público, ya sea físico o virtual. Esta información, puede ser grabada en el sistema Séneca y en Moodle Centros, puesto que son plataformas en las que el acceso se halla restringido y la Consejería de Educación y Deporte asegura la salvaguarda de esos datos.