MAGNO International School, Alicante
an Orbital Education School

Política de seguridad online y uso aceptable de las TIC

Aprobada por	Rosa María Tortosa
Última revisión:	Septiembre 25
Próxima revisión:	Septiembre 26

Contenido

1.Alcance de la política

Esta política se aplica a todos los miembros de la comunidad del colegio (incluyendo personal, estudiantes, padres, visitantes y usuarios de la comunidad) que tienen acceso y utilizan los sistemas de tecnología digital del colegio, tanto dentro como fuera del colegio. El colegio gestionará cualquier incidente relacionado con la seguridad online e informará, cuando sea posible, a los padres de incidentes de comportamiento inapropiado relacionado con la seguridad online que ocurran fuera del colegio.

2. Roles y responsabilidades

A continuación, se detallan los roles y responsabilidades en materia de seguridad online de individuos y grupos dentro del colegio:

2.2 Jefe Regional de Colegios (RHoS), actuando en nombre del Consejo de Administración.

- El Consejo es responsable de aprobar la Política de Seguridad Online y de revisar su efectividad. Esto se llevará a cabo mediante la recepción de información regular por parte del RHoS sobre incidentes de seguridad online e informes de seguimiento.

2.3 Director

- Tiene el deber de garantizar la seguridad (incluida la seguridad online) de los miembros de la comunidad del colegio, aunque la responsabilidad diaria de la seguridad online se delegará en el Responsable Designado de Protección (DSL).
- Es responsable de garantizar que el DSL y otros miembros del personal relevante reciban formación adecuada para desempeñar sus funciones de seguridad online y formar a otros compañeros, según sea necesario.
- Asegurará que exista un sistema para monitorear y apoyar a quienes realicen labores internas de supervisión de la seguridad online en el colegio.

2.4 Coordinador de Seguridad Online

- Se encarga de la responsabilidad diaria de las cuestiones relacionadas con la seguridad online y desempeña un papel principal en el establecimiento y revisión de las políticas/documentos de seguridad online del colegio.
- Garantiza que todo el personal esté al tanto de los procedimientos a seguir en caso de un incidente de seguridad online.
- Proporciona formación y asesoramiento al personal.
- Colabora, si es necesario, con las autoridades municipales.
- Se coordina con el personal técnico del colegio.
- Recibe informes de incidentes de seguridad online y crea un registro de estos para informar sobre futuros desarrollos en seguridad online.
- Informa regularmente al Director/a y reporta de inmediato cualquier incidente al Director

Responsabilidades del **Equipo Técnico / Gerente de TI**:

- Seguridad de la Infraestructura: Garantizar que la infraestructura técnica del colegio sea

segura y esté protegida contra usos indebidos o ataques malintencionados.

- Cumplimiento: Asegurar el cumplimiento de los requisitos técnicos de seguridad online y las directrices nacionales, municipales u otras pertinentes.
- Control de Acceso: Implementar políticas de contraseñas robustas con cambios periódicos.
- Actualización de Información: Mantenerse actualizado en temas técnicos de seguridad online y compartir información relevante.
- Supervisión y Reporte: Monitorizar regularmente el uso de las redes y reportar cualquier uso indebido al director o al DDSL (Líder Adjunto de Protección).
- Implementación de Políticas: Mantener y actualizar los sistemas de supervisión conforme a las políticas del colegio

Responsabilidades del **Personal Docente y de Apoyo**:

- Conocimiento de Políticas: Mantenerse al día sobre el contenido de la Política de Seguridad Online del colegio y firmar el Acuerdo de Uso Aceptable (AUP).
- Reporte de Incidentes: Informar de cualquier uso indebido sospechoso al director o al DSL (Líder de Protección Designado).
- Comunicación Digital: Mantener un nivel profesional en las comunicaciones digitales con estudiantes y padres, utilizando únicamente los sistemas oficiales del colegio.
- Integración en el Currículo: Incluir temas de seguridad online en las lecciones y garantizar que los estudiantes comprendan las políticas.
- Supervisión de Contenidos: Vigilar el uso de herramientas digitales y guiar a los estudiantes hacia contenido adecuado durante las clases.
- Cumplimiento de Políticas: Seguir los procedimientos establecidos para gestionar incidentes de seguridad online relacionados con el personal

2.5 Responsabilidades del Líder de Protección Designado (DSL) y Adjuntos:

- Formación Especializada: Recibir formación en temas de seguridad online.
- Protección de Menores: Abordar riesgos como el uso indebido de datos personales, acceso a material inapropiado, contacto online con adultos desconocidos, grooming y ciberacoso

2.6 Estudiantes:

- Cumplimiento de Políticas: Usar los sistemas tecnológicos del colegio según el Acuerdo de Uso Aceptable para Estudiantes.
- Desarrollo de Habilidades: Comprender la ética en la investigación, evitar el plagio y respetar los derechos de autor.
- Reporte de Incidentes: Informar sobre materiales inapropiados o usos indebidos.
- Conocimiento de Políticas: Familiarizarse con las normas del colegio respecto al uso de dispositivos móviles, cámaras y comportamiento online.

2. 7 Padres

- Promoción de la Seguridad: Apoyar al colegio en la promoción de buenas prácticas de seguridad online.
- Cumplimiento de Directrices: Respetar las normas sobre el uso de imágenes digitales y de

vídeo, así como el acceso a plataformas online del colegio.

- Concienciación y Supervisión: Informarse sobre los riesgos de seguridad online y supervisar el uso de internet de sus hijos.
- Participación: Participar en iniciativas organizadas por el colegio, como reuniones, formaciones y eventos como el Día de Internet Seguro

2.8 Educación

Aunque la regulación y las soluciones técnicas son muy importantes, su uso debe equilibrarse con la educación de los estudiantes para que adopten un enfoque responsable en el uso de la tecnología y las actividades online. Por tanto, la educación de los estudiantes en seguridad online es una parte esencial de la provisión de seguridad online del colegio. Los niños y jóvenes necesitan la ayuda y el apoyo del colegio para reconocer y evitar los riesgos de seguridad online y desarrollar su resiliencia.

La seguridad online debe ser un tema central en todas las áreas del currículo, y el personal debe reforzar los mensajes de seguridad online en todo el currículo. El currículo de seguridad online debe ser amplio, relevante y proporcionar progresión, con oportunidades para actividades creativas, y se proporcionará de las siguientes maneras:

- Se debe impartir un currículo planificado de seguridad online como parte de las clases de Informática, PSHE u otras asignaturas y revisarlo regularmente.
  ● Los mensajes clave de seguridad online deben reforzarse como parte de un programa planificado de asambleas y actividades de consejería.
  ● Se debe enseñar a los estudiantes en todas las lecciones a ser críticamente conscientes de los materiales o contenidos que acceden online y guiarlos para validar la precisión de la información.
  ● Se debe enseñar a los estudiantes a reconocer las fuentes de la información que utilizan y a respetar los derechos de autor al usar material accesible en internet.
  ● Se debe apoyar a los estudiantes para que desarrollen resiliencia frente a la radicalización, proporcionando un entorno seguro para debatir temas controvertidos y ayudándoles a comprender cómo pueden influir y participar en la toma de decisiones.
  ● Se debe ayudar a los estudiantes a comprender la necesidad del Acuerdo de Uso Aceptable para Estudiantes y fomentar el uso seguro y responsable tanto dentro como fuera del colegio.
  ● El personal debe actuar como buenos modelos a seguir en su uso de tecnologías digitales, internet y dispositivos móviles.
  ● Cuando los estudiantes puedan buscar libremente en internet, el personal debe estar atento para supervisar el contenido de las páginas web que visiten los jóvenes.
  ● Se acepta que, ocasionalmente y por razones educativas válidas, los estudiantes puedan necesitar investigar temas (por ejemplo, racismo, drogas, discriminación) que normalmente implicarían el bloqueo de búsquedas en internet. En tal situación, el personal puede solicitar al Equipo Técnico (u otra persona designada pertinente) que elimine temporalmente esos sitios de la lista filtrada durante el período de estudio. Cualquier solicitud de este tipo debe ser auditable y contar con razones claras que justifiquen la necesidad.

2.9 Educación Recomendada – La Comunidad en General (Colaboraciones)

El colegio proporcionará oportunidades a grupos de la comunidad local y a miembros de la comunidad para beneficiarse del conocimiento y experiencia del colegio en seguridad online. Esto se podrá ofrecer mediante:

- Cursos de aprendizaje familiar sobre el uso de nuevas tecnologías digitales, alfabetización digital y seguridad online.
  ● Mensajes de seguridad online dirigidos a abuelos y otros familiares, así como a los padres.
  ● La página web del colegio proporcionará información sobre seguridad online para la comunidad en general.
  ● Apoyo a grupos comunitarios, por ejemplo, Centros de Educación Infantil, cuidadores, grupos juveniles, deportivos o voluntarios, para mejorar su provisión de seguridad online

2.10 Formación del Personal

Es esencial que todo el personal reciba formación en seguridad online y comprenda sus responsabilidades, tal como se describe en esta política. La formación se ofrecerá de la siguiente manera:

- Un programa planificado de formación formal en seguridad online estará disponible para el personal, con actualizaciones regulares y refuerzos.
  ● Todo el personal nuevo debe recibir formación en seguridad online (EduCare - Seguridad Online para Colegios Internacionales) como parte de su programa de inducción, asegurándose de que comprende completamente la Política de Seguridad Online del colegio y los Acuerdos de Uso Aceptable.
  ● Esta Política de Seguridad Online y sus actualizaciones se presentarán y discutirán con el personal.
  ● El DSL y el coordinador de seguridad online proporcionarán asesoramiento, orientación y formación individual según sea necesario.
-

3. Técnico – infraestructura / equipo, filtrado y monitoreo

El colegio será responsable de garantizar que la infraestructura y la red del colegio sean lo más seguras posible y que las políticas y procedimientos aprobados en esta normativa se implementen.

Los sistemas técnicos del colegio se gestionarán de manera que el colegio cumpla con los requisitos técnicos recomendados:

- Habrá revisiones y auditorías periódicas de la seguridad de los sistemas técnicos del colegio.
  ● Los servidores, sistemas inalámbricos y cableado deben estar ubicados de forma segura y con acceso físico restringido.
  ● Todos los usuarios tendrán derechos de acceso claramente definidos a los sistemas y dispositivos técnicos del colegio.
  ● Todos los usuarios recibirán un nombre de usuario y una contraseña segura proporcionados por el equipo de TIC y los profesores, quienes mantendrán un registro actualizado de los usuarios y sus nombres de usuario. Los usuarios son responsables de la seguridad de su nombre de usuario y contraseña.
  ● Las contraseñas "maestras o de administrador" de los sistemas TIC del colegio, utilizadas por el Administrador de la Red (u otra persona), también deben estar disponibles para el Director y guardarse en un lugar seguro.

● El responsable de TIC es responsable de garantizar que los registros de licencias de software sean precisos y estén actualizados, y de realizar comprobaciones periódicas para reconciliar el número de licencias adquiridas con el número de instalaciones de software.
● El acceso a internet está filtrado para todos los usuarios. El contenido ilegal (imágenes de abuso sexual de menores) es filtrado por el proveedor de banda ancha o filtrado. Las listas de contenido se actualizan regularmente y el uso de internet se registra y monitorea con regularidad.
● El monitoreo de internet debe garantizar que los menores estén protegidos del material de radicalización cuando acceden a internet.
● El colegio ha implementado un filtrado mejorado y diferenciado según el nivel del usuario.
● El personal técnico del colegio monitorea y registra regularmente la actividad de los usuarios en los sistemas técnicos del colegio, y los usuarios son informados de esto en el Acuerdo de Uso Aceptable.
● Existe un sistema adecuado para que los usuarios informen cualquier violación real o potencial de seguridad técnica a la persona correspondiente, según lo acordado.
● Se han implementado medidas de seguridad adecuadas para proteger servidores, cortafuegos, enrutadores, sistemas inalámbricos, estaciones de trabajo, dispositivos móviles, etc., de intentos accidentales o malintencionados que puedan comprometer la seguridad de los sistemas y datos del colegio. Estas medidas se prueban regularmente. La infraestructura del colegio y las estaciones de trabajo individuales están protegidas por software antivirus actualizado.

● Existe una política acordada para proporcionar acceso temporal a "invitados" (por ejemplo, profesores en prácticas, profesores suplentes, visitantes) a los sistemas del colegio.
● Existe una política acordada sobre el uso de medios extraíbles (por ejemplo, memorias USB / CDs / DVDs) por parte de los usuarios en dispositivos del colegio. **Los datos personales no pueden enviarse por internet ni sacarse de las instalaciones del colegio a menos que estén debidamente encriptados o asegurados de otra forma**.

Tecnologías móviles

Los dispositivos móviles pueden ser útiles en muchos contextos educativos, como registrar el trabajo de un estudiante mediante imágenes o archivos de audio, o en el uso de calendarios electrónicos para planificar el trabajo. En términos de enseñanza y aprendizaje, pueden ser útiles para enviar trabajos por correo electrónico a casa, investigar en internet, escuchar podcasts de repaso o como diccionarios electrónicos. La regulación para el uso seguro y adecuado de las tecnologías móviles es:

- El personal puede tener teléfonos móviles y otros dispositivos en el colegio, pero deben mantenerse en modo silencioso durante el horario escolar y no deben usarse en las aulas o mientras se está enseñando;
  ● No se permite a los estudiantes tener dispositivos móviles en el colegio, incluidos teléfonos móviles y relojes inteligentes.
  ● Si los padres necesitan contactar urgentemente con su hijo o si los estudiantes necesitan hacer una llamada telefónica a sus padres, deben hacerlo a través de Recepción.
  ● El personal no puede usar teléfonos móviles durante las clases ni mientras está de servicio. Deben ser discretos en otros momentos para no molestar a otros miembros del colegio ni permitir que otros escuchen información personal, y no deben usar teléfonos móviles cerca de los estudiantes;

● No se permite el uso de equipos digitales para tomar fotos de estudiantes, personal o del colegio, salvo con el permiso expreso de un miembro del personal. Incluso cuando se haya dado dicho permiso, también debe obtenerse el consentimiento de la persona o de los padres de la persona afectada.
● No se pueden publicar imágenes de estudiantes, personal o del colegio en páginas web públicas o privadas, ni transferirlas ni entregarlas a otra persona sin el permiso del Director.

4. Uso de imágenes digitales y en vídeo

El desarrollo de tecnologías de imagen digital ha generado beneficios significativos para el aprendizaje, permitiendo a los profesores y estudiantes usar instantáneamente imágenes que han grabado ellos mismos o descargado de internet. Sin embargo, el personal, los padres y los estudiantes deben ser conscientes de los riesgos asociados con la publicación de imágenes digitales en internet. Dichas imágenes pueden abrir vías para el ciberacoso. Las imágenes digitales pueden permanecer disponibles en internet de forma indefinida y causar daño o vergüenza a las personas a corto o largo plazo. Es habitual que los empleadores realicen búsquedas en internet sobre posibles y actuales empleados.

- Se obtendrá permiso por escrito de los padres antes de publicar fotografías de los estudiantes en la página web del colegio, redes sociales o prensa local.
- Los padres pueden tomar vídeos e imágenes digitales de sus hijos en eventos del colegio para su uso personal. Para respetar la privacidad de todos y, en algunos casos, la protección, estas imágenes no deben publicarse en redes sociales ni deben los padres comentar sobre actividades que involucren a otros estudiantes en dichas imágenes.
- El personal y los voluntarios pueden tomar imágenes digitales o en vídeo para apoyar objetivos educativos, pero deben seguir las políticas del colegio respecto al uso, distribución y publicación de dichas imágenes. Estas imágenes deben tomarse únicamente con equipo del colegio; **no se debe usar equipo personal del personal para estos fines**.
- Se debe tener cuidado al tomar imágenes digitales o en vídeo para asegurarse de que los estudiantes estén vestidos de manera adecuada y no participen en actividades que puedan poner en entredicho a las personas o al colegio.
- Los estudiantes no deben tomar, usar, compartir, publicar ni distribuir imágenes de otras personas sin su permiso.
- Las fotografías publicadas en la página web o en otros lugares que incluyan a estudiantes se seleccionarán cuidadosamente y cumplirán con las guías de buenas prácticas sobre el uso de dichas imágenes.
- No se utilizarán los nombres completos de los estudiantes en ninguna página web o blog, especialmente en asociación con fotografías.

5. Protección de datos

Los datos personales serán registrados, procesados, transferidos y puestos a disposición de acuerdo con la legislación vigente en materia de protección de datos. En línea con la Política de Protección de Datos, Magno International School garantizará que:

- Se retendrán únicamente los datos personales mínimos necesarios para permitir el

desempeño de su función y no se conservarán más tiempo del necesario para los fines para los que fueron recopilados.
● Los datos almacenados deben ser precisos y estar actualizados. Las inexactitudes se corregirán sin retrasos innecesarios.
● La base legal para procesar datos personales (incluyendo, cuando corresponda, el consentimiento) se ha identificado, documentado y detallado en un Aviso de Privacidad.
● Existen disposiciones claras y comprendidas para el acceso, la seguridad, el almacenamiento y la transferencia de datos personales, incluyendo, cuando sea necesario, cláusulas contractuales adecuadas o salvaguardas para la transferencia de datos personales a terceros, como proveedores de servicios en la nube.
● Se dispone de políticas claras y comprendidas para la retención de datos y rutinas para la eliminación y destrucción de los mismos.
● Se ha establecido una política para informar, registrar, gestionar y recuperarse de incidentes relacionados con riesgos de información, que reconoce la obligación de reportar brechas de datos relevantes al ICO dentro de las 72 horas posteriores a la brecha, cuando sea posible.
● Se ha considerado la protección de datos personales cuando se accede a ellos mediante soluciones de acceso remoto.
● Todo el personal recibe formación sobre el manejo de datos y la protección de datos, y se les informa sobre sus responsabilidades.

El personal debe asegurarse de lo siguiente:

- Tener cuidado para garantizar la seguridad de los datos personales, minimizando el riesgo de pérdida o uso indebido.
  ● Utilizar datos personales solo en ordenadores y dispositivos protegidos por contraseñas seguras, asegurándose de cerrar sesión correctamente al finalizar cualquier sesión en la que se utilicen datos personales.
  ● Transferir datos utilizando cifrado y dispositivos protegidos con contraseñas seguras.

Cuando los datos personales se almacenen en un sistema portátil, memoria USB u otro medio extraíble:

- Los datos deben estar cifrados y protegidos con contraseña.
  ● El dispositivo debe estar protegido con contraseña (muchos dispositivos de memoria USB / tarjetas y otros dispositivos móviles no permiten protección mediante contraseña).
  ● El dispositivo debe contar con un software aprobado de comprobación de virus y malware.
  ● Los datos deben ser eliminados de forma segura del dispositivo, de acuerdo con la política del colegio, una vez que hayan sido transferidos o que su uso haya concluido.
- **Al utilizar tecnologías de comunicación, el colegio considera las siguientes prácticas como buenas:**
  ● El servicio de correo electrónico oficial del colegio se considera seguro y está monitorizado. Los usuarios deben ser conscientes de que las comunicaciones por correo electrónico son supervisadas. Por tanto, el personal y los estudiantes deben usar únicamente el servicio de correo electrónico del colegio para comunicarse con otros mientras estén en el colegio o utilizando los sistemas del colegio (por ejemplo, mediante acceso remoto).
  ● Los usuarios deben informar inmediatamente al Director sobre la recepción de cualquier comunicación que les haga sentir incómodos, que sea ofensiva, discriminatoria, amenazante o de naturaleza acosadora, y no deben responder a dichas comunicaciones.
  ● Cualquier comunicación digital entre el personal y los estudiantes o padres (correo electrónico, redes sociales, chat, blogs, entornos virtuales de aprendizaje, etc.) debe ser profesional en tono y contenido. Estas comunicaciones solo pueden realizarse a través de los sistemas oficiales (supervisados) del colegio. No deben utilizarse direcciones de correo

electrónico personales, mensajes de texto ni redes sociales para estas comunicaciones.
● Se pueden usar direcciones de correo electrónico de clase o grupo en KS1, mientras que

los estudiantes de KS2 y niveles superiores recibirán direcciones de correo electrónico individuales del colegio para fines educativos.
● Se debe enseñar a los estudiantes sobre los problemas de seguridad online, como los riesgos asociados al intercambio de datos personales. También se les deben enseñar estrategias para manejar comunicaciones inapropiadas y recordarles la importancia de comunicarse de manera adecuada al utilizar tecnologías digitales.
● No se debe publicar información personal en la página web del colegio, y solo se deben utilizar direcciones de correo electrónico oficiales para identificar a los miembros del personal

6. Redes Sociales - Protección de la Identidad Profesional

Los colegios están utilizando cada vez más las redes sociales como una herramienta de aprendizaje y un medio de comunicación efectivo. Es fundamental que este uso se realice de manera segura y responsable.

Todos los colegios tienen el deber de garantizar un entorno de aprendizaje seguro para estudiantes y personal. Podrían ser responsables, de forma indirecta, de los actos de sus empleados durante el desempeño de sus funciones. Los miembros del personal que acosen, participen en ciberacoso, discriminen por motivos de sexo, raza o discapacidad, o difamen a terceros, podrían hacer que el colegio sea responsable ante la parte afectada. Deben tomarse medidas razonables para prevenir daños previsibles.

El colegio implementa las siguientes medidas para garantizar que se minimicen los riesgos para estudiantes, personal y la propia institución:

- Garantizar que no se publique información personal.
  ● Proveer formación sobre uso aceptable, riesgos de las redes sociales, configuración de privacidad, protección de datos y reporte de problemas.
  ● Ofrecer directrices claras para el reporte de incidentes, incluyendo responsabilidades, procedimientos y sanciones.
  ● Realizar evaluaciones de riesgos, incluyendo riesgos legales

El personal del colegio debe asegurarse de lo siguiente:

- No se debe hacer referencia a estudiantes, padres o personal del colegio en las redes sociales.
  ● No deben participar en discusiones online sobre asuntos personales relacionados con miembros de la comunidad escolar.
  ● Las opiniones personales no deben atribuirse al colegio ni a Orbital Education.
  ● Se deben revisar regularmente las configuraciones de seguridad en los perfiles personales de redes sociales para minimizar el riesgo de pérdida de información personal

Cuando se crean **cuentas oficiales de redes sociales del colegio, deben** cumplir con lo siguiente:

- Un proceso de aprobación por parte del Director antes de publicar cualquier contenido.
  ● Procesos claros para la administración y supervisión de estas cuentas, que incluyan al menos a dos miembros del personal.
  ● Un código de conducta para los usuarios de las cuentas.

- Sistemas para reportar y gestionar abusos y usos indebidos.
- Un entendimiento de cómo los incidentes pueden ser tratados bajo los procedimientos disciplinarios del colegio

7. Uso personal

- Las comunicaciones personales realizadas a través de una cuenta personal en redes sociales. En todos los casos en los que se utilice una cuenta personal que se asocie con el colegio o que tenga un impacto sobre este, se debe dejar claro que el miembro del personal no está comunicándose en nombre del colegio mediante un descargo de responsabilidad apropiado. Tales comunicaciones personales están dentro del alcance de esta política.
- Las comunicaciones personales que no se refieran ni tengan impacto sobre el colegio quedan fuera del alcance de esta política.
- Si se sospecha un uso excesivo de redes sociales personales durante el horario escolar y se considera que interfiere con las responsabilidades laborales, se podrán tomar medidas disciplinarias

8. Supervisión de Redes Sociales Públicas

- Como parte del compromiso activo en redes sociales, se considera una buena práctica monitorear proactivamente Internet en busca de publicaciones públicas sobre el colegio.
- El colegio debe responder de manera efectiva a los comentarios en redes sociales realizados por terceros según una política o proceso definido.

El uso de redes sociales por parte del colegio con fines profesionales será revisado regularmente por el Responsable de Seguridad Online y el Director de Admisiones para garantizar el cumplimiento de las políticas del colegio

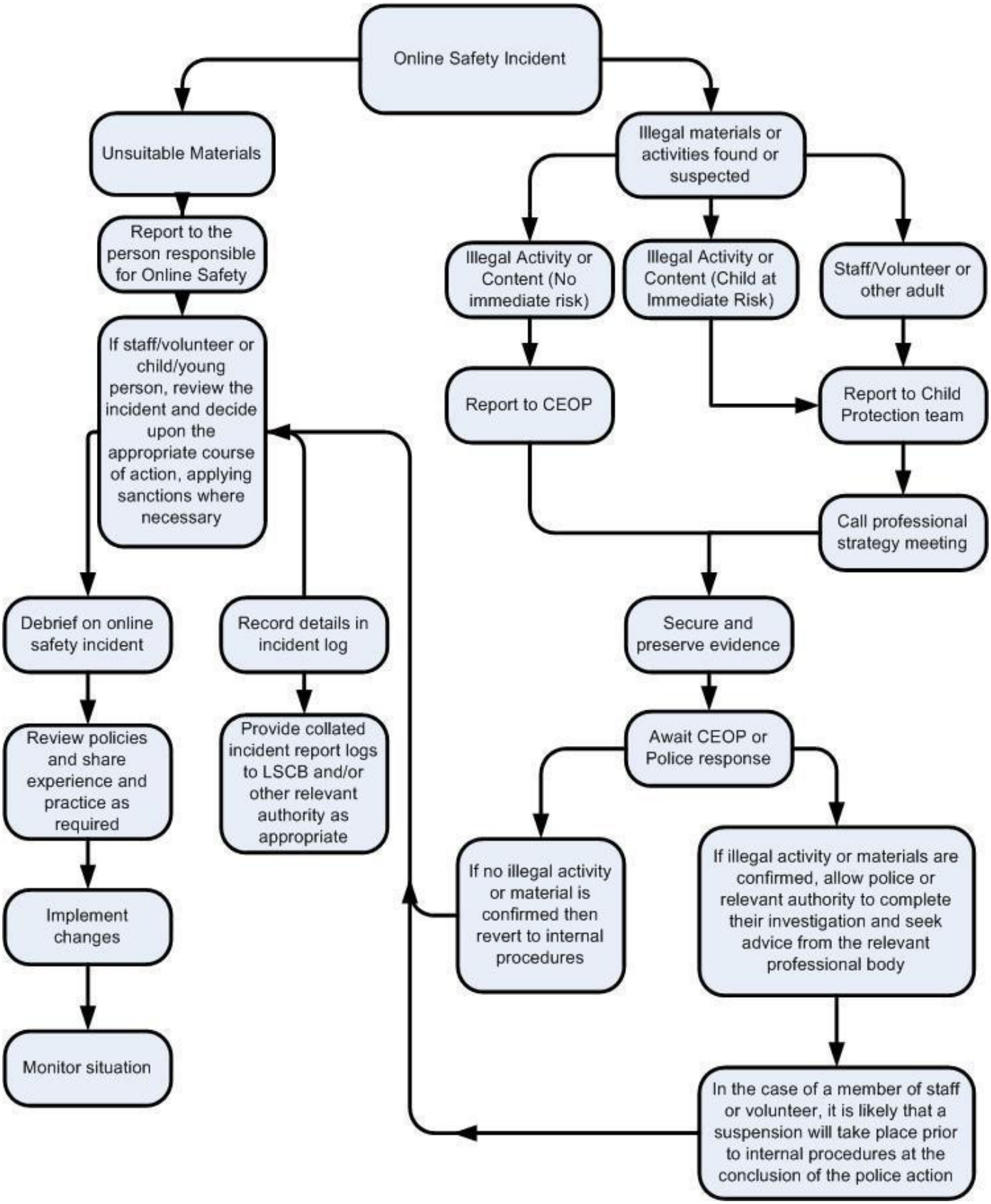
9. Respuesta a Incidentes de Uso Inadecuado

Esta guía está destinada a ser utilizada cuando el personal necesite gestionar incidentes relacionados con el uso de servicios online. Promueve un enfoque seguro y protegido para la gestión del incidente. Los incidentes pueden involucrar actividades ilegales o inapropiadas.

10. Incidentes ilegales

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the Principal and DSL.

MAGNO International School, Alicante
an Orbital Education School



11. Otros incidentes

Se espera que todos los miembros de la comunidad escolar sean usuarios responsables de las tecnologías digitales, que comprendan y sigan las políticas del colegio. Sin embargo, puede haber ocasiones en las que se produzcan infracciones de la política, ya sea por descuido, irresponsabilidad o, muy rara vez, por un uso deliberado indebido.

12. En caso de sospecha, deben seguirse todos los pasos de este procedimiento:

- Involucrar a más de un miembro del personal senior en este proceso. Esto es fundamental para proteger a los individuos si posteriormente se realizan acusaciones.
  ● Llevar a cabo el procedimiento utilizando un ordenador designado que no sea utilizado por estudiantes y que, si es necesario, pueda ser retirado del sitio por la policía. Utilice el mismo ordenador durante todo el procedimiento.
  ● Asegurarse de que el personal relevante tenga acceso adecuado a internet para llevar a cabo el procedimiento, pero también que los sitios y contenidos visitados sean supervisados y registrados de cerca (para mayor protección).
  ● Registrar la URL de cualquier sitio que contenga el supuesto uso indebido y describir la naturaleza del contenido que causa preocupación. También puede ser necesario registrar y almacenar capturas de pantalla del contenido en el ordenador utilizado para la investigación. Estas capturas pueden imprimirse, firmarse y adjuntarse al formulario (excepto en casos de imágenes de abuso infantil, véase más abajo).
  ● Una vez completada y totalmente investigada, el grupo deberá juzgar si esta preocupación tiene fundamento o no. Si lo tiene, será necesario tomar medidas apropiadas, que podrían incluir:

- Procedimientos internos o de disciplina.
- Participación del Responsable Regional de Colegios / Grupo o de una organización nacional o local (según corresponda).
- Implicación y/o actuación de la policía.
  ● Si el contenido revisado incluye imágenes de abuso infantil, se debe detener el monitoreo y remitir el caso inmediatamente al Director, al Responsable Regional de Colegios y a la Policía. Otras instancias que deben ser notificadas a la policía incluyen:
- Comportamiento de "grooming".
- El envío de materiales obscenos a un menor.
- Material para adultos que pueda infringir la Ley de Publicaciones Obscenas.

- Material racista de carácter delictivo.
- Promoción del terrorismo o extremismo.
- Otros materiales, conductas o actividades delictivas.
  ● Aislar el ordenador en cuestión lo mejor posible. Cualquier cambio en su estado podría dificultar una investigación policial posterior.

    Es importante que se sigan todos los pasos anteriores, ya que proporcionarán un rastro de evidencia para el colegio y, posiblemente, para la policía, demostrando que las visitas a estos sitios se realizaron por motivos de protección. El formulario completado debe ser retenido por el grupo como evidencia y para fines de referencia

13. Acciones y Sanciones del Colegio

Es más probable que el colegio necesite gestionar incidentes relacionados con un uso indebido inapropiado más que ilegal. Es importante que cualquier incidente se aborde lo antes posible de una manera proporcional y que los miembros de la comunidad escolar sepan que los incidentes se han gestionado. Se pretende que los incidentes de uso indebido se gestionen a través de los procedimientos normales de comportamiento / disciplina de la siguiente manera:

Incidentes de Estudiantes	**Referir al profesor / tutor de clase**	Referir al Director	Referir a la Policía	Referir al personal técnico para acciones de filtrado / seguridad, etc.	Informar a los padres / tutores	Retiro de derechos de acceso a la red / internet	Advertencia	Sanción adicional, por ejemplo, detención / expulsión
Acceso deliberado o intento de acceso a material que podría considerarse ilegal		X	X		x		x	x
Uso no autorizado de sitios no educativos durante las clases	x	x					x	x

Uso no autorizado/inapropiado de teléfono móvil, cámara digital u otro dispositivo móvil	x	x					x	x

Uso no autorizado/inapropiado de redes sociales, apps de mensajería o correo personal								
Descarga o subida no autorizada de archivos	x	x					x	x

Permitir a otros acceder a la red del colegio compartiendo usuario y contraseña	x	x						
Intento de acceso o acceso a la red del colegio usando la cuenta de otro estudiante	x	x		x	x		x	x
Intento de acceso o acceso a la red del colegio usando la cuenta de un miembro del personal	x	x		x	x		x	x

Corromper o destruir datos de otros usuarios								
	x	x		x	x		x	x
	x	x		x	x		x	x

	Referir al profesor/tutor	Referir al Director	Referir a la Policía	Referir al personal técnico para acciones de filtrado/seguridad, etc.	Informar a los padres/tutores	Retiro de derechos de acceso a la red/internet	Advertencia	Sanción adicional (ej. detención/expulsión)
Infracciones continuadas tras advertencias o sanciones previas	x	x			x		x	x

Acciones que puedan desprestigiar a la escuela o violar la integridad del ethos de la escuela	x	x			x		x	x

Uso de sitios proxy u otros medios para subvertir el sistema de filtrado de la escuela	x	x		x	x		x	x
Acceso accidental a material ofensivo o pornográfico y no reportar el incidente	x	x		x	x		x	

Acceso deliberado o intento de acceder a material ofensivo o pornográfico	x	x		x	x	x	x	x
Recepción o transmisión de material que infringe derechos de autor o la Ley de Protección de Datos	x	x		x	x	x	x	x

Incidentes del personal	Referir a RHoS/ HR	Referir a la Policía	Referir al personal técnico para acciones de filtrado/seguridad, etc.	Advertencia	Suspensión	Acción disciplinaria
Acceder deliberadamente o intentar acceder a material que podría considerarse ilegal (ver lista en sección anterior sobre actividades inadecuadas).	x	x	x	x	x	x
Uso personal inapropiado de internet/redes sociales/correo personal				x		

Descarga o carga no autorizada de archivos				x		
	Referir a RHoS/ HR	Referir a la Policía	Referir al personal técnico para acciones de filtrado/seguridad, etc.	Advertencia	Suspensión	Acción disciplinaria
Permitir que otros accedan a la red de la escuela compartiendo nombre de usuario y contraseña o utilizando la cuenta de otra persona	x		x	x		x
Uso negligente de datos personales, como mantener o transferir datos de manera insegura				x		

Acciones deliberadas para infringir las normas de protección de datos o seguridad de la red	x	x	x	x		x
Corromper o destruir datos de otros usuarios o causar daño deliberado a hardware o software	x	x	x			x
Enviar un correo electrónico, texto o mensaje considerado ofensivo, acoso o de naturaleza intimidante	x			x		
Uso de correo electrónico/redes sociales/mensajería instantánea/mensajes de texto personales para comunicarse con estudiantes	x		x	x		x
Acciones que puedan comprometer la posición profesional del miembro del personal	x			x		

Acciones que puedan desacreditar a la escuela o infringir la integridad de su ética	x		x	x	x	x

Uso de sitios proxy u otros medios para evadir el sistema de filtrado de la escuela	x		x	x		
Acceder accidentalmente a material ofensivo o pornográfico y no reportarlo	x		x	x		
Acceder deliberadamente o intentar acceder a material ofensivo o pornográfico	x	x	x	x	x	x
Infringir regulaciones de copyright o licencias	x			x		x
Infracciones continuas de las mencionadas anteriormente, tras advertencias o sanciones previas	x	x	x	x		x