

Política de Seguridad en Línea

ID del documento	MT-SA009
N.º de versión	V1.2
Aprobado por	
Fecha de aprobación	junio de 2026
Próxima revisión	junio de 2028



Índice

Finalidad	3
Ámbito de aplicación	3
Legislación y orientaciones	3
Tipos de riesgos	4
Contenido inapropiado	4
Funciones y responsabilidades	5
Consejo del Colegio	5
Responsable Regional de Colegios (RHoS)	5
Dirección y equipo directivo	5
Responsable de Seguridad en Línea / Responsable Designado de Salvaguarda (o adjunto/a)	5
Responsable de Redes/TI y personal técnico	6
Personal docente y de apoyo	7
Alumnado	7
Familias	8
Educación y formación.....	8
Educación del alumnado	8
Educación y participación de las familias	9
Educación y participación del personal y el voluntariado	9
Responsable Regional de Colegios (RHoS) y Consejo del Colegio	10
Gestión de incidentes de uso indebido.....	10
Incidentes	10
Derivación obligatoria a la policía	10
Medidas de salvaguarda	11
Medidas y sanciones	11
Seguimiento y revisión	11
Calendario de seguimiento, revisión y desarrollo posterior	12
Políticas relacionadas.....	12
Referencias útiles.....	12
ANEXOS	14
Anexo 1 – Diagrama de flujo del proceso	14
Anexo 2 – Incidentes del alumnado y medidas	15
Anexo 3 – Incidentes del personal y medidas	16

Finalidad

La seguridad en línea es un componente esencial de la salvaguarda en el Colegio Alminar, ya que contribuye a proteger a la comunidad educativa frente a riesgos como la exposición a contenidos dañinos, el ciberacoso, el grooming (captación en línea) y la radicalización. Esta política ayuda a garantizar que el alumnado pueda aprovechar las ventajas de internet de forma segura, reduciendo al mínimo los posibles riesgos y daños.

Ámbito de aplicación

Esta política se aplica a todos los miembros de la comunidad educativa (personal, alumnado, familias, visitantes, voluntariado y otras personas usuarias) que utilicen los sistemas y redes de tecnología digital del colegio, tanto dentro como fuera del centro.

Cuando el colegio derive a alumnado a un proveedor de escolarización alternativa, seguirá siendo responsable de su salvaguarda. Se realizará con el proveedor una evaluación conforme a esta política, y el colegio deberá obtener confirmación por escrito de que dispone de controles de seguridad en línea.

Legislación y orientaciones

La guía estatutaria Keeping Children Safe in Education (KCSIE) recoge las definiciones de los riesgos en línea, incluidos los derivados de la inteligencia artificial (IA) y de las tecnologías de ultrafalsificación (deepfakes). En España, estos riesgos se abordan en la *Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPVI)* –arts. 45–46 (deberes en materia de seguridad en línea)— y en la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)*, art. 84 (derecho de las personas menores a la intimidad en el uso de dispositivos digitales). En el ámbito autonómico, la *Ley 4/2021, de 27 de julio, de infancia y adolescencia de Andalucía* reconoce el derecho de niños, niñas y adolescentes al uso seguro de las TIC.

En virtud de la Education and Inspections Act 2006 del Reino Unido, los directores y directoras de los colegios están razonablemente facultados para regular la conducta del alumnado fuera del centro, y el personal puede imponer medidas disciplinarias por conductas inadecuadas vinculadas a la pertenencia al colegio, incluido el acoso en línea. La Education Act 2011 (sección 24b) amplía estas facultades al registro de dispositivos electrónicos y la eliminación de datos. En el contexto normativo español, la potestad del colegio para abordar conductas fuera del centro o en línea deriva de su propio *Reglamento de Régimen Interno / Normas de convivencia* (adoptado voluntariamente por el Colegio Alminar como centro privado, siguiendo el *Decreto 327/2010*, art. 34, y el protocolo andaluz de ciberacoso de la *Orden de 20 de junio de 2011*), que permite al colegio actuar siempre que una conducta afecte a la comunidad educativa o al bienestar de un alumno o alumna.

El colegio abordará las conductas inadecuadas en línea a través de diversas políticas e informará a las familias cuando detecte un comportamiento en línea inadecuado fuera del colegio.

Tipos de riesgos

La variedad de cuestiones que abarca la seguridad en línea es considerable y está en constante evolución, pero pueden clasificarse en cuatro áreas de riesgo:

- **Contenido:** exposición a contenidos ilegales, inapropiados o dañinos, incluidos imágenes, audio o vídeo generados por IA.
Algunos ejemplos son la pornografía, el racismo, la misoginia, las autolesiones, el suicidio, el antisemitismo, la radicalización, el extremismo, la suplantación de identidad, la información errónea, la desinformación (incluidas las noticias falsas) y las teorías conspirativas.
- **Contacto:** sufrir interacciones en línea dañinas con otras personas usuarias.
Algunos ejemplos son la presión entre iguales, la publicidad comercial o personas adultas que se hacen pasar por niños, niñas o jóvenes con la intención de captarlos (grooming) o explotarlos con fines sexuales, delictivos, económicos o de otro tipo.
- **Conducta:** comportamiento en línea que aumenta la probabilidad de sufrir un daño o que lo causa.
Algunos ejemplos son crear, enviar, recibir o compartir imágenes explícitas (tanto el intercambio consentido como no consentido de desnudos y semidesnudos y/o pornografía), el hostigamiento o el ciberacoso
- **Comercio:** riesgos como el juego en línea, la publicidad inapropiada, el phishing o las estafas económicas.

Contenido inapropiado

Se espera que:

- se impida de forma eficaz y fiable que las personas usuarias generen contenidos dañinos e inapropiados o accedan a ellos;
- los estándares de filtrado se mantengan de forma eficaz durante toda la conversación o interacción con una persona usuaria;
- el filtrado se ajuste en función de los distintos niveles de riesgo, la edad, la idoneidad y las necesidades de cada persona usuaria —por ejemplo, las personas usuarias con necesidades educativas especiales y/o discapacidad (SEND)—;
- El contenido multimodal se modere eficazmente, incluida la detección y el filtrado de contenidos prohibidos en varios idiomas, en imágenes y con errores ortográficos y abreviaturas habituales
- Se mantengan plenas capacidades de moderación de contenidos con independencia del dispositivo utilizado, incluidos los dispositivos propios (BYOD) y los teléfonos inteligentes, cuando se acceda a los productos mediante una cuenta institucional educativa

- El contenido se modere a partir de una comprensión contextual adecuada de la conversación, garantizando que el contenido generado sea sensible al contexto
- El filtrado se actualice periódicamente en respuesta a los tipos nuevos o emergentes de contenido dañino y a las herramientas de IA a las que puedan acceder las personas usuarias.

Funciones y responsabilidades

Todas las personas, incluidas las invitadas externas, deben leer y aceptar la política de uso aceptable antes de acceder a los sistemas y redes locales y en línea del colegio y de utilizarlos. Las siguientes responsabilidades en materia de seguridad en línea corresponden a funciones específicas:

Consejo del Colegio

- Aprobación de la Política de Seguridad en Línea
- Revisión de la eficacia de la política a partir de la información aportada por el RHoS

Responsable Regional de Colegios (RHoS)

- Actuar como miembro del Consejo Operativo responsable de la seguridad en línea, lo que incluye:
 - celebrar reuniones periódicas con el/la Coordinador/a de Seguridad en Línea / Responsable Designado de Salvaguarda / Director/a;
 - revisar y aprobar cualquier modificación de la política;
 - supervisar los incidentes e informes de seguridad en línea;
 - comunicar los incidentes al Consejo Operativo.

Dirección y equipo directivo

- Garantizar la seguridad de la comunidad educativa
- Garantizar que existe una autoridad/potestad equivalente conforme a la legislación local
- Garantizar que existe un sistema para supervisar, comunicar y recibir los informes de incidentes del/de la Responsable de Seguridad en Línea / Responsable Designado de Salvaguarda (DSL)
- Delegar las responsabilidades cotidianas de seguridad en línea en el/la Responsable de Seguridad en Línea / Responsable Designado de Salvaguarda (DSL)
- Garantizar que todo el personal recibe la formación adecuada

Responsable de Seguridad en Línea / Responsable Designado de Salvaguarda (o adjunto/a)

- Dirigir el Grupo de Seguridad en Línea

- Gestionar los incidentes cotidianos de seguridad en línea y mantener un registro de todos ellos
- Revisar los procesos y la política, y proponer mejoras o comunicar incumplimientos al equipo directivo
- Impartir formación y asesoramiento a todo el personal
- Coordinarse con el personal técnico y las autoridades externas

Responsable de Redes/TI y personal técnico

- Mantenerse al día en cuanto a la política, las prácticas y la formación en seguridad en línea
- Garantizar la seguridad física de la infraestructura técnica del colegio
- Implantar y supervisar las medidas de seguridad en línea y garantizar que estén actualizadas, incluidos el cortafuegos y la protección antivirus
- Garantizar que toda la tecnología relacionada con el acceso en línea esté protegida conforme a la normativa local, la Política de Seguridad en Línea y los estándares de referencia del grupo
- Garantizar que los proveedores externos contratados cumplan las medidas de seguridad en línea y conozcan plenamente los procesos del colegio antes de trabajar en él
- Garantizar que las plataformas de mensajería y colaboración se supervisen para detectar usos indebidos y, en caso de incidente, informar al/a la Responsable de Seguridad en Línea y al equipo directivo para su investigación
- Garantizar que el acceso físico a los sistemas informáticos esté restringido al nivel adecuado y que las personas usuarias tengan derechos de acceso claramente definidos (esto incluye el almacenamiento en línea y extraíble, los sistemas de datos del personal y del alumnado, los datos de la organización y el acceso a internet).
- Garantizar que todo el alumnado y el personal disponga de un nombre de usuario y una contraseña que cumplan los estándares de seguridad establecidos en la Política de Contraseñas, y que no se utilicen cuentas de usuario genéricas en ningún sistema del colegio.
- Garantizar que todos los nombres de usuario y contraseñas maestros de administración se almacenen en un gestor cifrado, y que el/la Director/a tenga acceso a él en caso de emergencia, a efectos de continuidad de la actividad.
- Garantizar que todas las licencias de software estén actualizadas y cubran el número de personas usuarias/dispositivos en uso en el colegio.

- Garantizar que todo el acceso a internet esté filtrado según la edad y el perfil de cada persona usuaria en el colegio, que el cortafuegos y las pasarelas de seguridad estén actualizados, y que los controles de seguridad reflejen los controles de salvaguarda recogidos en la Política de Controles de Salvaguarda.
- Apoyar al/a la Responsable de Seguridad en Línea / DSL para garantizar que exista un sistema de supervisión, registro y comunicación de incidentes de seguridad en línea.
- Garantizar que la Política de Uso Aceptable de TI esté a disposición del personal, el alumnado, las familias y los colaboradores externos, y que se haga cumplir antes de conceder acceso a los sistemas y redes del colegio.
- Realizar una evaluación anual de riesgos cibernéticos y revisarla cada trimestre
- Elaborar e implantar un plan de copias de seguridad de los datos del colegio y revisarlo cada año
- Comunicar todos los ciberataques

Personal docente y de apoyo

- Leer, comprender y cumplir las políticas de Seguridad en Línea y de Uso Aceptable de TI
- Mantenerse informado sobre las cuestiones de seguridad en línea
- Integrar la seguridad en línea en el currículo
- Supervisar y orientar el uso que el alumnado hace de las tecnologías digitales
- Comunicar cualquier uso indebido al/a la Responsable de Seguridad en Línea y al equipo directivo para su investigación
- Garantizar que todas las comunicaciones con el alumnado y las familias se realicen a través de los sistemas oficiales del colegio y que las conversaciones tengan siempre carácter profesional
- Garantizar que el alumnado comprenda la Política de Seguridad en Línea y sepa cómo evitar el plagio y la vulneración de los derechos de autor
- En las clases en las que el uso de internet esté planificado, se deberá dirigir al alumnado a sitios web cuya idoneidad se haya comprobado, garantizando que existan procedimientos para gestionar cualquier material inadecuado que aparezca en las búsquedas
- supervisar y aplicar las políticas vigentes sobre dispositivos siempre que se permita el uso de tecnologías digitales, dispositivos móviles, cámaras, etc. en las clases y otras actividades del colegio

Alumnado

- Comprender las políticas de Seguridad en Línea y de Uso Aceptable de TI

- Utilizar de forma responsable los sistemas de tecnología digital del colegio, conforme a la Política de Uso Aceptable de TI
- Comunicar los usos indebidos o los materiales inapropiados
- Seguir las orientaciones sobre buenas prácticas, la toma segura de imágenes y el uso adecuado del teléfono móvil, y comprender qué es el ciberacoso

Familias

- Apoyar las políticas de seguridad en línea del colegio
- Supervisar las actividades en línea de sus hijos e hijas
- Comprender la importancia de una buena seguridad en línea y en qué consiste, con especial atención a:
 - el buen uso de los dispositivos personales
 - las fotografías y vídeos digitales en los eventos del colegio y en su entorno
 - las orientaciones sobre el acceso seguro y el intercambio de información en las secciones para familias de las plataformas de aprendizaje y en los expedientes del alumnado en línea

Educación y formación

Aunque la regulación y las medidas técnicas son importantes, es fundamental educar al alumnado para que actúe de forma responsable en línea. La seguridad en línea y la alfabetización digital son elementos clave de la propuesta educativa del colegio, ya que ayudan al alumnado a reconocer los riesgos y a desarrollar su resiliencia. La seguridad en línea debe integrarse en todo el currículo, y el personal debe reforzar los mensajes clave. El currículo de seguridad en línea debe ser amplio, adecuado a la edad y progresivo, con oportunidades de aprendizaje creativas adaptadas a la estructura del colegio y a los grupos de edad del alumnado.

Educación del alumnado

Para garantizar un enfoque coherente y eficaz de la seguridad en línea, el colegio aplicará las siguientes medidas:

- **Impartición curricular:** se impartirá un currículo estructurado de seguridad en línea a través de Informática, PSHE (educación personal, social y para la salud) y otras materias pertinentes, con refuerzo periódico.
- **Mensajes para todo el colegio:** los mensajes clave de seguridad en línea se integrarán en las asambleas, las tutorías y los programas de orientación y bienestar (pastoral).
- **Pensamiento crítico:** se enseñará al alumnado a evaluar críticamente los contenidos en línea y a verificar su exactitud.
- **Responsabilidad digital:** las clases incluirán orientaciones sobre cómo citar las fuentes y respetar los derechos de autor.

- **Resiliencia frente a la radicalización:** se ayudará al alumnado a desarrollar su resiliencia mediante debates seguros sobre temas controvertidos y la comprensión de la participación cívica frente al extremismo.
- **Uso aceptable:** se formará al alumnado sobre la importancia de la Política de Uso Aceptable de TI y se le animará a utilizar la tecnología de forma responsable dentro y fuera del colegio.
- **Ejemplo del personal:** el personal servirá de modelo en el uso adecuado de las tecnologías digitales, internet y los dispositivos móviles.
- **Prácticas de navegación segura:** en el uso planificado de internet, se dirigirá al alumnado a sitios web verificados, y existirán procedimientos para gestionar la exposición a contenidos inadecuados.
- **Supervisión:** cuando el alumnado tenga acceso abierto a internet, el personal supervisará activamente su actividad.
- **Acceso a contenido restringido:** con fines educativos legítimos (p. ej., investigar sobre racismo, drogas o discriminación), el personal podrá solicitar acceso temporal a sitios bloqueados. Estas solicitudes deberán ser auditables y justificadas, y podrán ser aprobadas por el/la Director/a, en consulta con el RHoS cuando sea necesario.

Educación y participación de las familias

Las familias desempeñan un papel fundamental en la orientación y supervisión del comportamiento en línea de sus hijos e hijas; sin embargo, muchas pueden desconocer los riesgos o cómo responder ante una preocupación relacionada con la seguridad en línea. Para apoyar a las familias, el colegio promoverá la sensibilización y ofrecerá información periódica mediante:

- actividades vinculadas al currículo
- comunicaciones (p. ej., cartas, boletines, página web, plataforma de aprendizaje)
- sesiones, talleres y actos para familias
- campañas (p. ej., el Día de Internet Segura)
- la orientación hacia recursos fiables (p. ej., saferinternet.org.uk, childnet.com)
- información y recursos para apoyar la seguridad en línea en el hogar

Educación y participación del personal y el voluntariado

- Todo el personal recibe formación periódica, formal y auditada en seguridad en línea como parte de su desarrollo profesional continuo (CPD) y de su plan de formación obligatoria
- El personal de nueva incorporación recibe formación en seguridad en línea como parte de su proceso de acogida, que debe completarse en las tres primeras semanas

- Todo el personal revisa y acepta formalmente la Política de Seguridad en Línea y otras políticas relacionadas como parte de las actividades de inicio de curso o de la acogida durante el curso

Responsable Regional de Colegios (RHoS) y Consejo del Colegio

- Participar en formación periódica, formal y auditada en seguridad en línea como parte de su desarrollo profesional continuo (CPD) y de su plan de formación obligatoria

Gestión de incidentes de uso indebido

Este apartado recoge los pasos necesarios para gestionar los incidentes y tiene como objetivo garantizar que:

- se sigan procedimientos claros para la gestión de incidentes; y
- los incidentes graves se comuniquen de inmediato a las autoridades competentes.

Incidentes

Al investigar incidentes, el equipo directivo del colegio:

- implicará al menos a dos miembros del personal directivo, para garantizar la rendición de cuentas;
- utilizará un ordenador designado al que no tenga acceso el alumnado. Este dispositivo podría ser requerido por la policía;
- garantizará que el acceso a internet de quienes investigan esté supervisado y registrado;
- mantendrá una cronología de los hechos ante una posible denuncia a la policía;
- registrará las URL y describirá el contenido preocupante. Realizar y conservar capturas de pantalla puede ser útil, pero nunca deben incluir imágenes de abuso infantil;

Tras la investigación, el equipo directivo determinará si la preocupación es fundada y adoptará las medidas oportunas:

- medidas disciplinarias internas;
- derivación al/a la Responsable Regional de Colegios y/u otras autoridades competentes;
- intervención policial.

Derivación obligatoria a la policía

Determinados incidentes deben comunicarse a la policía sin excepción:

- imágenes de abuso infantil
- conductas de grooming (captación en línea)
- envío de material obsceno a un menor

- infracciones de la Obscene Publications Act (ley británica sobre publicaciones obscenas)
- contenido racista constitutivo de delito
- promoción del terrorismo o del extremismo
- otras actividades delictivas

Medidas de salvaguarda

- El ordenador utilizado para la investigación debe aislarse, para preservar las pruebas y evitar cualquier posibilidad de manipulación.
- Todos los pasos seguidos deben anotarse en un registro cronológico, a fin de crear una trazabilidad clara de las pruebas a efectos de salvaguarda y legales.
- El formulario/registro de investigación cumplimentado debe conservarse para su consulta.

Medidas y sanciones

Es importante que todos los incidentes se gestionen lo antes posible y de forma proporcionada. También es importante que los miembros de la comunidad educativa sepan que los incidentes se han gestionado.

En los Anexos se incluyen un diagrama de flujo del proceso y una propuesta de medidas y sanciones para los incidentes.

Seguimiento y revisión

Esta política ha sido elaborada por un grupo de trabajo integrado por:

- Director/a / Equipo directivo
- Responsable de Seguridad en Línea / Responsable Designado de Salvaguarda
- Personal (docente, de apoyo y técnico)
- Responsable Regional de Colegios / Consejo
- Familias
- Representantes del alumnado

Calendario de seguimiento, revisión y desarrollo posterior

- Aprobación V1: Por el Consejo, el 31/07/2025
- Seguimiento: Por el equipo directivo, al menos una vez al año
- Informes: Anualmente al Responsable Regional de Colegios y al Consejo, con comunicación inmediata de los incidentes graves
- Revisión: Anualmente, o cuando sea necesario en función de nuevos acontecimientos o tras incidentes, por el RHoS en nombre del Consejo

Políticas relacionadas

Esta política debe leerse junto con los siguientes documentos:

- Política de Salvaguarda
- Políticas de Conducta y contra el Acoso Escolar
- Políticas de Uso Aceptable de TI, de IA, de Contraseñas, de Redes Sociales y de Controles de Salvaguarda
- Keeping Children Safe in Education (KCSIE) 2026

Referencias útiles

UK Safer Internet Centre: saferinternet.org.uk - [guías y recursos](#)

- En particular, el UK Safer Internet Centre ha elaborado, por encargo del DfE, una serie de seminarios web para docentes con el fin de informar y apoyar a los colegios en sus responsabilidades de filtrado y supervisión - [Filtrado y supervisión adecuados](#)

Gobierno del Reino Unido: [Educación, formación y competencias - gov.uk](#)

- [Estándares de filtrado y supervisión](#)
- [Estándares de ciberseguridad para colegios y centros de formación](#), elaborados para ayudarles a mejorar su resiliencia frente a los ciberataques
- [Prevención del acoso escolar](#) (incluye el ciberacoso)
- [Intercambio de información para quienes prestan servicios de salvaguarda a menores](#)

UK Council for Internet Safety: [UKCIS](#)

- [Intercambio de desnudos y semidesnudos](#): orientaciones para colegios y centros de formación sobre cómo responder a incidentes de intercambio consentido y no consentido de desnudos y semidesnudos.

Childnet: [Childnet](#)

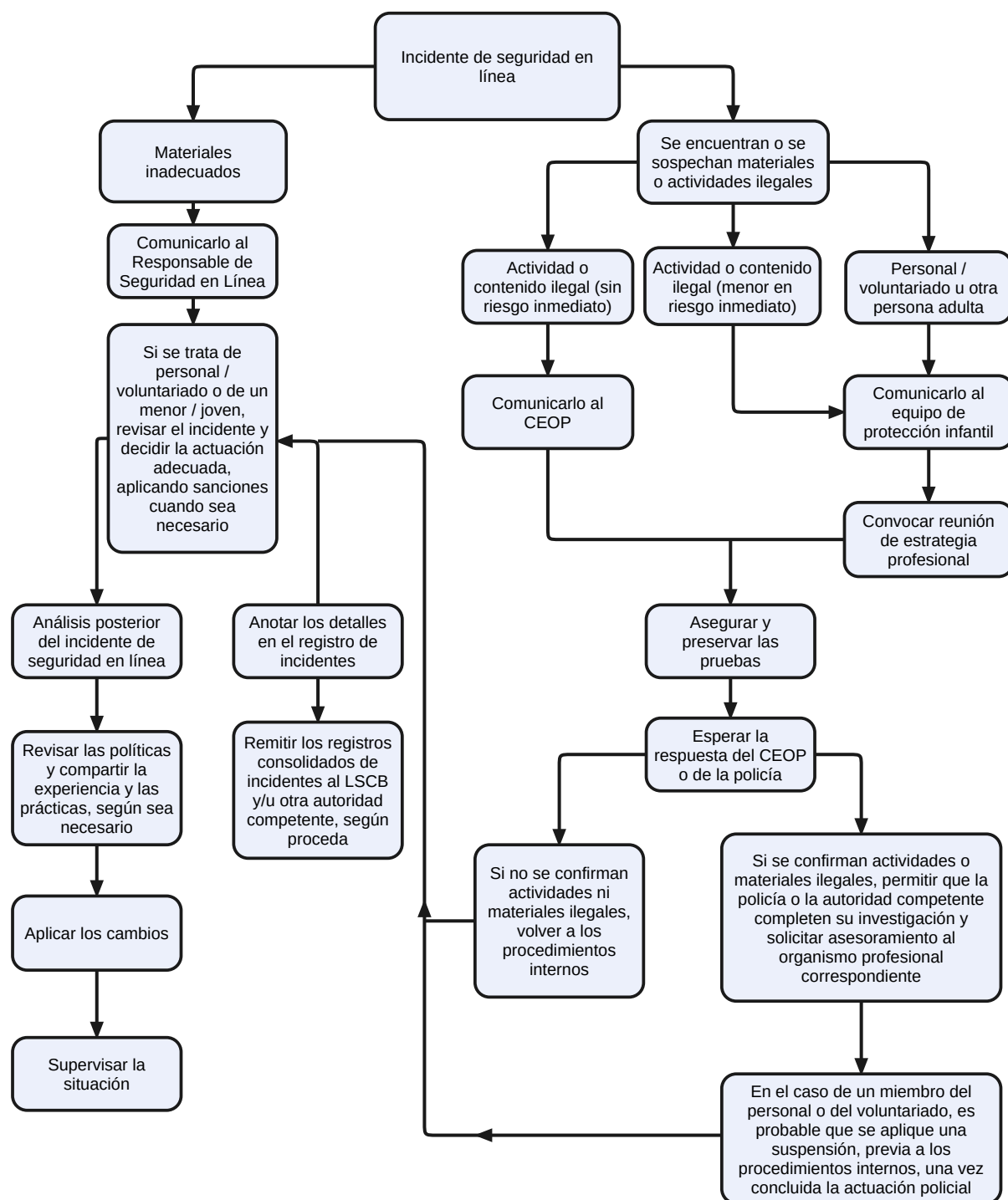
- [Just a joke?](#) – planes de clase, actividades, un cuestionario y una guía docente para abordar el comportamiento sexual problemático en línea con alumnado de 9 a 12 años.

Information Commissioner's Office (ICO): [Guía y recursos sobre el RGPD](#)

- [Centro de información sobre intercambio de datos](#) – recursos para ayudar a colegios y centros de formación a cumplir la legislación de protección de datos, incluido el RGPD del Reino Unido (UK GDPR).

ANEXOS

Anexo 1 – Diagrama de flujo del proceso



Anexo 2 – Incidentes del alumnado y medidas

[elimine o modifique las medidas de cada supuesto según sea necesario para su organización]

Supuesto	Medida 1	Medida 2	Medida 3	Medida 4	Medida 5
Descarga o subida no autorizada de archivos	Advertencia	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Reiteración de las infracciones anteriores, tras advertencias o sanciones previas	Sanción adicional, p. ej., castigo / expulsión	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Acceder <u>accidentalmente</u> a material ofensivo o pornográfico y no comunicar el incidente	Advertencia	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Acceder <u>deliberadamente</u> , o intentar acceder, a material ofensivo o pornográfico	Suspensión	retirada del acceso a la red / internet	derivar a Dirección	informar a la familia / tutores	derivar a la Policía
Acceder deliberadamente, o intentar acceder, a material que pueda considerarse ilegal	Suspensión	retirada del acceso a la red / internet	derivar a Dirección	informar a la familia / tutores	derivar a la Policía
Utilizar sitios proxy u otros medios para eludir el sistema de filtrado del colegio	Medida disciplinaria	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Acciones que puedan desprestigiar al colegio o atentar contra la integridad de su ideario	Medida disciplinaria	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Infringir los derechos de autor o las normas de licencias	Advertencia	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Dañar o destruir datos ajenos	Medida disciplinaria	retirada del acceso a la red / internet	derivar a Dirección	informar a la familia / tutores	derivar a la Policía
Uso negligente de datos personales, p. ej., conservar o transferir datos de forma insegura	Advertencia	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Permitir el acceso de terceros a la red del colegio compartiendo usuarios y contraseñas, o acceder o intentar acceder a la red con la cuenta de otra persona	Medida disciplinaria	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Acciones deliberadas para vulnerar las normas de protección de datos o de seguridad de la red	Medida disciplinaria	retirada del acceso a la red / internet	derivar a Dirección	informar a la familia / tutores	derivar a la Policía
Uso personal inapropiado de internet / redes sociales / correo electrónico personal	Advertencia	retirada del acceso a la red / internet	derivar al tutor/a o docente	informar a la familia / tutores	–
Enviar un correo electrónico, SMS o mensaje considerado ofensivo, de hostigamiento o de acoso	Medida disciplinaria	retirada del acceso a la red / internet	derivar a Dirección	informar a la familia / tutores	derivar a la Policía

Anexo 3 – Incidentes del personal y medidas

[elimine o modifique las medidas de cada supuesto según sea necesario para su organización]

Supuesto	Medida 1	Medida 2	Medida 3	Medida 4	Medida 5
Acciones que puedan comprometer la reputación profesional del miembro del personal	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Descarga o subida no autorizada de archivos	Advertencia	medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.
Reiteración de las infracciones anteriores, tras advertencias o sanciones previas	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Acceder <u>accidentalmente</u> a material ofensivo o pornográfico y no comunicar el incidente	Advertencia	medida disciplinaria	derivar a Dirección	derivar al RHoS / RR. HH.	
Acceder <u>deliberadamente</u> , o intentar acceder, a material ofensivo o pornográfico	Suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	derivar a la Policía	
Acceder deliberadamente, o intentar acceder, a material que pueda considerarse ilegal	Suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	derivar a la Policía	
Utilizar sitios proxy u otros medios para eludir el sistema de filtrado del colegio	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Acciones que puedan desprestigiar al colegio o atentar contra la integridad de su ideario	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Infringir los derechos de autor o las normas de licencias	Advertencia	medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.
Dañar o destruir datos ajenos o causar daños deliberados al hardware o al software	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	derivar a la Policía
Uso negligente de datos personales, p. ej., conservar o transferir datos de forma insegura	Advertencia	medida disciplinaria	derivar a Dirección	derivar al RHoS / RR. HH.	
Permitir el acceso de terceros a la red del colegio compartiendo usuarios y contraseñas, o acceder o intentar acceder a la red con la cuenta de otra persona	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Acciones deliberadas para vulnerar las normas de protección de datos o de seguridad de la red	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	derivar a la Policía
Uso personal inapropiado de internet / redes sociales / correo electrónico personal	Advertencia	medida disciplinaria	derivar a Dirección	derivar al RHoS / RR. HH.	
Usar el correo personal / redes sociales / mensajería instantánea / SMS para comunicarse digitalmente con el alumnado	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	
Enviar un correo electrónico, SMS o mensaje considerado ofensivo, de hostigamiento o de acoso	Medida disciplinaria	suspensión	derivar a Dirección	derivar al RHoS / RR. HH.	derivar a la Policía