1 de septiembre de 2020

MEMORANDO

Ref.: 2020-08-M-1-es-1/AB
Orig.: EN
Versión: ES

A: **Directores**
Responsables de Protección de Datos (RPD)
Técnicos informáticos

De: **Andreas Beckmann, Secretario General adjunto**

Asunto: **Carta informática de las Escuelas Europeas**

Estimados colegas:

El Grupo de Trabajo 'Preparación del curso escolar 2020/21' proporcionó, a fines de julio de 2020, un análisis detallado y un conjunto de propuestas y recomendaciones sobre cómo preparar el curso escolar 2020/21 (doc. 2020-07-D-9-en-2).

Este análisis y las propuestas y recomendaciones se han debatido en la reunión extraordinaria del Consejo Superior de 31 de agosto de 2020.

Los miembros del Grupo de Trabajo subrayaron la necesidad de revisar las normas informáticas vigentes en las Escuelas y de establecer para el comienzo del curso escolar 2020/21 una Carta armonizada, la cual debería abordar, por ejemplo, aspectos relativos a la seguridad informática, la protección y privacidad de datos, la propiedad intelectual, el acoso cibernético y la "etiqueta en la red".

Este Memorando incluye en su anexo la Carta informática revisada y armonizada dirigida a los alumnos.

La Carta es el resultado de un proceso de consulta que incluye los servicios legales internos y externos de la Oficina del Secretario General de las Escuelas Europeas (OSG), el Responsable de Protección de Datos de la OSG, el Departamento de Desarrollo Pedagógico, el Departamento de informática y representantes de los Directores y los Responsables de Protección de Datos de las Escuelas.

La Carta informática adjunta sustituirá a las Cartas informáticas vigentes en las Escuelas. Sin embargo, el Director de una Escuela puede decidir que se añadan elementos específicos de la Escuela, sin contradecir los principios generales de la Carta adjunta.

Se invita a las Escuelas a aplicar la Carta informática revisada desde el comienzo del curso escolar 2020/21 y a que la Carta informática revisada sea comunicada a los alumnos, padres y profesores.

La Carta informática será revisada de forma periódica.

Andreas BECKMANN

Secretario General adjunto

Anexo

Carta sobre el uso de recursos y dispositivos informáticos por los alumnos de la Escuela Europea […]

Índice

MEMORANDO 1
1. PREÁMBULO 4
2. RECURSOS Y DISPOSITIVOS INFORMÁTICOS 4
2.1 Definición 4
2.2 Regla de oro 4
2.3 Acceso a los recursos y dispositivos informáticos 4
3. REGLAS GENERALES DE BUEN COMPORTAMIENTO 5
3.1 Comentarios generales 5
3.2 Respeto de la confidencialidad 6
3.3 Respeto de la red y de los puestos de trabajo informatizado 6
3.4 Respeto de los derechos de propiedad intelectual 7
3.5 Respeto por los miembros de la comunidad escolar y por la Escuela 7
4. REGLAS ESPECIALES SOBRE EL USO DE INTERNET 7
4.1 La red de la Escuela 7
4.2 Supervisión y asistencia en una sesión a los alumnos de la Escuela 8
4.3 Redes sociales 8
5. REGLAS ESPECIALES RELATIVAS AL APRENDIZAJE/ENSEÑANZA EN LÍNEA 9
6. INFORMAR AL EQUIPO EDUCATIVO/INFORMÁTICO 9
7. RESPONSABILIDAD 10
8. SANCIONES PREVISTAS 10
9. REVISIÓN 11

1. PREÁMBULO

Las Escuelas Europeas se esfuerzan por ofrecer a los alumnos las mejores condiciones de trabajo posibles en términos de servicios informáticos y multimedia. La presente Carta establece las reglas para el buen uso y buen comportamiento con respecto a los recursos informáticos con finalidad pedagógica a disposición de los alumnos.

La presente Carta constituye un anexo del Reglamento Interno de la Escuela Europea, […] (en lo sucesivo, "la Escuela") y se inscribe en el marco de las leyes y reglamentos vigentes relacionados en particular con los derechos de autor, los derechos de propiedad intelectual, la protección de la privacidad (incluidos, en particular, los derechos de imagen) y el tratamiento de datos personales, así como los delitos informáticos.

2. RECURSOS Y DISPOSITIVOS INFORMÁTICOS

2.1 Definición

Se entiende por ``Recursos y dispositivos informáticos" el conjunto de elementos compuesto por la red de la Escuela, los servidores y estaciones de trabajo, pizarras digitales interactivas, dispositivos periféricos (impresoras, discos duros externos), software, computadoras portátiles y tabletas, uso de Internet en la Escuela y recursos de aprendizaje digital[1] proporcionados por la misma.

2.2 Regla de oro

Los recursos informáticos de la Escuela Europea deberán ser utilizados *únicamente* para realizar actividades pedagógicas.

2.3 Acceso a los recursos y dispositivos informáticos

El acceso a los recursos y dispositivos proporcionados por la Escuela es un privilegio y no un derecho.

[1] De acuerdo con la definición mencionada en el “Procedimiento para la aprobación del uso de un recurso de aprendizaje digital en las Escuelas Europeas” (Anexo del MEMO 2019-12-M-3/GM).

Todos y cada uno de los alumnos deben cumplir escrupulosamente con las condiciones operativas y las reglas para el uso adecuado y el buen comportamiento contenidas en esta Carta.

La Escuela puede realizar verificaciones periódicas u ocasionales para verificar que los recursos y dispositivos informáticos se utilicen de acuerdo con las disposiciones de esta Carta y se reserva el derecho de revocar este privilegio si fuese necesario.

En la Escuela, el acceso a los recursos y dispositivos informáticos se proporciona bajo la responsabilidad de la Dirección de la Escuela y bajo el control de un miembro del equipo educativo.

La Escuela ofrece acceso a diferentes recursos informáticos:

- a los ordenadores de la Escuela mediante el uso de una cuenta personal;
- a la red de la Escuela, que comprende:
  - espacios de almacenamiento en los servidores de la Escuela: espacios compartidos o restringidos a la cuenta personal;
  - impresoras en red;
- los servicios en línea de Office 365 (incluido, en particular, un servicio de correo electrónico/mensajería) gestionados por la Escuela Europea;
- software propietario, con licencia o de código abierto;
- Internet.

Todas las cuentas de acceso que se proporcionan al alumno son personales y solo pueden ser utilizadas por el alumno en cuestión. Por tanto, las claves de acceso deben ser absolutamente confidenciales y no pueden ser divulgadas a terceros (a excepción de los representantes legales del alumno). Antes de abandonar su terminal, el alumno siempre debe asegurarse de cerrar la sesión correctamente.

El alumno informará a su asesor educativo en caso de problema con su cuenta o en caso de pérdida, robo o peligro de sus claves de acceso.

3. REGLAS GENERALES DE BUEN COMPORTAMIENTO

3.1 Comentarios generales

Los alumnos deberán respetar las reglas de buena conducta cuando utilicen los recursos y dispositivos puestos a disposición de la Escuela con fines pedagógicos. Por lo tanto, el acceso a los recursos por un alumno que esté utilizando su propio dispositivo móvil personal en la Escuela (es decir, acceso a la red) o fuera de la Escuela también conlleva el deber de cumplir con esta Carta.

Para uso personal fuera de la Escuela, cada alumno recibirá 5 licencias de instalación de Office 365 para computadoras y/o teléfonos inteligentes y tabletas. Estas licencias pueden ser usadas e instaladas en dispositivos informáticos utilizados regularmente por el alumno y protegidas con contraseña de acuerdo con las reglas generales de buena conducta establecidas en esta Carta.

3.2 Respeto de la confidencialidad

Se prohíbe a los alumnos:

- intentar apropiarse de las contraseñas de otras personas;
- iniciar sesión con los nombres de usuario y contraseñas de otras personas;
- utilizar la sesión abierta de otro usuario sin su permiso explícito;
- abrir, editar o eliminar archivos de otras personas y, en general, intentar acceder a información de terceros sin su permiso;
- guardar una contraseña en software de Internet como Google Chrome, Internet Explorer, Firefox, etc., cuando se utilizan dispositivos no personales.

3.3 Respeto de la red y de los puestos de trabajo informatizado

Se debe mostrar un escrupuloso respeto por las instalaciones y el hardware. Los teclados y ratones de ordenador deben manipularse con cuidado, por lo cual los alumnos no deben comer ni beber cuando utilicen los puestos de trabajo de la Escuela, para evitar deteriorarlos.

Se prohíbe a los alumnos:

- realizar cambios en la configuración de la estación de trabajo;
- cambiar o destruir datos de la red o de la estación de trabajo;
- instalar software o copiar software presente en la red;
- acceder o intentar acceder a recursos distintos a los permitidos por la Escuela;
- abrir mensajes, archivos, documentos, enlaces o imágenes enviados por remitentes desconocidos;
- insertar una unidad extraíble en cualquier dispositivo, sin el permiso de un adulto responsable;
- conectar un dispositivo o medio de almacenamiento (USB, teléfono móvil, otro) sin el permiso de un adulto responsable;
- interferir deliberadamente en el funcionamiento de la red y, en particular, mediante el uso de programas diseñados para introducir programas maliciosos o eludir la seguridad (virus, software espía u otros);
- subvertir o intentar subvertir los sistemas de protección instalados (firewall, programas antivirus, etc.);
- Utilizar túneles VPN[2].

[2] En informática, una **Red Privada Virtual, VPN** según la abreviatura en inglés, es un sistema que permite crear un enlace directo entre ordenadores remotos, aislando el tráfico en una especie de túnel.

3.4 Respeto de los derechos de propiedad intelectual

Se prohíbe a los alumnos:

- descargar o realizar copias ilegales de material (streaming, audio, películas, software, juegos, etc.) protegido por derechos de propiedad intelectual;
- plagiar, es decir, reproducir, (re)difundir, comunicar al público, en cualquier forma, cualquier información, independientemente del medio (tabla, gráfico, ecuación, artículo de un acto jurídico, imagen, texto, hipótesis, teoría, opinión, etc.), que puedan estar protegidos por derechos de propiedad intelectual (derechos de autor, etc.).

El uso de la información que se encuentra en Internet para el trabajo de clase implica que las fuentes deben ser incluidas y correctamente citadas por el alumno, que podrá recabar la ayuda de uno de los miembros del equipo educativo a tal efecto.

3.5 Respeto por los miembros de la comunidad escolar y por la Escuela

Se prohíbe a los alumnos:

- exhibir en la pantalla documentos, publicar documentos o participar en intercambios de naturaleza difamatoria, abusiva, extremista, pornográfica o discriminatoria, ya sea por motivos de origen racial o étnico, opiniones políticas, religión o creencias filosóficas, estado de salud u orientación sexual;
- intimidar a otras personas (ciberacoso), en su propio nombre o utilizando una identidad falsa o un seudónimo;
- utilizar listas de direcciones de correo electrónico o datos personales de otras personas para fines distintos de los previstos por los objetivos pedagógicos o educativos;
- utilizar expresiones inadecuadas en correos electrónicos, publicaciones, chats o cualquier otro medio de comunicación (el autor del mensaje es el único responsable del contenido enviado);
- dañar la reputación de un miembro de la comunidad escolar o de la Escuela, en particular mediante la difusión de textos, imágenes y/o videos;
- celebrar contratos, vender o publicitar de cualquier forma en nombre de la Escuela, salvo que el proyecto haya sido previamente aprobado por la Dirección de la Escuela.

4. REGLAS ESPECIALES SOBRE EL USO DE INTERNET

4.1 La red de la Escuela

El acceso a Internet dentro de la Escuela Europea es un privilegio y no un derecho.

El uso de la red pedagógica con base en Internet tiene como único fin las actividades de enseñanza y aprendizaje correspondientes a los cometidos de las Escuelas Europeas.

Se prohíbe estrictamente a los alumnos:

- conectarse a servicios de chat en vivo o foros de discusión a menos que un miembro del equipo educativo lo autorice específicamente, por un motivo pedagógico, o a las redes sociales;
- compartir información personal que permita la identificación del alumno (nombre, apellido(s), correo electrónico, dirección, etc.);
- acceder a sitios pornográficos, xenófobos, antisemitas o racistas;
- descargar o instalar cualquier programa.

En ningún caso los alumnos deben mencionar su nombre, mostrar una foto, mencionar su dirección, número de teléfono o cualquier otro dato que facilite su identificación en Internet.

Los alumnos tienen prohibido utilizar la dirección de correo electrónico vinculada a su cuenta de O365 (…@student.eursc.eu) para crear cuentas en aplicaciones, sitios web o software no autorizados por un miembro del equipo educativo o por la Dirección de la Escuela.

4.2 Supervisión y asistencia en una sesión a los alumnos de la Escuela

La Escuela utilizará un sistema de supervisión y asistencia para garantizar que los alumnos participen en un proceso de aprendizaje continuo y permitir que las personas responsables del curso en cuestión y el personal de la biblioteca ayuden a los alumnos directamente desde su puesto de trabajo.

Solo las personas autorizadas por la Administración podrán utilizar el software de supervisión y asistencia y deben cumplir con la Carta informática aplicable a su función en la Escuela.

Este sistema permite:

- acceder a las pantallas de los alumnos de forma remota para ayudarlos y mantenerlos concentrados en sus tareas.
- enseñar para ser más eficaz, mostrando a la clase la pantalla del responsable de impartir la lección;
- seleccionar las pantallas de los alumnos para presentar su trabajo;
- desactivar todas las pantallas de los alumnos para captar su atención.

No se realizará ninguna grabación de la sesión ni de la actividad.

4.3 Redes sociales

Se prohíbe a los alumnos conectarse a las redes sociales con la dirección de correo electrónico vinculada a su cuenta de O365 (…@student.eursc.eu).

El uso de un dispositivo digital privado (teléfono, tableta, computadora portátil) no exime a los alumnos de seguir las reglas de uso adecuado y buen comportamiento establecidas en esta Carta, por lo que se refiere al respeto a los miembros de la comunidad escolar y a la Escuela. Los alumnos serán responsables del contenido mostrado.

5. REGLAS ESPECIALES RELATIVAS AL APRENDIZAJE/ENSEÑANZA EN LÍNEA

El aprendizaje o la enseñanza en línea implican seguir las reglas de buen uso y buen comportamiento que establece la presente Carta, en los siguientes contextos:

- Aprendizaje en línea o enseñanza en la Escuela ("aprendizaje combinado"), lo que implica el uso de recursos de aprendizaje digitales aprobados por la dirección de la Escuela o la participación en actividades asincrónicas en línea (deberes).
- Enseñanza o aprendizaje remoto en línea ("aprendizaje a distancia"), cuando se suspenden las lecciones presenciales en la Escuela.
- Enseñanza o aprendizaje en línea a distancia y presencial ("aprendizaje híbrido"), cuando algunos alumnos asistan a las lecciones de forma presencial y otros a distancia.

Además, se prohíbe lo siguiente:

- fotografiar y/o filmar, por medio de dispositivos personales, a profesor(es) y alumno(s) que participen en el aprendizaje en línea y, a fortiori, publicar tales imágenes/videos;
- participar en sesiones de enseñanza o aprendizaje en línea a cuya asistencia el alumno no haya sido invitado expresamente;
- invitar a los participantes a sesiones de enseñanza o aprendizaje en línea sin el consentimiento de la persona que organiza la sesión;
- utilizar recursos de aprendizaje digitales para intimidar, acosar, difamar o amenazar a otras personas.

Los derechos de imagen son derechos reconocidos a cada uno de los miembros de la comunidad escolar, por lo que la Escuela no tolerará el uso de imágenes/videos tomados sin el conocimiento de las personas implicadas.

6. INFORMAR AL EQUIPO EDUCATIVO/INFORMÁTICO

El alumno se compromete a informar a un miembro del equipo educativo y/o informático (asesor educativo, coordinador informático, profesor, etc.), cuanto antes con respecto a:

- cualquier software o dispositivo sospechoso;
- cualquier pérdida, robo o puesta en peligro de su información de autenticación;
- cualquier mensaje, archivo, documento, enlace o imagen enviados por un remitente desconocido.

7. RESPONSABILIDAD

El daño intencional a los dispositivos y recursos informáticos de la Escuela puede conllevar gastos de reparación para los representantes legales de los alumnos afectados, de acuerdo con el artículo 32 del Reglamento General de las Escuelas Europeas.

Cualquier alumno que opte por llevar un teléfono móvil u otro dispositivo electrónico a la Escuela, lo hará bajo su propio riesgo y será personalmente responsable de la seguridad de su teléfono o dispositivo móvil.

Sin perjuicio de las excepciones previstas cuando los alumnos deban llevar un dispositivo a la Escuela para los fines del programa BYOD, la Escuela no aceptará responsabilidad alguna por la pérdida, robo, daño o vandalismo de un teléfono o cualquier otro dispositivo, o por el uso no autorizado del mismo.

8. SANCIONES PREVISTAS

Cualquier alumno que contravenga las reglas establecidas anteriormente será responsable de soportar las medidas disciplinarias previstas por el Reglamento General de las Escuelas Europeas y el Reglamento Interno de la Escuela y las sanciones y procedimientos penales previstos por la ley.

Todos los miembros del equipo educativo deben comprometerse a garantizar que tales disposiciones sean respetadas por los alumnos sometidos a su responsabilidad y deben ejercer un control riguroso al respecto.

El administrador informático debe asegurarse constantemente de forma satisfactoria de que los recursos informáticos funcionen correctamente y se utilicen adecuadamente. Para ello, la monitorización de los recursos y dispositivos informáticos permite detectar anomalías (uso anormal de la red, exceso de espacio de almacenamiento, intento de ciberataque, etc.). En caso de detectarse anomalías, el administrador informático se dirigirá a la Dirección de la Escuela para acordar las medidas pertinentes. Sin embargo, en casos de emergencia absoluta y para proteger el sistema informático de la Escuela, el administrador informático puede tomar la decisión inmediata de bloquear el acceso informático a uno o más alumnos y luego remitirá el asunto de inmediato a la Dirección.

Este tipo de intervención solo se puede realizar de acuerdo con finalidades claramente definidas, a saber:

- prevención de acciones ilegales o difamatorias, acciones contrarias a las normas aceptadas de buen comportamiento o que puedan atentar contra la dignidad de otras personas;

- protección de los intereses económicos o financieros de las Escuelas, a los que se adjunta la confidencialidad;
- seguridad y/o funcionamiento técnico fluido de los sistemas informáticos, incluido el control de los costos relacionados y la protección física de las instalaciones de la Escuela;
- cumplimiento de buena fe de los principios y reglas de uso de las tecnologías disponibles y de la presente Carta.

9. REVISIÓN

Esta Carta se revisará de acuerdo con las experiencias obtenidas en el curso escolar 2020/21.