MAGNO International School, Alicante
an Orbital Education School

Política de seguridad en línea

Aprobado por:	Administrador de Soporte Informático Óscar Morell Directora del Colegio Rosa Tortosa	**Fecha:** 16/09/2025
Última revisión el:	Septiembre 2025	

Próxima revisión antes de:	Septiembre 2026

Contenido

Desarrollo / Seguimiento / Revisión de esta Política

Esta política ha sido desarrollada por un grupo de trabajo compuesto por:

- Directores / Líderes Senior
- Oficial / Coordinador de seguridad en línea
- Personal (profesores, personal de apoyo, personal técnico)
- Director Regional de Escuelas / Junta
- Padres
- Representantes estudiantiles

Cronograma de Desarrollo / Monitoreo / Revisión:

- Aprobación: Por la Junta Directiva el 31/07/2025
- Monitoreo: Por el Equipo de Liderazgo Senior al menos una vez al año
- Informes: Anualmente al Director Regional de Escuelas y a la Junta, con informes inmediatos de incidentes graves
- Revisión: Anualmente o según sea necesario en función de nuevos desarrollos o incidentes de RHoS en nombre de la junta

Alcance de la Política

En el marco de la LOE/LOMLOE, los equipos de dirección escolar están facultados para garantizar la convivencia dentro de la escuela y regular el comportamiento de los estudiantes, incluso fuera de la escuela, cuando está vinculado a la vida escolar. El Real Decreto 732/1995 sobre derechos y deberes de los estudiantes establece que los centros educativos pueden aplicar medidas correctoras contra conductas que menoscaben la convivencia, incluido el ciberacoso.

El Plan de Convivencia y el Reglamento de Régimen Interno deben plasmar estas actuaciones, en línea con la normativa autonómica. Además, la LOPIVI (Ley Orgánica 8/2021) y la Ley Orgánica 1/1996 de Protección Jurídica del Menor obligan a los centros educativos a velar por el bienestar de los menores también en el entorno digital.

El colegio actuará de acuerdo con sus Políticas de Convivencia, Uso Responsable de la Tecnología y Antibullying, e informará a las familias cuando se identifique un comportamiento inapropiado en línea fuera del colegio.

Si un alumno es remitido a un recurso externo o a un centro de educación alternativo, la escuela sigue siendo responsable de la protección del alumno. Por lo tanto, debe garantizar que la institución cumpla con los requisitos de protección infantil y cuente con las medidas de seguridad digital adecuadas, con confirmación por escrito de los controles realizados al personal y los controles aplicados.

Tipos de riesgos

- La amplitud de los problemas clasificados dentro de la seguridad en línea es considerable y está en constante evolución, pero se puede clasificar en cuatro áreas de riesgo:
- **Contenido:** estar expuesto a contenido ilegal, inapropiado o dañino, por ejemplo: pornografía, racismo, misoginia, autolesiones, suicidio, antisemitismo, radicalización, extremismo, información errónea, desinformación (incluidas noticias falsas) y teorías de conspiración.
- **Contacto:** ser objeto de una interacción dañina en línea con otros usuarios; por ejemplo: presión entre pares, publicidad comercial y adultos que se hacen pasar por niños o adultos jóvenes con la intención de prepararlos o explotarlos con fines sexuales, delictivos, financieros o de otro tipo.
- **Conducta:** comportamiento en línea que aumenta la probabilidad de daño o lo causa; por ejemplo, hacer, enviar y recibir imágenes explícitas (por ejemplo, compartir desnudos y semidesnudos y/o pornografía de forma consensuada y no consentida, compartir otras imágenes explícitas y acoso en línea, y
- **Comercio:** riesgos como juegos de azar en línea, publicidad inapropiada, phishing o estafas financieras. Si cree que sus alumnos, estudiantes o personal están

Contenido de IA

La expectativa es que

- Se impide de manera efectiva y confiable que los usuarios generen o accedan a contenido dañino e inapropiado
- Los estándares de filtrado se mantienen de manera efectiva durante la duración de una conversación o interacción con un usuario
- El filtrado se ajustará en función de los diferentes niveles de riesgo, edad, idoneidad y necesidades del usuario, por ejemplo, usuarios con necesidades educativas especiales y discapacidades (SEND)
- El contenido multimodal se modera de manera efectiva, incluida la detección y el filtrado de contenido prohibido en varios idiomas, imágenes, errores ortográficos comunes y abreviaturas
- **Las capacidades completas de moderación de contenido se mantienen independientemente del dispositivo utilizado, incluido el uso de dispositivos propios (BYOD) y teléfonos inteligentes al acceder a productos a través de una cuenta institucional educativa**
- El contenido se modera en función de una comprensión contextual adecuada de la conversación, lo que garantiza que el contenido generado sea sensible al contexto
- El filtrado debe actualizarse en respuesta a tipos nuevos o emergentes de contenido dañino, consulte la política de IA escolar para obtener más información.

Funciones y responsabilidades

Todos los roles, incluidos los invitados externos, deben leer y aceptar la política de uso aceptable antes de acceder y utilizar los sistemas y redes locales y en línea de las escuelas. Las siguientes responsabilidades de seguridad en línea se aplican a los roles en el grupo, como se detalla a continuación:

Junta Directiva

- Aprobación de la política de seguridad en línea
- Revisión de la eficacia de la política en función de los comentarios del RHoS

Director Regional de Escuelas (RHoS)

- Asumir el papel de miembro de la junta operativa de seguridad en línea, que incluye:
    - Reunión periódica con el Coordinador de Seguridad en Línea/Líder de Salvaguardia Designado/Director
    - Aprueba y revisa cualquier cambio en la política
    - Monitorea incidentes e informes de seguridad en línea
    - Reportar a la junta de Incidentes

Directores y Líderes Sénior

- Garantizar la seguridad de la comunidad escolar
- Asegúrese de que exista una autoridad / poder comparable bajo la legislación del país anfitrión
- Asegúrese de que exista un sistema para monitorear, informar y recibir informes de incidentes del oficial de seguridad en línea / Líder
- Delegar las responsabilidades diarias de seguridad en línea al Oficial de Seguridad en Línea / Líder de Protección Designado (DSL)
- Asegurarse de que todo el personal reciba la capacitación adecuada

Oficial de seguridad en línea / Líder (DSL o DDSL)

- Lidera el Grupo de Seguridad en Línea
- Gestiona los incidentes de seguridad en línea del día a día y mantiene el registro de incidentes *(se puede proporcionar una muestra de uno si es necesario)*
- Revisa el proceso y la política y sugiere mejoras o incumplimiento al equipo de liderazgo
- Proporciona formación y asesoramiento a todo el personal

- Sirve de enlace con el personal técnico y las autoridades externas

Gerente de red / TI / Personal técnico

- Se mantiene actualizado sobre la capacitación y la política de seguridad en línea
- Garantiza la seguridad del acceso físico de la infraestructura técnica de la escuela
- Implementa y supervisa las medidas de seguridad en línea y garantiza que estén actualizadas, incluida la protección antivirus y de cortafuegos
- Garantiza que toda la tecnología relacionada con el acceso en línea esté protegida de acuerdo con las regulaciones locales y la política y las líneas de base de seguridad en línea
- Garantiza que los proveedores externos contratados sigan las medidas de seguridad en línea y sean plenamente conscientes del proceso de las escuelas antes de trabajar en la escuela *(esto debe hacerse durante la inducción / incorporación al inicio del contrato)*
- Garantiza que todas las plataformas de mensajería y colaboración sean monitoreadas para detectar un uso indebido y, en caso de un incidente, informar al Oficial de Seguridad en Línea y al equipo de liderazgo sénior para su investigación.
- Garantiza que el acceso físico a los sistemas informáticos esté restringido al nivel adecuado y que los usuarios tengan derechos de acceso claramente definidos, incluido el almacenamiento en línea y extraíble, los sistemas de datos del personal y los estudiantes, los datos de la organización y el acceso a Internet.
- Garantiza que todos los estudiantes y el personal reciban un nombre de usuario y una contraseña que cumplan con los estándares de seguridad descritos en la política de contraseñas. Y que no se utilizan cuentas de usuario genéricas en ningún sistema escolar.
- Se asegura de que todos los nombres de usuario y contraseñas de administrador maestro se almacenen en una bóveda cifrada a la que la entidad principal tenga acceso en caso de emergencias para la continuidad del negocio.
- Garantiza que todas las licencias de software estén actualizadas y cubran el número de puestos / dispositivos en uso en la escuela.
- Garantiza que todo el acceso a Internet se filtre a la edad y el nivel de rol apropiados en la escuela y que el firewall y las puertas de enlace de seguridad estén actualizados y que los controles de seguridad reflejen los controles de protección descritos en la política de controles de protección.
- Apoyar al Oficial de Seguridad en Línea para garantizar que exista un sistema para monitorear, registrar e informar sobre incidentes de seguridad en línea.

- Asegura que la política de uso aceptable esté disponible para el personal, los estudiantes, los padres y los colaboradores de terceros y se aplique antes de que se otorgue acceso a los sistemas y redes escolares.
- Realizar una evaluación de riesgos cibernéticos anualmente y revisar cada término
- Desarrolle e implemente un plan para hacer una copia de seguridad de sus datos y revisarlos cada año
- Reportar todos los ataques cibernéticos

Personal docente y de apoyo

- Manténgase actualizado sobre asuntos de seguridad en línea
- Integrar la seguridad en línea en el plan de estudios
- Asegúrese de que hayan leído la política de seguridad en línea y la Política de uso aceptable
- Monitorear y guiar el uso de las tecnologías digitales por parte de los estudiantes
- En caso de observar algún uso indebido, informe al Oficial de Seguridad en Línea y al equipo de liderazgo superior para su investigación
- Asegurar que todas las comunicaciones con los alumnos y padres se lleven a cabo en los sistemas Escolares Oficiales y que las conversaciones sean siempre de carácter profesional
- Asegúrese de que los estudiantes comprendan la política de seguridad en línea y cómo evitar el plagio y la infracción de derechos de autor
- En las lecciones en las que el uso de Internet está planificado previamente, los estudiantes deben ser guiados a sitios verificados como adecuados para su uso y que existen procesos para tratar cualquier material inadecuado que se encuentre en las búsquedas en Internet
- Monitorear el uso de tecnologías digitales, dispositivos móviles, cámaras, etc. en las lecciones y otras actividades escolares (donde esté permitido) e implementar las políticas actuales con respecto a estos dispositivos.

Estudiantes

- Utilizar los sistemas de tecnología digital de la escuela de forma responsable siguiendo la política de uso aceptable
- Denunciar el uso indebido o materiales inapropiados
- Comprenda la política de seguridad en línea y la política de uso aceptable.
- Siga las pautas sobre buenas prácticas, tomar imágenes de manera segura, uso apropiado del teléfono móvil y comprender el acoso en línea.

Padres

- Apoyar las políticas de seguridad en línea de la escuela
- Monitorear las actividades en línea de sus hijos
- Comprenda la importancia de una buena seguridad en línea y cómo se ve
    - Imágenes digitales de fotos y videos en y alrededor de los eventos escolares
    - Acceso seguro y orientación para compartir en las secciones de los padres de las plataformas de aprendizaje y los registros de estudiantes en línea
    - Buen uso de dispositivos personales (donde esté en la escuela)

Educación y Capacitación

Si bien la regulación y las medidas técnicas son importantes, es esencial educar a los estudiantes para que actúen de manera responsable en línea. La seguridad en línea y la alfabetización digital son partes clave de la provisión de la escuela, ya que ayudan a los estudiantes a reconocer los riesgos y desarrollar resiliencia. La seguridad en línea debe integrarse en todo el plan de estudios, con el personal reforzando los mensajes clave. El plan de estudios para la seguridad en línea debe ser amplio, apropiado para la edad y ofrecer progresión a través de oportunidades de aprendizaje creativas, adaptadas a la estructura de la escuela y los grupos de edad de los estudiantes.

Educación de los estudiantes

Para garantizar un enfoque coherente y eficaz de la seguridad en línea, la escuela implementará las siguientes medidas:

- **Entrega del plan de estudios:** Se impartirá un plan de estudios estructurado de seguridad en línea a través de Computación, PSHE y otras materias relevantes, con refuerzo regular.
- **Mensajes para toda la escuela:** Los mensajes clave de seguridad en línea se integrarán en asambleas, tutoriales y programas pastorales.
- **Pensamiento crítico:** Se enseñará a los estudiantes a evaluar críticamente el contenido en línea y verificar su precisión.
- **Responsabilidad digital:** Las lecciones incluirán orientación sobre el reconocimiento de fuentes y el respeto de los derechos de autor.
- **Resiliencia a la radicalización:** Los estudiantes recibirán apoyo para desarrollar resiliencia a través de discusiones seguras sobre temas controvertidos y comprender la participación cívica en lugar del extremismo.
- **Uso aceptable:** Los estudiantes serán educados sobre la importancia de la Política de uso aceptable y se les alentará a usar la tecnología de manera responsable dentro y fuera de la escuela.

- **Modelo a seguir del personal:** El personal modelará el uso apropiado de las tecnologías digitales, Internet y los dispositivos móviles.
- **Prácticas de navegación segura:** En el uso de Internet planificado previamente, los estudiantes serán dirigidos a sitios web examinados y se implementarán procedimientos para administrar la exposición a contenido inadecuado.
- **Monitoreo:** Cuando los estudiantes tienen acceso abierto a Internet, el personal monitoreará activamente su actividad.
- **Acceso a contenido restringido:** para fines educativos legítimos (por ejemplo, investigación sobre racismo, drogas, discriminación), el personal puede solicitar acceso temporal a sitios bloqueados. Dichas solicitudes deben ser auditables y justificadas, utilizando una plantilla disponible en Orbital.

Educación y participación de los padres

Los padres desempeñan un papel vital en la orientación y el seguimiento del comportamiento en línea de sus hijos, pero muchos pueden desconocer los riesgos o cómo responder a las preocupaciones de seguridad en línea. Para apoyar a los padres, la escuela proporcionará información periódica y creará conciencia a través de:

- Actividades relacionadas con el plan de estudios
- Comunicaciones (por ejemplo, cartas, boletines, sitio web, plataforma de aprendizaje)
- Sesiones y eventos para padres
- Campañas como el Día de Internet Seguro
- Señalización de recursos confiables (por ejemplo, saferinternet.org.uk, childnet.com)
- Se le proporciona información y recursos para apoyar la seguridad en línea en el hogar

Educación y participación del personal / voluntarios

- Recibir capacitación formal y auditada en seguridad en línea como parte de su plan de capacitación obligatoria y CPD
- Nuevo personal capacitado como parte de su inducción, completado dentro de las primeras 3 semanas
- Se le pedirá que revise y acepte formalmente las políticas de seguridad en línea y otras políticas relacionadas como parte de los días INSET

Director Regional de Escuelas y Junta

Participar en una capacitación regular formal y auditada sobre seguridad en línea como parte de su CPD y plan de capacitación obligatorio

Lidiar con incidentes de uso indebido

Esta sección cubrirá los pasos necesarios para hacer frente a los incidentes y tiene como objetivo garantizar:

- Se siguen procedimientos claros para manejar incidentes
- Se lleva a cabo la notificación inmediata de incidentes graves a las autoridades correspondientes

Incidentes

Al investigar incidentes, debe:

- Involucrar al menos a dos altos funcionarios para garantizar la rendición de cuentas.
- Usar una computadora designada que no sea accesible para los estudiantes; Este dispositivo puede ser requerido por la policía.
- Asegúrese de que los investigadores hayan monitoreado y registrado el acceso a Internet.
- Mantenga una línea de tiempo de los eventos para posibles informes policiales.
- Registrar URL y describir el contenido relacionado; Capture y almacene capturas de pantalla si es necesario (excluyendo imágenes de abuso infantil).
- Después de la investigación, determine si la inquietud es válida y tome las medidas adecuadas:
    - Medidas disciplinarias internas
    - Remisión al Director Regional de Escuelas o autoridades pertinentes
    - Participación policial

Remisión policial obligatoria

Los siguientes incidentes deben ser denunciados a la policía sin excepción:

- Imágenes de abuso infantil
- Comportamiento de grooming
- Enviar materiales obscenos a un niño
- Infracciones de la Ley de Publicaciones Obscenas
- Contenido criminalmente racista
- Promoción del terrorismo o el extremismo
- Otras actividades delictivas

Medidas de salvaguardia

- Aísle la computadora para preservar la evidencia y evitar la posibilidad de manipulación.

- Siga todos los pasos de un registro cronológico para crear un rastro de evidencia claro para fines legales y de protección.
- Conserve el formulario / registro de investigación completo como referencia.

Acciones y sanciones

Es importante que cualquier incidente se trate lo antes posible de manera proporcionada, y que los miembros de la comunidad escolar sean conscientes de que se han tratado los incidentes. Se sugieren las siguientes acciones y sanciones para incidentes del personal y los estudiantes que se adaptan a la estructura, las autoridades gubernamentales y los procesos de su organización:

Incidentes y acciones del personal:

Escenario	Acción 1	Acción 2	Acción 3	Acción 4	Acción 5
Descarga o carga no autorizada de archivos	Advertencia	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR
Infracciones continuas de lo anterior, tras advertencias o sanciones anteriores	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	
Incumplimiento de las regulaciones de derechos de autor o licencias	Advertencia	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR
Acceder o intentar acceder deliberadamente a material ofensivo o pornográfico	Suspensión	consulte Principal	consulte RHoS / HR	consulte Policía	
Acceder accidentalmente a material ofensivo o pornográfico y no informar el incidente	Advertencia	Acción disciplinaria	consulte Principal	consulte RHoS / HR	
Usar sitios proxy u otros medios para subvertir el sistema de filtrado de la escuela	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	
Acciones que podrían desprestigiar a la escuela o violar la integridad del espíritu de la escuela	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	
Acciones que podrían comprometer la posición profesional del agente	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	
Uso del correo electrónico personal / redes sociales / mensajería instantánea / mensajes de texto para llevar a cabo comunicaciones digitales con los estudiantes	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	

Enviar un correo electrónico, mensaje de texto o mensaje que se considere ofensivo, de acoso o de naturaleza intimidatoria	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	consulte Policía
Corromper o destruir los datos de otros usuarios o causar daños deliberados al hardware o software	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	consulte Policía
Acciones deliberadas para violar las normas de protección de datos o seguridad de la red	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	consulte Policía
Uso descuidado de datos personales, por ejemplo, mantener o transferir datos de manera insegura	Advertencia	Acción disciplinaria	consulte Principal	consulte RHoS / HR	
Permitir que otros accedan a la red escolar compartiendo nombres de usuario y contraseñas o intentando acceder o accediendo a la red escolar, utilizando la cuenta de otra persona	Acción disciplinaria	suspensión	consulte Principal	consulte RHoS / HR	
Uso personal inapropiado de Internet / redes sociales / correo electrónico personal	Advertencia	Acción disciplinaria	consulte Principal	consulte RHoS / HR	
Acceder o intentar acceder deliberadamente a material que podría considerarse ilegal	Suspensión	consulte Principal	consulte RHoS / HR	**consulte Policía**	

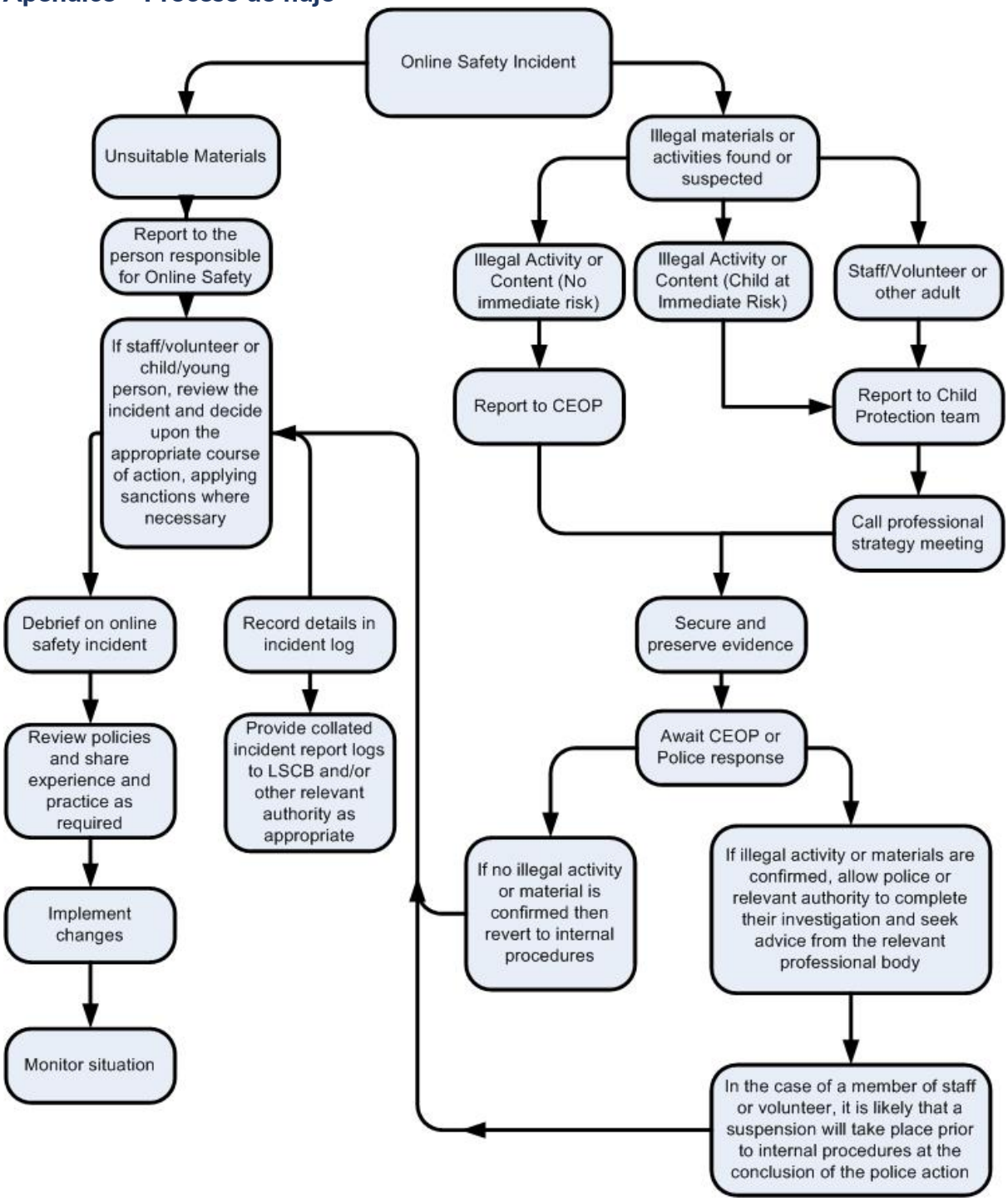
Incidentes y acciones de los estudiantes

Escenario	Acción 1	Acción 2	Acción 3	Acción 4	Acción 5
Descarga o carga no autorizada de archivos	Advertencia	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Infracciones continuas de lo anterior, tras advertencias o sanciones anteriores	Sanciones adicionales, por ejemplo, detención /	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–

	exclusión				
Incumplimiento de las regulaciones de derechos de autor o licencias	Advertencia	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Acceder o intentar acceder deliberadamente a material ofensivo o pornográfico	Suspensión	Eliminación de los derechos de acceso a la red / Internet	consulte Principal	informar a los padres / cuidadores	consulte Policía
Acceder accidentalmente a material ofensivo o pornográfico y no informar el incidente	Advertencia	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Usar sitios proxy u otros medios para subvertir el sistema de filtrado de la escuela	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Acciones que podrían desprestigiar a la escuela o violar la integridad del espíritu de la escuela	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Enviar un correo electrónico, mensaje de texto o mensaje que se considere ofensivo, de acoso o de naturaleza intimidatoria	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	consulte Principal	informar a los padres / cuidadores	consulte Policía
Corromper o destruir los datos de otros usuarios	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	consulte Principal	informar a los padres / cuidadores	consulte Policía
Acciones deliberadas para violar las normas de protección de datos o seguridad de la red	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	consulte Principal	informar a los padres / cuidadores	consulte Policía
Uso descuidado de datos personales, por ejemplo, mantener o transferir datos de manera insegura	Advertencia	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Permitir que otros accedan a la red escolar compartiendo nombres de usuario y contraseñas o intentando acceder o accediendo a la red	Acción disciplinaria	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–

escolar, utilizando la cuenta de otra persona					
Uso personal inapropiado de Internet / redes sociales / correo electrónico personal	Advertencia	Eliminación de los derechos de acceso a la red / Internet	Consultar al profesor / tutor de la clase	informar a los padres / cuidadores	–
Acceder o intentar acceder deliberadamente a material que podría considerarse ilegal	Suspensión	Eliminación de los derechos de acceso a la red / Internet	consulte Principal	informar a los padres / cuidadores	**consulte Policía**

Apéndice – Proceso de flujo



Referencias

Prevención del acoso y el ciberacoso: Ministerio de Educación y Formación Profesional – Plan Estratégico de Convivencia Escolar
https://www.educacionyfp.gob.es/servicios-al-ciudadano/catalogo/convivencia-escolar.html

Centro Español de Internet Segura: Internet Segura for Kids (IS4K), gestionado por INCIBE – Proporciona guías, materiales y recursos para profesores sobre seguridad digital y filtrado/monitorización.
https://www.is4k.es/profesores

Formación del profesorado en seguridad digital y convivencia escolar: INTEF – Aulas del Futuro / Recursos sobre la competencia digital del profesorado y la seguridad en línea
https://intef.es/competencia-digital/

Estándares de ciberseguridad:

INCIBE – Cybersecurity guide for schools – Practical guidance to help protect school systems against cyberattacks.
https://www.incibe.es/protege-tu-empresa/guias/ciberseguridad-centros-educativos

Orientación sobre la difusión de información para la protección de la infancia: Agencia Española de Protección de Datos (AEPD) – Canal prioritario y orientación sobre protección de datos en los centros educativos
https://www.aepd.es/menores

Protección de datos en los centros educativos (equivalente a la ICO / RGPD del Reino Unido):Agencia Española de Protección de Datos (AEPD) – Recursos para centros educativos y familias sobre privacidad, uso de imágenes y datos personales en
https://www.aepd.es/areas-de-actuacion/menores educativos

Materiales educativos para estudiantes sobre comportamiento en línea:
PantallasAmigas – Recursos educativos y guías para abordar el ciberacoso, la huella digital y la gestión de la identidad en línea
https://www.pantallasamigas.net/

Respuesta al intercambio no consentido de imágenes íntimas (equivalente UKCIS): AEPD – Canal prioritario (denuncia y eliminación urgente de contenido sensible en línea, especialmente difusión de imágenes íntimas de menores)
https://www.aepd.es/canalprioritario