eSafety Label - !action_plan_for! IES San José

!assessment_form_submitted_by! Miguel Garcia - 2015-05-07 12:55:32

!action_plan_intro!

Infraestructura

Seguridad técnica

- Tener los entornos de enseñanza y de administración juntos puede entrañar un riesgo de seguridad. El centro escolar debe garantizar la seguridad de los datos personales de profesores y alumnos es un papel fundamental del centro escolar. Le recomendamos que su coordinador TIC o responsable de seguridad digital en el centro, junto con el personal y un experto técnico, definan e implementen una estrategia para separar los entornos de enseñanza y de administración o bien aseguren el nivel de seguridad más alto posible entre ellos. Consulte la hoja informativa sobre *protección de información confidencial en los centros educativos* en www.esafetylabel.eu/group/teacher/protecting-sensitive-data.
- Tiene niveles de filtros diferenciados en su centro educativo. Es un buen protocolo. Un buen reglamento necesita actualizarse de forma regular. ¿Actualizan el suyo periódicamente? ¿Con qué frecuencia se solicita el bloqueo o desbloqueo de sitios web? Evalúe periódicamente si es adecuado para el objetivo marcado y si involucra a todos los grupos de interés en este proceso.
  Además, tenga en cuenta que adoptar un enfoque educativo y hacer que los alumnos de todas las edades se formen con mayor flexibilidad y adaptación es también fundamental para un uso de Internet seguro y responsable. De este modo, todos los profesores podrán reflexionar sobre el modo de dirigirse a los alumnos a la hora de explicarles cómo ser un buen ciudadano digital con seguridad. Consulte www.paneuyouth.eu para ver ejemplos de conversaciones que pueden mantener lugar en el aula sobre el tema, a través de juegos de roles y en grupo.

Acceso de profesores y estudiantes a la tecnología

- Todo el personal y los alumnos pueden utilizar sus memorias USB en el centro educativo. Es una buena práctica y su Reglamento de Uso Aceptable debería estipular que todos los dispositivos extraíbles se comprobarán antes de ser utilizados en los equipos informáticos del centro. Consulte la hoja informativa sobre *Uso de dispositivos extraíbles* en www.esafetylabel.eu/group/teacher/removable-devices para asegurarse de que cumple con todos los aspectos de seguridad.
- Es positivo que en su centro las aulas de informática se puedan reservar con facilidad. Contemplen la posibilidad de incluir otros dispositivos digitales en las aulas, ya que su uso proporciona al alumnado la mejor práctica para tratar con las nuevas tecnologías. Asegúrense de que se aborden también temas relacionados con la seguridad.

Protección de datos

- Posee una buena política al mantener los entornos de enseñanza y de administración separados. Así se garantiza actualizar la formación del profesorado en la gestión de estos entornos y a su vez permite seguir examinando el reglamento escolar. Suba en su perfil escolar el reglamento junto con el certificado de seguridad digital.
- Sus nuevos usuarios reciben una contraseña estándar y se les pide que pongan su propia contraseña la primera vez que acceden. Las contraseñas facilitan puntos de acceso únicos al sistema informático del centro educativo, por lo que deben respetarse rigurosamente algunas normas básicas. Para más información, consulte la hoja informativa sobre *Contraseñas seguras* en www.esafetylabel.eu/group/teacher/safe-passwords.
  Incluya estas normas en su Reglamento de Uso Aceptable y evite dar a los nuevos usuarios una contraseña

estándar de "nuevo acceso".

Licencias de software

- Es importante asegurarse de que todos los nuevos miembros del centro conocen los procesos válidos para la instalación de software. Esto significa que se puede mantener la seguridad de los sistemas y que el personal puede probar nuevas aplicaciones de software que contribuirán a la enseñanza y al aprendizaje.
- El cumplimiento de los acuerdos de concesión de licencias es importante. Alguien tiene que asumir la responsabilidad general para garantizar que eso se cumple y que todas las licencias son válidas para los objetivos del centro. Se debe comunicar a todo el personal quién es la persona responsable.
  El apartado sobre el Contrato de licencia de usuario final en Wikipedia le permitirá conocer los términos y condiciones y comparar los contratos de software.

Gestión de las TIC

- Es una buena práctica que la persona responsable de la red TIC esté informada sobre qué software está instalado en el hardware del centro y esto debe quedar claramente reflejado en el Reglamento escolar y el Reglamento de Uso Aceptable. La persona responsable de la red tiene que ser capaz de garantizar la conformidad con los requisitos de licencia y que el nuevo software no interferirá en el funcionamiento de la red.
- En su centro hay un procedimiento establecido que permite a cualquiera de los miembros del personal realizar una solicitud de adquisición de hardware o software nuevo. Esta solicitud conlleva la toma de una decisión informada dentro de un plazo razonable. Esto es estupendo, ya que permite a los docentes beneficiarse de las ventajas de las nuevas tecnologías y a la vez respetar el Reglamento escolar del centro.

Reglamento

Reglamento de uso aceptable (RUA)

- Es esencial que todos los centros educativos cuenten con un Reglamento de Uso Aceptable (RUA) para todo el personal y alumnos. Elabore un RUA de forma urgente junto con todas las partes interesadas. Consulte la hoja informativa y la ficha de evaluación sobre el *Reglamento de Uso Aceptable* en www.esafetylabel.eu/group/teacher/acceptable-use-policy.
- Revise de forma regular el Reglamento sobre teléfonos móviles para asegurarse de que encaja en los objetivos y que se aplica con firmeza en todo el centro educativo. Las hojas informativas sobre *Uso de teléfonos móviles en el centro educativo* (www.esafetylabel.eu/group/teacher/mobile-phones) y *Reglamento escolar* (www.esafetylabel.eu/group/teacher/school-policy) le proporcionarán información útil acerca de este tema.

Gestión de incidentes

- ¿Todo el personal conoce el procedimiento para tratar con material que pudiera ser ilegal? ¿Hay una persona del equipo directivo designada para asumir la responsabilidad general en este tipo de situación? El procedimiento debe ser comunicado de forma clara a todo el personal del centro educativo, y a los profesores y alumnos, a través del Reglamento de Uso Aceptable del centro. Recuerde que debe informar acerca de cualquier contenido ilegal a su línea directa INHOPE nacional (www.inhope.org).
- Mantenga un registro central de cualquier incidente relacionado con el ciberacoso que pueda ayudar a informar al personal sobre el alcance de los posibles problemas y el tipo de alumno, edad, etc., que se están viendo afectados. También hay que asegurarse de cumplimentar el Formulario de gestión de incidentes del Certificado de seguridad digital. Su aportación contribuirá a la elaboración de una base de datos sobre prácticas exitosas de gestión de incidentes procedentes de centros educativos de toda Europa y que puede ser de utilidad para el futuro.

Práctica/comportamiento del profesorado

- Tiene que haber un código de conducta para los profesores para que tengan claro qué tipo de comportamiento es aceptable cuando se conectan a Internet. Esto debe ser comunicado de forma clara a todo el personal a través del Reglamento escolar y a los profesores y alumnos a través del Reglamento de Uso Aceptable. Revise y actualice ambos reglamentos siempre que sea necesario.

- El uso de teléfonos móviles personales en clase puede implicar cierto tipo de riesgos. Considere por qué el personal tendría que utilizar sus dispositivos y, en su caso, considere la posibilidad de ofrecer uno propio del centro. Invite al personal a leer la hoja informativa sobre *Uso de teléfonos móviles en el centro educativo* (www.esafetylabel.eu/group/teacher/mobile-phones) y asegúrese de que las directrices para el personal se comunican de forma clara en el reglamento escolar.

Práctica/comportamiento del alumnado

- Las directrices de comunicación electrónicas para los alumnos deben transmitirse de forma clara en el Reglamento de Uso Aceptable. La comunicación entre alumnos puede empeorar rápidamente si no se establecen unas normas, dando lugar a incidentes como el ciberacoso. Aprender sobre comunicación práctica y responsable también debería formar parte del plan de estudios, ya que se trata de una competencia necesaria en la vida de cada joven. Es conveniente abordar el tema en una reunión de profesores para establecer las normas que se quieran aplicar.
- Your school partly has a school wide approach of positive and negative consequences for pupil behaviour. This is a good start, make sure that the policy and associated hierarchy applies to all on- and offline issues and is shared widely and re-visited by all staff and pupils at least annually.

Presencia del centro en la red

- Eche un vistazo a la hoja informativa sobre *Tomar y publicar fotografías y vídeos en el centro educativo* (www.esafetylabel.eu/group/teacher/photos-videos) para comprobar que el reglamento de su centro educativo cubre todas las áreas. Después, suba esta sección de su reglamento a su página de perfil a través de Mi área escolar para que otros centros educativos puedan tomarlo como referencia.
- Controle de forma regular la presencia online del centro en las redes sociales para asegurarse de que no hay contenidos inapropiados. Establezca un proceso para mantener el sitio/página actualizado y revise la hoja informativa sobre *Centros educativos en redes sociales* (www.esafetylabel.eu/group/teacher/social-networks) para obtener más información y asegurarse de que sigue las directrices de buenas prácticas. Pida información a las partes interesadas sobre la utilidad del perfil.

Práctica

Gestión de la seguridad digital

- En su centro educativo, los profesores son responsables de la actividad online de sus alumnos. Deben aplicarse muchos controles y análisis de herramientas de auditoría sobre la seguridad de red y la privacidad de los usuarios para garantizar la seguridad de sus alumnos y de las redes del centro y todos ellos deben estar reflejados en el Reglamento escolar. Consulte la hoja informativa sobre *Reglamento escolar* en www.esafetylabel.eu/group/teacher/school-policy.
  Para garantizar que esto se aplica de la forma más eficiente y regular posible, aconsejamos que el director del centro nombre a un miembro de los profesores para encargarse de la seguridad digital. Esta persona será responsable de comprobar que todos los aspectos incluidos en el Reglamento son debatidos y tratados con los demás profesores, así como con los alumnos.
  Para asegurarse de que todo el personal del centro, los alumnos y los padres están informados de sus derechos y responsabilidades online, consulte la hoja informativa sobre *Reglamento de Uso Aceptable* (www.esafetylabel.eu/group/teacher/acceptable-use-policy).
- Hay que asegurarse de que el responsable o el miembro de la dirección que haya sido nombrado para ocuparse de la seguridad digital tiene la posibilidad de recibir formación de forma regular y de que los compañeros de trabajo también tienen conocimiento de estos aspectos de seguridad digital. Es bueno que la dirección se implique en la elaboración y revisión periódica del Reglamento escolar. Consulte la hoja informativa sobre el *Reglamento escolar* www.esafetylabel.eu/group/teacher/school-policy.

La seguridad digital en el plan de estudios

- La seguridad digital debe integrarse en el plan de estudios sea o no una obligación legal en su país. Existen protocolos de trabajo muy buenos disponibles de forma gratuita que podrían ser de utilidad Para más información, consulte la hoja informativa de *Integración de la seguridad digital en el plan de estudios* en www.esafetylabel.eu/group/teacher/esafety-in-curriculum.

- Asegúrese de que el plan de estudios sobre seguridad digital esté al día con los aspectos más recientes. Utilice para ello todos los recursos disponibles y asegúrese de que se basa en un aprendizaje anterior. Tenga en cuenta además que los alumnos necesitarán un mensaje distinto en función de cómo utilicen la tecnología.

Atividades extracurriculares

- Es bueno que los alumnos reciban orientación sobre seguridad digital fuera del horario del plan de estudios cuando lo soliciten. Hay que sopesar ofrecerles orientación para abordar aspectos relacionados con la seguridad digital. Puede ser útil facilitarles algún tipo de "consultorio" que ayude a los alumnos a configurar su privacidad en Facebook, etc. El portal del Certificado de seguridad digital ofrece recursos útiles sobre este tema: échele un vistazo a la hoja informativa sobre el *Uso de la tecnología fuera del aula por parte de los alumnos* en www.esafetylabel.eu/group/teacher/social-media-pupils.
- Trate de implicar a los alumnos para que colaboren entre ellos y facilíteles las oportunidades necesarias para que compartan sus ideas y conocimientos con los compañeros. Además, también puede consultar la sección de recursos del portal del Certificado de seguridad digital para obtener más ideas y recursos.

Fuentes de ayuda

- Todo el personal debería tener algo de responsabilidad en el campo de la seguridad digital. Orientadores, personal sanitario, etc., pueden ofrecer asesoramiento y orientar sobre estos aspectos y se les debería invitar a que contribuyeran al desarrollo y revisión periódica del reglamento. Se debe sopesar si sería conveniente que estos empleados recibieran algún tipo de formación.
- Es bueno que se proporcione orientación sobre seguridad digital a los padres cuando lo soliciten. Considere la posibilidad de informar de forma regular a los padres a través del sitio web del centro educativo y enviando enlaces en el boletín de noticias del centro. Podría organizarse una reunión informativa de tarde para los padres. Consulte la hoja informativa *Información para padres* en www.esafetylabel.eu/group/teacher/info-for-parents para encontrar recursos que podrían compartirse con los padres e ideas para las reuniones con ellos.

Formación del personal

- Todo el personal debe estar al día sobre las nuevas tendencias que surgen en temas de seguridad digital. Considere la posibilidad de realizar un análisis de necesidades para determinar quién necesita formación y consulte el portal de Certificado de seguridad digital para ver las sugerencias sobre cursos de formación en www.esafetylabel.eu/group/teacher/esafety-training-courses.
- All teachers should be able to recognise signs of cyberbullying and be aware on how to best proceed. Make sure that your teachers are regularly trained bearing in mind the rapid changes of new technology. Also check the eSafety fact sheet on *Cyberbullying* at www.esafetylabel.eu/group/teacher/cyberbullying.

!action_plan_conclusion!