MAGNO International School, Alicante
an Orbital Education School

POLÍTICA DE SEGURIDAD ONLINE

Aprobado por:	Rosa María Tortosa	
Última revisión:	Septiembre 24	
Próxima revisión:	Julio 25	

Contenido

1. Desarrollo / Seguimiento / Revisión de esta Política

Esta política de Seguridad online ha sido desarrollada por un grupo de trabajo/comité compuesto por:

- Director / Equipo directivo
- Responsable / Coordinador de seguridad online
- Personal – incluyendo Profesores, Personal de Apoyo y Personal Técnico
- Director regional de colegios / Junta directiva
- Padres
- Representante de los estudiantes

1.2 Cronograma para el Desarrollo, Seguimiento y Revisión

Esta política de Seguridad online fue aprobada por la Junta Directiva		
La implementación de esta Política de Seguridad online será supervisada por:		*El Equipo Directivo y otros grupos relevantes.*
El seguimiento se llevará a cabo en intervalos regulares:		*Insertar período de tiempo (se sugiere al menos una vez al año)*
El Director/a Regional de Colegios / Responsable del Grupo de TIC y la Junta Directiva recibirán un informe sobre la implementación de la política de Seguridad online, elaborado por el grupo de seguimiento (que incluirá detalles anónimos de incidentes relacionados con la seguridad online) en intervalos regulares:		Anualmente, salvo que ocurran incidentes de preocupación que requieran un informe inmediato. Los incidentes reportables también se incluirán en el Informe Mensual del Director
La política de Seguridad online será revisada anualmente, o con mayor frecuencia en caso de nuevos desarrollos significativos en el uso de tecnologías, nuevas amenazas a la seguridad online o incidentes ocurridos. La próxima revisión prevista será:		Julio 2025
Si se producen incidentes graves relacionados con la seguridad online, se deberá informar a las siguientes personas o agencias externas:		Director Regional de Colegios y Responsable del Grupo de IT. En caso de infracciones legales, se remitirá a la autoridad correspondiente.

El colegio supervisará el impacto de la política utilizando:

- Registros de incidentes reportados
- Registros de monitoreo de la actividad en internet (incluidos los sitios visitados) / filtrado
- Datos internos de monitoreo de la actividad en la red
- Encuestas / cuestionarios dirigidos a:
    - alumnos
    - padres
    - personal

2. Ámbito de aplicación de la Política

Esta política se aplica a todos los miembros de la comunidad escolar (incluidos el personal, estudiantes, voluntarios, padres, visitantes y usuarios de la comunidad) que tengan acceso a y utilicen los sistemas y redes de tecnología digital del colegio, tanto dentro como fuera del recinto escolar.

En el Reino Unido, la Ley de Educación e Inspecciones de 2006 (**los directores deben asegurarse de que exista una autoridad/poder comparable bajo la legislación del país anfitrión**) faculta a los directores, dentro de límites razonables, a regular el comportamiento de los estudiantes fuera del colegio y permite al personal imponer sanciones disciplinarias por conductas inapropiadas. Esto es relevante en casos de ciberacoso u otros incidentes de Seguridad online contemplados en esta política, que pueden ocurrir fuera del colegio pero que están vinculados con la pertenencia al mismo.

El colegio abordará estos incidentes en el marco de esta política, así como de las políticas asociadas de comportamiento y contra el acoso escolar, y, cuando sea posible, informará a los padres sobre incidentes de comportamiento inapropiado relacionado con la Seguridad Online que ocurran fuera del colegio.

3.Funciones y responsabilidades

La siguiente sección describe las funciones y responsabilidades en materia de seguridad online de los individuos y grupos dentro *del colegio*. (En colegios pequeños, algunos de estas funciones pueden combinarse, pero es importante garantizar una adecuada "separación de responsabilidades" en esos casos).

3.1 Director Regional de Colegios (RHoS) actuando en representación de la Junta Directiva

La Junta Directiva es responsable de la aprobación de la Política de Seguridad Online y de revisar su efectividad. Esto se lleva a cabo mediante la recepción de información regular sobre incidentes de seguridad online y reportes de seguimiento por parte del RHoS. El RHoS asume el papel de *miembro operativo de la Junta de Seguridad Online* (se sugiere combinar este rol con el del *Responsable de Protección y Seguridad de la Oficina Central*). Sus funciones incluyen:

- Reuniones regulares con el Coordinador de Seguridad Online, el Responsable de Protección o el Director
- Seguimiento regular de los registros de incidentes de seguridad online
- Revisión de registros de filtrado/control de cambios
- Presentación de informes a las reuniones pertinentes de la Junta Directiva

3.2 Director y Equipo Directivo

- El Director tiene la responsabilidad de garantizar la seguridad (incluida la seguridad online) de los miembros de la comunidad escolar, aunque la responsabilidad diaria se delegará al *Responsable de Seguridad en Línea / Responsable de Protección Designado* (DSL) o su adjunto (DDSL)
- El Director y al menos otro miembro del Equipo Directivo deben conocer los procedimientos a seguir ante acusaciones graves relacionadas con la seguridad online contra un miembro del personal.
- Aseguran que el Responsable de Seguridad Online y otros miembros relevantes del personal reciban formación adecuada para desempeñar sus funciones y capacitar a otros colegas.
- Garantizan un sistema de monitoreo y apoyo para quienes desempeñen roles internos de supervisión de seguridad en línea
- Reciben informes regulares del Responsable de Seguridad en Línea.

3.3 Responsable de Seguridad en Línea (DSL o DDSL)

Cada colegio debe contar con un miembro del personal encargado de la seguridad online diaria. Este rol puede combinarse con el de Responsable de Protección (DSL/DDSL) si el colegio lo decide. Sus responsabilidades incluyen:

- Liderar el Grupo de Seguridad en Línea
- Gestionar las cuestiones diarias de seguridad en línea y liderar la revisión y actualización de las políticas escolares de seguridad en línea
- Asegurar que todo el personal conozca los procedimientos ante incidentes de seguridad en línea.
- Proporcionar formación y asesoramiento al personal
- Coordinarse con la autoridad municipal cuando sea necesario
- Coordinarse con el personal técnico del colegio
- Recibir informes de incidentes de seguridad en línea y crear registros para mejorar las políticas futuras
- Informar regularmente al Equipo Directivo

3.4 Responsable de Redes / Personal Técnico

En colegios con un servicio externo de TIC, es responsabilidad del colegio garantizar que el proveedor implemente las medidas de seguridad online. Las responsabilidades incluyen:

- Asegurar la seguridad de la infraestructura técnica del colegio
- Cumplir con los requisitos técnicos de seguridad online establecidos por cuerpos nacionales o municipales.
- Implementar políticas de acceso con contraseñas protegidas y registradas.
- Actualizarse en información técnica de seguridad online para asesorar a otros
- Supervisar el uso de la red/internet y reportar posibles malusos al equipo correspondiente
- Implementar y actualizar sistemas de monitoreo según las políticas del colegio

3.5 Personal Docente y de Apoyo

El personal es responsable de:

- **Mantenerse actualizado en temas de seguridad online y políticas del colegio mediante formaciones regulares**
- **Leer, entender y firmar el Acuerdo de Uso Aceptable (AUP)**
- **Reportar sospechas de maluso al Responsable de Seguridad online o al Equipo Directivo**

- **Usar sistemas digitales *oficiales* para las comunicaciones profesionales**
- Integrar temas de seguridad online en el currículo y actividades
- Asegurar que los estudiantes comprendan las políticas de uso aceptable y la importancia de evitar el plagio y respetar los derechos de autor
- Supervisar el uso de tecnologías digitales en clase y actividades escolares
- Guiar a los estudiantes a sitios seguros en clases que requieran uso de internet

3.6 Designated Safeguarding Lead / Designated Person

Debe estar capacitado en seguridad online y consciente de los riesgos relacionados con:

- Compartición de datos personales
- Acceso a materiales ilegales o inapropiados.
- Contacto online inapropiado con adultos/desconocidos
- Grooming y ciberacoso

(Este rol puede combinarse con el del Responsable de Seguridad Online según decida el colegio).

4. Grupo de seguridad online opcional

El Grupo de Seguridad Online proporciona un grupo consultivo con amplia representación de la comunidad *del colegio*, responsable de asuntos relacionados con la seguridad online y el seguimiento de la Política de Seguridad Online, incluyendo el impacto de las iniciativas. Dependiendo del tamaño o la estructura del colegio, este grupo puede formar parte del grupo de protección. También será responsable de informar regularmente al Director.

Los miembros del Grupo de Seguridad Online (u otro grupo pertinente) apoyarán al Responsable / Coordinador de Seguridad Online (u otra persona designada) en las siguientes tareas:

- Revisar y supervisar la Política de Seguridad Online del colegio y los documentos relacionados.
- Analizar y evaluar la oferta curricular de seguridad online y alfabetización digital, asegurando relevancia, amplitud y progresión
- Monitorizar registros de red/internet e incidentes
- Consultar a las partes interesadas, incluyendo a las familias y el alumnado, sobre la provisión de seguridad online
- Supervisar las acciones de mejora identificadas mediante la herramienta de autoevaluación 360-degree safe

4.1 Alumnado:

- Es responsable de utilizar los sistemas tecnológicos del colegio de acuerdo con el Acuerdo de Uso Aceptable para Estudiantes.
- Debe tener un buen conocimiento de las habilidades de investigación y la necesidad de evitar el plagio y respetar las normativas de derechos de autor.
- Debe entender la importancia de reportar abusos, usos indebidos o acceso a materiales inapropiados y saber cómo hacerlo.
- Deberá conocer y comprender las políticas sobre el uso de dispositivos móviles y cámaras digitales, así como las políticas relativas al uso de imágenes y al ciberacoso.
- Debe adoptar buenas prácticas de seguridad online al usar tecnologías digitales fuera del colegio, reconociendo que la Política de Seguridad Online del colegio cubre sus acciones fuera del ámbito escolar si están relacionadas con su pertenencia al colegio

4.2 Familias

Las familias desempeñan un papel crucial para asegurar que los menores entiendan la necesidad de utilizar internet y los dispositivos móviles de manera adecuada. El colegio aprovechará todas las oportunidades para ayudar a las familias a comprender estos temas mediante *reuniones*, *boletines*, *cartas*, *página web/plataforma de aprendizaje y campañas/lfolletos* nacionales o locales sobre seguridad online. Se alentará a las familias a apoyar al colegio en la promoción de buenas prácticas de seguridad online y a seguir las directrices sobre el uso apropiado de:

- Imágenes digitales y de vídeo tomadas en eventos del colegio.
- El acceso a secciones para padres en la página web/plataforma de aprendizaje y los registros online de los estudiantes

5.Usuarios de la comunidad

Los usuarios de la comunidad que accedan a los sistemas del colegio, a la web o a la plataforma de aprendizaje como parte de la oferta educativa ampliada deberán firmar un Acuerdo de Uso Aceptable (AUA) para Usuarios de la Comunidad antes de recibir acceso a los sistemas del colegio. Si contratistas externos acceden a los recursos digitales del colegio, sin importar cuán limitado sea ese acceso, también deberán firmar un AUA.

5.1 Declaraciones de Política

Educación – Alumnado

Aunque la regulación y las soluciones técnicas son muy importantes, su uso debe equilibrarse con la educación del alumnado para que adopte un enfoque responsable. La formación en seguridad online y alfabetización digital es, por tanto, 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 riesgos online, y para desarrollar su resiliencia.

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

- **Se debe incluir un currículo planificado de seguridad online como parte de las clases de Informática, PSHE u otras asignaturas, revisándolo de manera regular.**
- **Los mensajes clave de seguridad online deben reforzarse como parte de un programa planificado de asambleas y actividades tutoriales o de orientación.**
- **En todas las asignaturas, se debe enseñar al alumnado a ser crítico con los materiales y contenidos que accede online, guiándoles para validar la precisión de la información.**
- **Se debe enseñar al alumnado a reconocer las fuentes de información utilizadas y a respetar los derechos de autor al usar materiales accesibles en internet.**
- **Se debe apoyar al alumnado en desarrollar resiliencia frente a la radicalización, proporcionándoles un entorno seguro para debatir temas controvertidos y ayudándoles a entender cómo pueden influir y participar en la toma de decisiones.**
- *Se debe ayudar al alumnado a comprender la importancia del Acuerdo de Uso Aceptable para Estudiantes, fomentando un uso seguro y responsable dentro y fuera del colegio.*
- *El personal debe actuar como modelo de referencia en el uso de tecnologías digitales, internet y dispositivos móviles.*
- *En las clases donde el uso de internet esté planificado, es una buena práctica guiar al alumnado hacia sitios previamente revisados como adecuados para su uso, estableciendo procesos para gestionar el acceso a materiales inadecuados encontrados en búsquedas online.*
- *Cuando el alumnado pueda buscar libremente en internet, el personal debe estar atento para supervisar el contenido de las páginas que visiten.*
- *En ocasiones, por razones educativas válidas, el alumnado puede necesitar investigar temas (como racismo, **drogas** o discriminación) que normalmente activarían bloqueos en búsquedas online. En estos casos, el personal puede solicitar al equipo técnico (u otra persona designada) que elimine temporalmente esos sitios de la lista filtrada durante el periodo de estudio. Estas solicitudes deben ser auditables y contar con motivos claros. (Puede solicitarse un modelo de solicitud a Orbital si no existe uno).*

5.2 Educación – Familias

Muchas familias tienen una comprensión limitada de los riesgos y problemas de seguridad online, aunque desempeñan un papel esencial en la educación de sus hijos y en la supervisión y regulación de su comportamiento online. Es posible que subestimen la frecuencia con la que los menores encuentran material potencialmente dañino o inapropiado en internet y no sepan cómo reaccionar.

Por ello, el colegio buscará proporcionar información y sensibilización a las familias mediante:

- *Actividades curriculares.*
- *Cartas, boletines informativos, web, plataforma de aprendizaje.*
- *Reuniones o sesiones informativas para las familias.*
- *Eventos o campañas destacadas, como el Día de Internet Seguro.*
- *Referencias a sitios web o publicaciones relevantes, como: www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers*

5.3 Educación Recomendada – Comunidad en General (Colaboraciones)

El colegio ofrecerá oportunidades a grupos y miembros de la comunidad local para beneficiarse de su conocimiento y experiencia en seguridad online. Esto podría incluir:

- *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, además de a los padres.*
- *Información sobre seguridad online disponible en la web del colegio*

Apoyo a grupos comunitarios (como guarderías, cuidadores, grupos juveniles, deportivos o voluntarios) para mejorar su provisión de seguridad online

5.4 Formación y Capacitación – Personal/Voluntarios

Es esencial que todo el personal reciba formación sobre seguridad online y entienda sus responsabilidades, según lo establecido en esta política. La formación se ofrecerá de las siguientes maneras:

- **Un programa planificado de formación formal en seguridad online estará disponible para el personal, con actualizaciones regulares. Se llevará a cabo periódicamente una auditoría de las necesidades de formación en seguridad online del personal.**
- **Todo el personal nuevo recibirá formación sobre seguridad online (EduCare – Seguridad Online para Colegios Internacionales) como parte de su programa de inducción, asegurándose de que comprenden plenamente 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 en reuniones de personal o jornadas de formación**.
- *El Responsable o Coordinador de Seguridad Online (u otra persona designada) proporcionará asesoramiento, orientación o formación individual cuando sea necesario*

6. Formación – Responsable Regional de Colegios y Junta Directiva

Los miembros de la junta directiva deben participar en sesiones de formación o concienciación sobre seguridad online, especialmente aquellos que formen parte de subcomités o grupos

relacionados con tecnología, seguridad online, salud, seguridad o protección. Esto puede ofrecerse de varias maneras:

- Formación proporcionada por el Responsable del Grupo de IT.
- Participación en formación online ofrecida por organizaciones relevantes, como EduCare.
- Participación en sesiones de formación/información en el colegio para el personal o las familias (esto puede incluir asistencia a asambleas o clases)

6.1 Técnico – Infraestructura/equipamiento, filtrado y supervisión

Si el colegio tiene un servicio de TIC gestionado por un contratista externo, es responsabilidad del colegio asegurarse de que el proveedor de servicios gestionados lleva a cabo todas las medidas de seguridad online que, de otro modo, corresponderían al colegio, según lo sugerido a continuación. Además, es importante que el proveedor de servicios gestionados conozca plenamente la Política de Seguridad Online del colegio y los Acuerdos de Uso Aceptable.

El colegio será responsable de garantizar que la infraestructura/red del colegio sea lo más segura posible y de que se implementen las políticas y procedimientos aprobados en esta política. También deberá asegurarse de que las personas relevantes mencionadas en las secciones anteriores puedan desempeñar eficazmente sus responsabilidades relacionadas con la seguridad online: (Los colegios tendrán infraestructuras técnicas muy diferentes y diferentes perspectivas sobre cómo se abordarán estas cuestiones técnicas; por tanto, es esencial que esta sección sea discutida ampliamente por personal técnico, educativo y administrativo antes de que se acuerden y se añadan estas declaraciones a la política)

(Un modelo más detallado de Política de Seguridad Técnica puede solicitarse a la Oficina Central de Orbital)

- Los sistemas técnicos del colegio se gestionarán de manera que cumplan con los requisitos técnicos recomendados.
- Habrá revisiones y auditorías regulares de la seguridad de los sistemas técnicos del colegio.
- Los servidores, equipos de red, sistemas inalámbricos y cableado deben estar ubicados de manera 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** (*en 3º Primaria y superiores*) **recibirán un nombre de usuario y una contraseña segura**, proporcionados por el responsable de de seguridad online *quien mantendrá un registro actualizado de los usuarios y sus nombres de usuario*. **Los usuarios serán responsables de la seguridad de su nombre de usuario y contraseña**. *Cualquier usuario que deje el colegio debe tener su cuenta desactivada el último día de su relación con el colegio para evitar su uso por otros*.

- Las contraseñas de administrador o docente de los sistemas de TIC del colegio, utilizadas por el Gestor de Red (u otra persona), también deben estar disponibles para el director o un líder senior designado y mantenerse en un lugar seguro (por ejemplo, caja fuerte del colegio o, **preferiblemente, en un almacén de claves seguro y encriptado)**
- El responsable de seguridad online es responsable de garantizar que los registros de licencias de software sean precisos y estén actualizados, y que se realicen verificaciones regulares para reconciliar el número de licencias adquiridas con el número de instalaciones de software
- **El acceso a internet está filtrado para todos los usuarios**. Los contenidos ilegales (imágenes de abuso sexual infantil) son filtrados por el cortafuegos, el proveedor de banda ancha o de filtrado, empleando activamente la **lista CAIC de la Fundación Internet Watch**. Las listas de contenido se actualizan regularmente y el uso de internet se registra y supervisa periódicamente (el colegio deberá decidir los méritos del servicio de filtrado interno/externo)
- **El filtrado/supervisión de internet debe garantizar que los menores estén protegidos contra material de radicalización al acceder a internet.**
- *El colegio ha proporcionado un filtrado a nivel de usuario mejorado/diferenciado* (permitiendo diferentes niveles de filtrado para diferentes edades, etapas y grupos de usuarios: personal, alumnos, etc.)
- *El personal técnico del colegio supervisa y registra regularmente la actividad de los usuarios en los sistemas técnicos del colegio, y los usuarios son conscientes de ello a través del Acuerdo de Uso Aceptable*
- *Existe un sistema adecuado para que los usuarios informen sobre cualquier incidente técnico o brecha de seguridad potencial o real al responsable correspondiente, según lo acordado.*
- Hay medidas de seguridad adecuadas en vigor para proteger los servidores, cortafuegos, routers, sistemas inalámbricos, estaciones de trabajo, dispositivos móviles, etc., contra intentos accidentales o maliciosos 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 con software antivirus actualizado.
- Existe una política acordada (Política de Ciclo de Vida de Usuarios) para proporcionar acceso temporal y limitado en el tiempo a “invitados” (por ejemplo, profesores en prácticas, suplentes, visitantes) a los sistemas del colegio
- *Existe una política acordada (AUP) sobre el alcance del uso personal permitido a los usuarios (personal/alumnos/usuarios de la comunidad) y sus familiares en dispositivos del colegio que puedan utilizarse fuera del colegio.*
- *Existe una política acordada (AUP) que permite/prohíbe al personal descargar archivos ejecutables e instalar programas en dispositivos del colegio.*
- *Existe una política acordada (AUP) 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 del colegio, a menos que estén aprobados, encriptados de forma segura o protegidos de otro modo

7. Tecnologías móviles (incluyendo BYOD/BYOT)

Los dispositivos de tecnología móvil pueden ser proporcionados o propiedad del colegio, o ser de propiedad personal y podrían incluir: teléfonos inteligentes, tabletas, portátiles u otros dispositivos que normalmente tengan la capacidad de utilizar la red inalámbrica del colegio. El dispositivo tendrá entonces acceso a internet, lo que puede incluir la plataforma de aprendizaje del colegio y otros servicios basados en la nube, como correo electrónico y almacenamiento de datos.

Todos los usuarios deben entender que el propósito principal del uso de dispositivos móviles/personales en el contexto del colegio es educativo. La política de tecnologías móviles debe ser coherente con y estar relacionada con otras políticas relevantes del colegio, incluyendo, entre otras, la Política de Protección, la Política de Comportamiento, la Política contra el Acoso, la Política de Uso Aceptable y las políticas relacionadas con el robo o los daños maliciosos. Enseñar sobre el uso seguro y apropiado de las tecnologías móviles es una parte integral del programa de educación en seguridad online del colegio.

Al preparar una política de tecnologías móviles, el colegio debe considerar posibles problemas y riesgos. Estos pueden incluir: riesgos de seguridad al permitir conexiones a la red del colegio, filtrado de dispositivos personales, roturas y seguros, acceso a dispositivos para todos los estudiantes, evitar distracciones potenciales en el aula, velocidades de conexión a la red, tipos de dispositivos, instalaciones para carga, coste total de propiedad. Es posible implementar una variedad de enfoques para la tecnología móvil.

El colegio puede, sin embargo, optar por incluir estos aspectos de su política en lugar de en una política separada de Tecnologías Móviles.

Lista de puntos a considerar.

- **Los Acuerdos de Uso Aceptable del colegio para personal, estudiantes y padres considerarán el uso de tecnologías móviles.**
- **El colegio permite**:

	Dispositivos del colegio			Dispositivos personales		
	Propiedad del colegio para un solo usuario	**Propiedad del colegio para múltiples usuarios**	**Dispositivo permitido[1]**	**Propiedad del alumno**	**Porpiedad del personal**	**Propiedad de visitante**
Permitido en el colegio	*Sí*	*Sí*	*Sí*	*Sí /No*	*Sí /No*	*Sí /No*
Acceso completo a la red	*Sí*	*Sí*	*Sí*	*No*	*Parcialmente*	*No*
Solo internet				*Sí - filtrado*	*Sí - filtrado*	*Sí - filtrado*
Sin acceso a la red						

Aspectos que el colegio puede considerar e incluir en su Política de Seguridad Online, Política de Tecnologías Móviles o Acuerdos de Uso Aceptable:

Dispositivos proporcionados por el colegio:

- A quién se asignarán.
- Dónde, cuándo y cómo se permite su uso (horarios/lugares/en el colegio/fuera del colegio).
- Si se permite el uso personal.
- Niveles de acceso a redes/internet (como se indica arriba).
- Gestión de dispositivos/instalación de aplicaciones/cambio de configuraciones/monitoreo/etiquetado de activos.
- Sistema de reservas para equipos en préstamo.
- Capacidad de red/banda ancha.

[1] Dispositivo autorizado: dispositivo adquirido por el alumno/familia a través de un plan organizado por el colegio. Este dispositivo puede recibir acceso completo a la red como si fuera propiedad del colegio.

- Soporte técnico.
- Filtrado de dispositivos.
- Acceso a servicios en la nube.
- Protección de datos.
- Captura/almacenamiento/uso de imágenes.
- Procesos de salida: qué sucede con los dispositivos/software/aplicaciones/datos almacenados cuando el usuario deja el colegio.
- Responsabilidad por daños.
- Formación del personal

7. 1 Dispositivos personales:

- Qué usuarios pueden usar dispositivos móviles personales en el colegio (personal / estudiantes / visitantes).
  • Restricciones sobre dónde, cuándo y cómo pueden ser utilizados en el colegio.
  • Almacenamiento.
  • Si el personal podrá utilizar dispositivos personales para asuntos del colegio.
  • Niveles de acceso a redes / internet (como se indicó anteriormente).
  • Capacidad de la red / banda ancha.
  • Soporte técnico (esto puede incluir una declaración clara de que no se ofrece soporte técnico).
  • Filtrado de la conexión a internet para estos dispositivos.
  • Protección de datos.
  • El derecho a tomar, examinar y registrar los dispositivos de los usuarios en caso de uso indebido (solo en Inglaterra); esta disposición también debe incluirse en la Política de Comportamiento.
  • Captura / almacenamiento / uso de imágenes.
  • Responsabilidad en caso de pérdida, daño o mal funcionamiento tras el acceso a la red (probablemente incluirá una cláusula de exención de responsabilidad del colegio).
  • Identificación / etiquetado de dispositivos personales.
  • Cómo se informará a los visitantes, incluidos contratistas externos, sobre los requisitos del colegio.
  • Cómo se integra la educación sobre el uso seguro y responsable de dispositivos móviles en los programas de educación sobre seguridad online del colegios

7. 2 Uso de imágenes digitales y de vídeo

El desarrollo de las tecnologías de imagen digital ha generado beneficios significativos para el aprendizaje, permitiendo al personal y a los estudiantes utilizar 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 caminos para que ocurra ciberacoso. Las imágenes digitales pueden permanecer disponibles en internet para siempre y pueden causar daño

o vergüenza a individuos a corto o largo plazo. Es común que los empleadores realicen búsquedas en internet para obtener información sobre empleados potenciales o actuales. El colegio informará y educará a los usuarios sobre estos riesgos e implementará políticas para reducir la probabilidad de que se produzcan daños:

- **Al utilizar imágenes digitales, el personal debe informar y educar a los estudiantes sobre los riesgos asociados con la captura, uso, compartición, publicación y distribución de imágenes. Deben reconocer los riesgos relacionados con la publicación de sus propias imágenes en internet, por ejemplo, en redes sociales.**

- **Se obtendrá el permiso por escrito de los padres antes de publicar fotografías de estudiantes en la página web del colegio / redes sociales / prensa local** (puede estar cubierto como parte del Acuerdo de Uso Aceptable firmado por los padres o tutores al inicio del curso; consultar el Acuerdo de Uso Aceptable para Padres disponible en la Oficina Central)

- De acuerdo con la guía de la Oficina del Comisionado de Información del Reino Unido (los directores deben buscar aclaración sobre los requisitos legales / legislación del país anfitrión), los padres pueden tomar vídeos e imágenes digitales de sus hijos en eventos escolares para su uso personal. Para respetar la privacidad de todos y, en algunos casos, la protección, estas imágenes **no deben** publicarse / hacerse públicas en redes sociales, **ni los padres deben** comentar sobre actividades que involucren a otros estudiantes en las imágenes digitales / de vídeo.

- El personal y los voluntarios pueden tomar imágenes digitales / de vídeo para apoyar objetivos educativos, pero deben seguir las políticas del colegio con respecto a la compartición, distribución y publicación de dichas imágenes. Estas imágenes deben tomarse únicamente con el equipo del colegio; no debe utilizarse el equipo personal del personal para estos fines.
  • Se debe tener cuidado al tomar imágenes digitales / de vídeo para asegurarse de que los estudiantes estén vestidos de manera adecuada y no participen en actividades que puedan desacreditar a los individuos o al colegio.
  • Los estudiantes no deben capturar, usar, compartir, publicar o distribuir imágenes de otros sin su permiso.
  • Las fotografías publicadas en la página web u otros medios que incluyan a estudiantes serán seleccionadas cuidadosamente y cumplirán con las buenas prácticas sobre el uso de dichas imágenes.
  • Los nombres completos de los estudiantes no se usarán en ninguna página web o blog, especialmente en asociación con fotografías.
  • El trabajo de los estudiantes solo se podrá publicar con el permiso del estudiante y de los padres.

8. Protección de datos

Con efecto desde el 25 de mayo de 2018, los arreglos para la protección de datos en el Reino Unido cambian debido a la entrada en vigor del Reglamento General de Protección de Datos

(GDPR) de la Unión Europea. Como resultado, es probable que los colegios estén sujetos a una mayor supervisión en el cuidado y uso de los datos personales. Se puede obtener una guía más detallada en la Oficina Central de Orbital.

Los datos personales se registrarán, procesarán, transferirán y estarán disponibles de acuerdo con la legislación actual de protección de datos.

El colegio debe asegurarse de que:

- Tiene una Política de Protección de Datos (esta puede solicitarse a la Oficina Central de Orbital).
- Posee únicamente los datos personales mínimos necesarios para llevar a cabo su función y no los conservará más tiempo del necesario para los fines para los que fueron recopilados.
- Los datos archivados son precisos y están actualizados. Las inexactitudes se corrigen sin demoras innecesarias.
- Se ha identificado y documentado la base legal para procesar datos personales (incluyendo, cuando sea relevante, el consentimiento) y los detalles se proporcionan en un Aviso de Privacidad.
- Cuando se procesen datos de categorías especiales, se ha identificado una base legal y una condición separada para su procesamiento.
- Se realizan Evaluaciones de Impacto en la Protección de Datos (DPIA) al introducir nuevos procesos o tecnologías en el colegio que procesen datos personales.
- Existen disposiciones claras y comprendidas sobre el acceso, la seguridad, el almacenamiento y la transferencia de datos personales, incluyendo, cuando sea necesario, cláusulas contractuales adecuadas o salvaguardas si los datos personales se transfieren a terceros (por ejemplo, proveedores de servicios en la nube). Puede ser necesario un acuerdo de manejo de datos confirmand si los datos son accesibles o proporcionados a un tercero.
- Están establecidos procedimientos para gestionar los derechos individuales del sujeto de los datos, como las Solicitudes de Acceso del Interesado, para ver todos o parte de sus datos personales mantenidos por el controlador de datos.
- Existen políticas claras y comprendidas de retención de datos y rutinas para la eliminación y disposición de los datos.
- Hay una política para informar, registrar, gestionar y recuperarse de incidentes de riesgo de información que reconozca la obligación de reportar las brechas relevantes de datos al ICO dentro de las 72 horas de ocurrido el incidente, cuando sea factible.
- Se ha considerado la protección de datos personales al acceder a ellos mediante soluciones de acceso remoto.
- Todos los colegios / academias (incluidas las academias que anteriormente estaban exentas) tienen una Política de Libertad de Información que establece cómo tratarán las solicitudes de FOI.
- Todo el personal recibe formación sobre el manejo y la protección de datos y es consciente de sus responsabilidades

El personal debe asegurarse de que:

- **En todo momento toman medidas para garantizar la protección de los datos personales, minimizando el riesgo de pérdida o uso indebido.**
- **Usan datos personales únicamente en dispositivos protegidos por contraseña, asegurándose de cerrar la sesión correctamente al finalizar cualquier uso de datos personales.**
- **Transfieren datos utilizando dispositivos encriptados y protegidos por contraseña**

Cuando los datos personales se almacenan en sistemas portátiles, memorias USB u otros medios extraíbles:

- **Los datos deben estar encriptados y protegidos por contraseña.**
- El dispositivo debe estar protegido por contraseña (muchos dispositivos como memorias USB / tarjetas y otros dispositivos móviles no permiten esta protección).
- **El dispositivo debe ofrecer software aprobado de comprobación de virus y malware.**
- **Los datos deben eliminarse de manera segura del dispositivo, conforme a la política del colegio, una vez transferidos o finalizado su uso**

9. Comunicados

Esta es un área de tecnologías y usos en rápido desarrollo. Los colegios deberán debatir y acordar cómo pretenden implementar y utilizar estas tecnologías; por ejemplo, algunos colegios no permiten que los estudiantes usen teléfonos móviles en las clases, mientras que otros reconocen su potencial educativo y permiten su uso. Esta sección también puede estar influenciada por la edad de los estudiantes.

Una amplia gama de tecnologías de comunicación en rápido desarrollo tiene el potencial de mejorar el aprendizaje. La siguiente tabla muestra cómo el colegio considera actualmente que los beneficios de utilizar estas tecnologías para la educación superan sus riesgos o desventajas:

Tecnología de Comunicación	Personal y demás adultos			Alumnado				
	Permitido	Permitido en determinados momenots	Permitido para personal seleccionado	No permitido	Permitido	Permitido en determinados momentos	Permitido con permiso del personal	No permitido
Los teléfonos móviles pueden ser llevados al colegio / academia								
Uso de teléfonos móviles en las clases								
Uso de teléfonos móviles durante el tiempo social								
Tomar fotos con teléfonos móviles / cámaras								
Uso de otros dispositivos móviles, p. ej., tabletas, consolas de juegos								
Uso de direcciones de correo electrónico personales en el colegio o en la red del colegio								
Uso del correo electrónico del colegio para correos personales								
Uso de aplicaciones de mensajería								
Uso de redes sociales								
Uso de blogs								

10. Orbital recomienda encarecidamente que los colegios incluyan las siguientes declaraciones:

El colegio también puede considerar añadir algunas de las siguientes declaraciones de política sobre el uso de tecnologías de comunicación, en lugar de, o además de la tabla anterior:

Al usar tecnologías de comunicación, el colegio considera las siguientes prácticas como buenas:

- **El servicio de correo electrónico oficial del colegio se considera seguro, protegido y monitorizado. Los usuarios deben ser conscientes de que las comunicaciones por correo electrónico están supervisadas.** Por lo tanto, el personal y los estudiantes deben utilizar únicamente el servicio de correo electrónico del colegio para comunicarse con otros mientras estén en el colegio o usando sistemas del colegio (por ejemplo, acceso remoto).
- **Los usuarios deben informar de inmediato a la persona designada, según la política del colegio, sobre la recepción de cualquier comunicado que les haga sentir incómodos, sea ofensivo, discriminatorio, amenazante o de naturaleza intimidatoria, y no deben responder a dichas comunicaciones.**
- **Toda comunicación digital entre el personal y los estudiantes o padres (correo electrónico, redes sociales, chats, blogs, entornos virtuales de aprendizaje, etc.) debe ser profesional en tono y contenido.** *Estas comunicaciones solo pueden realizarse a través de sistemas oficiales (monitorizados) del colegio. No se deben usar direcciones de correo electrónico personales, mensajes de texto ni redes sociales para estas comunicaciones.*
- *Para estudiantes de 3º Infantil y 1º Primaria se pueden usar direcciones de correo electrónico para toda la clase o grupo. Los estudiantes de 2º Priamria y niveles superiores recibirán direcciones de correo electrónico individuales para uso educativo.* (El colegio puede optar por usar direcciones grupales para estudiantes más jóvenes)
- ***Los estudiantes deben formarse sobre problemas de seguridad online, como los riesgos de compartir información personal. También deben aprender estrategias para lidiar con comunicaciones inapropiadas y ser recordados sobre la necesidad de comunicarse adecuadamente al usar tecnologías digitales.***
- ***No se debe publicar información personal en la página web del colegio, y solo se deben usar direcciones de correo oficiales para identificar a los miembros del personal***

Redes Sociales: Protección de la Identidad Profesional

Con el aumento del uso de todo tipo de redes sociales con fines profesionales y personales, es esencial contar con una política que proporcione una guía clara para que el personal gestione riesgos y comportamientos online. Los mensajes clave deben incluir la protección de los estudiantes, el colegio y el individuo al publicar cualquier material online. **Las expectativas para la conducta profesional de los profesores están establecidas en los 'Teachers Standards 2012' (que las Escuelas Orbital han incorporado en su Código de Conducta del Personal o tienen como una política independiente de Estándares para Profesores). El marco de inspección de seguridad online de Ofsted y los estándares de acreditación de CIS/COBIS revisan cómo un colegio protege y educa al personal y a los estudiantes en su uso de la tecnología, incluyendo las medidas que se esperarían para intervenir y brindar apoyo en caso de que surja un problema**. Los colegios están utilizando cada vez más las redes sociales como una poderosa herramienta de aprendizaje y un medio de comunicación. Es importante que esto se lleve a cabo de manera segura y responsable.

Una Política Modelo de Redes Sociales más detallada está disponible en la Oficina Central de Orbital. Sin embargo, el colegio puede optar por incluir estos aspectos de su política en un Acuerdo de Uso Aceptable integral, en lugar de en una Política de Redes Sociales independiente. Se sugiere que el colegio en este documento de política general esboce los puntos principales de su política acordada. A continuación, se incluye una lista de verificación de puntos a considerar.

Todas los colegios tienen el deber de cuidado de proporcionar un entorno de aprendizaje seguro para estudiantes y personal. Los colegios podrían ser consideradas responsables, indirectamente, de los actos de sus empleados durante su empleo. Los miembros del personal que acosen, participen en intimidación online, discriminen por motivos de sexo, raza o discapacidad, o que difamen a un tercero pueden hacer que el colegio sea responsable ante la parte perjudicada. Deben estar en vigor medidas razonables para prevenir daños previsibles.

El colegio proporciona las siguientes medidas para garantizar que se tomen medidas razonables para minimizar el riesgo de daño a estudiantes, personal y al colegio mediante:

- Garantizar que no se publique información personal.
- Proporcionar formación que incluya uso aceptable; riesgos de redes sociales; revisión de configuraciones; protección de datos; reporte de problemas.
- Directrices claras de reporte, incluyendo responsabilidades, procedimientos y sanciones.
- Evaluación de riesgos, incluyendo riesgos legales

El personal del colegio debe asegurarse de que:

- No se haga referencia en redes sociales a estudiantes, padres o personal del colegio.
- No participen en discusiones online sobre asuntos personales relacionados con miembros de la comunidad escolar.
- Las opiniones personales no se atribuyan al colegio ni a Orbital Education.
- Las configuraciones de seguridad en los perfiles personales de redes sociales se revisen regularmente para minimizar el riesgo de pérdida de información personal

Cuando se establezcan cuentas oficiales de redes sociales del colegio, se deben tener en cuenta:

- Un proceso de aprobación por parte de los líderes senior.
- Procesos claros para la administración y supervisión de estas cuentas, involucrando al menos a dos miembros del personal.
- Un código de conducta para los usuarios de las cuentas, incluyendo:
    - Sistemas para reportar y abordar abusos y mal uso.
    - Comprensión de cómo se pueden tratar los incidentes según los procedimientos disciplinarios del colegio

Uso Personal:

- Las comunicaciones personales son aquellas realizadas a través de una cuenta personal de redes sociales. En todos los casos, donde se use una cuenta personal que se asocie al colegio o impacte en el colegio, debe quedar claro que el miembro del personal no está comunicándose en nombre del colegio mediante un descargo de responsabilidad adecuado. Dichas comunicaciones personales están dentro del alcance de esta política.
- Las comunicaciones personales que no se refieran ni impacten en el colegio están fuera del alcance de esta política.
- Si se sospecha un uso personal excesivo de redes sociales en el colegio y se considera que interfiere con las funciones relevantes, pueden tomarse medidas disciplinarias.
- **El colegio permite un acceso razonable y apropiado a sitios de redes sociales privadas**

Supervisión de Redes Sociales Públicas

- Como parte del compromiso activo en redes sociales, se considera buena práctica monitorizar proactivamente publicaciones públicas sobre el colegio.
- El colegio debe responder efectivamente a los comentarios en redes sociales realizados por otros según una política o proceso definido

El uso de redes sociales del colegio con fines profesionales será revisado regularmente por el oficial senior de riesgos y el Gestor del Grupo de Seguridad Online para garantizar el cumplimiento de las políticas del colegio.

11. Cómo afrontar actividades inadecuadas o inapropiadas

Algunas actividades en internet, como acceder a imágenes de abuso infantil o distribuir material racista, son ilegales y obviamente estarían prohibidas en el colegio y en todos los demás sistemas técnicos. Otras actividades, como el ciberacoso, estarían prohibidas y podrían llevar a una acusación criminal. Sin embargo, existen una serie de actividades que, generalmente, pueden ser legales pero que serían inapropiadas en un contexto escolar, ya sea por la edad de los usuarios o

por la naturaleza de dichas actividades.
El colegio cree que las actividades mencionadas en la siguiente sección serían inapropiadas en un contexto escolar y que los usuarios, tal y como se definen a continuación, no deben participar en estas actividades dentro o fuera del colegio al utilizar los equipos o sistemas del colegio. La política del colegio restringe el uso de la siguiente manera:

Acciones del usuario		Aceptable	Aceptable en determinados moementos	Aceptable para usuarios designados	Inaceptable	Inaceptable e ilegal
Los usuarios no podrán visitar webs de Internet, realizar, publicar, descargar, subir, transferir datos, comunicar o transmitir material, observaciones, propuestas o comentarios que contengan o se relacionen con:	Imágenes de abuso sexual a menores: la creación, producción o distribución de imágenes indecentes de menores. Contrario al *Protection of Children Act* de 1978					X
	Acoso, incitación, organización o facilitación de actos sexuales contra menores. Contrario al *Sexual Offences Act* de 2003.					X
	Posesión de una imagen pornográfica extrema (gravemente ofensiva, repugnante o de otro carácter obsceno). Contrario al *Criminal Justice and Immigration Act* de 2008					X
	Material racista criminal: incitación al odio religioso (o al odio por motivos de orientación sexual), contrario al *Public Order Act* de 1986					X
	Pornografía				X	
	Promoción de cualquier tipo de discriminación				X	
	Comportamiento amenazante, incluida la promoción de violencia física o daño mental				X	
	Promoción del extremismo o terrorismo				X	

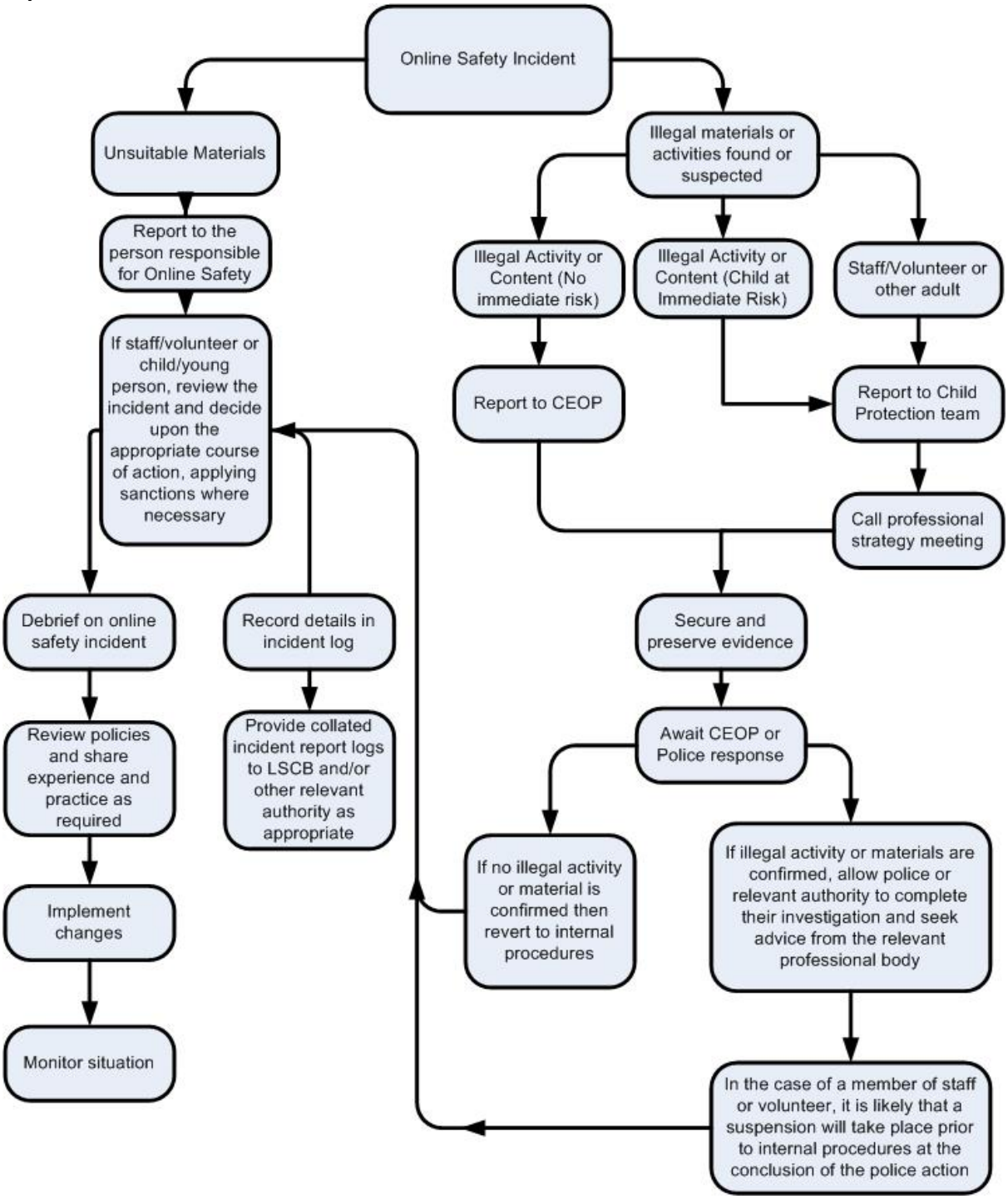
	Cualquier otra información que pueda resultar ofensiva para los compañeros o que vulnere la integridad del espíritu del colegio o desacredite al colegio				X	
Usar los sistemas del colegio para gestionar un negocio privado					X	
Usar sistemas, aplicaciones, páginas web u otros mecanismos que eludan los filtros u otras medidas de seguridad implementadas por el colegio					X	
Infracción de derechos de autor					X	
Revelar o hacer pública información confidencial o propietaria (por ejemplo, información financiera / personal, bases de datos, códigos de acceso a ordenadores / redes y contraseñas)					X	
Crear o propagar virus informáticos u otros archivos dañinos					X	
Uso injusto (descargar / subir archivos grandes que dificulten el uso de internet por parte de otros)					X	
Juegos online (educativos)						
Juegos online (no educativos)						
Apuestas online						
Compras / comercio online						
Compartición de archivos						
Uso de redes sociales - ver más arriba						
Uso de aplicaciones de mensajería						
Uso de transmisiones de vídeo, como YouTube						

12. Responder a incidentes de uso indebido

Esta guía está destinada a ser utilizada cuando el personal necesite gestionar incidentes que impliquen el uso de servicios online. Fomenta un enfoque seguro y protegido para la gestión del incidente. Los incidentes pueden involucrar actividades ilegales o inapropiadas (ver "Acciones del usuario" arriba).

12.1 Incidentes ilegales

Si hay alguna sospecha de que la página web(s) en cuestión puede contener imágenes de abuso a menores, o si hay alguna otra actividad sospechosa de ser ilegal, consulte el lado derecho del diagrama de flujo para responder a incidentes de seguridad online y repórtelo inmediatamente a la policía.



12.2 Otros incidentes

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

En caso de sospecha, se deben seguir todos los pasos de este procedimiento:

- Involucra a más de un miembro senior del personal en este proceso. Esto es vital para proteger a los individuos en caso de que se reporten acusaciones posteriormente.
- Realiza el procedimiento utilizando un ordenador designado que no será usado por jóvenes y que, si es necesario, puede ser retirado del centro por la policía en caso de que surja la necesidad. Utiliza el mismo ordenador durante todo el procedimiento.
- Es importante asegurar 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 proporcionar una protección adicional).
- Trata de mantener un cronograma de los eventos de la investigación a medida que se realicen, esto facilitará posteriormente si la policía solicita una declaración de la secuencia de los hechos.
- Registra la URL de cualquier sitio que contenga el uso indebido alegado y describe la naturaleza del contenido que causa preocupación. También puede ser necesario registrar y almacenar capturas de pantalla del contenido en el ordenador que se esté utilizando para la investigación. **Estas pueden ser impresas, firmadas y adjuntadas al formulario (excepto en el caso de imágenes de abuso sexual de menores – véase abajo)**
- Una vez que esto se haya completado e investigado a fondo, el grupo deberá juzgar si esta preocupación tiene fundamento o no. Si lo tiene, se requerirá una acción adecuada que podría incluir lo siguiente:
    - Respuesta interna o procedimientos disciplinarios
    - Involucramiento del Jefe Regional de Colegios/Grupo o de la organización nacional/local (según corresponda).
    - Involucramiento y/o acción policial
- **Si el contenido que se revisa incluye imágenes de abuso a menores, entonces la supervisión debe ser detenida y debe ser referido al Jefe Regional de Colegios y a la Policía de inmediato. Otros casos que deben ser reportados a la policía incluyen:**
    - incidentes de comportamientos de 'acercamiento'
    - el envío de materiales obscenos a un menor
    - material para adultos que potencialmente infrinja la Ley de Publicaciones Obscenas

- material criminalmente racista
- promoción del terrorismo o extremismo
- otras conductas, actividades o materiales criminales

- **Aísla el ordenador en cuestión lo mejor que puedas. Cualquier cambio en su estado puede dificultar una posterior investigación policial.**

Es importante que se sigan todos los pasos anteriores, ya que proporcionarán una prueba de la cadena de evidencias para el colegio y posiblemente para la policía, y demostrarán que las visitas a estos sitios se realizaron con fines de protección. El formulario completo debe ser retenido por el grupo como prueba y para fines de referencia.

13. Acciones y sanciones del colegio

Es más probable que el colegio tenga que gestionar incidentes que involucren un uso inapropiado en lugar de uno ilegal. Es importante que cualquier incidente se gestione lo antes posible de manera proporcionada, y que los miembros de la comunidad escolar sepan que los incidentes han sido tratados. Se pretende que los incidentes de uso indebido se gestionen a través de los procedimientos normales de comportamiento / disciplina de la siguiente manera:

	Acciones / Sanciones								
Incidentes con el alumnado	Referir al tutor	Referir al Jefe de Estudios	Referir al Director	Referir a la Policía	Referir al personal de soporte técnico para acciones relacionadas con filtrado / seguridad, etc	Informar a los padres / tutores	Retirar los derechos de acceso a la red /	Advertencia	Sanción adicional, por ejemplo, detención / expulsión
Acceder deliberadamente o intentar acceder a material que podría considerarse ilegal (ver lista en la sección anterior sobre actividades inapropiadas / inadecuadas).		X	X	X					

Uso no autorizado de sitios no educativos durante las clases									
Uso no autorizado / inapropiado de teléfono móvil / cámara digital / otro dispositivo móvil									
Uso no autorizado / inapropiado de redes sociales / aplicaciones de mensajería / correo electrónico personal									
Descarga o carga no autorizada de archivos									
Permitir que otros accedan a la red del colegio compartiendo el nombre de usuario y las contraseñas									
Intentar acceder o acceder a la red del colegio utilizando la cuenta de otro estudiante									
Intentar acceder o acceder a la red del colegio utilizando la cuenta de un miembro del personal									
Corromper o destruir los datos de otros usuarios									
Enviar un correo electrónico, mensaje de texto o mensaje que se considere ofensivo, acoso o de naturaleza intimidatoria									
Infracciones continuadas de lo anterior, tras advertencias o sanciones previas									
Acciones que podrían dañar la reputación del colegio o vulnerar la integridad de su ethos									
Uso de sitios proxy u otros medios para eludir el sistema de filtrado del colegio									
Acceder accidentalmente a material ofensivo o pornográfico y no informar del incidente									

Acceder deliberadamente o intentar acceder a material ofensivo o pornográfico									
Recepción o transmisión de material que infrinja los derechos de autor de otra persona o que infrinja la Ley de Protección de Datos									

Acciones / Sanciones

Incidentes con el personal	Referir al responsable directo	Referir al Director	Referir al Jefe Regional de Colegios / Recursos Humanos	Referir a la Policía	Referir al personal de soporte técnico para acciones relacionadas con filtrado, etc.	Advertencia	Suspensión	Acción disciplinaria
Acceder deliberadamente o intentar acceder a material que podría considerarse ilegal (ver lista en la sección anterior sobre actividades inapropiadas / inadecuadas).		X	X	X				
Uso personal inapropiado de internet / redes sociales / correo electrónico personal								
Descarga o carga no autorizada de archivos								
Permitir que otros accedan a la red del colegio compartiendo el nombre de usuario y las contraseñas o intentar acceder a la red del colegio utilizando la cuenta de otra persona								
Uso descuidado de datos personales, por ejemplo, almacenar o transferir datos de manera insegura								

Acciones deliberadas para vulnerar las normas de protección de datos o de seguridad de la red								
Corromper o destruir los datos de otros usuarios o causar daño deliberado a hardware o software								
Enviar un correo electrónico, mensaje de texto o mensaje que se considere ofensivo, acoso o de naturaleza intimidatoria								
Usar correo electrónico personal / redes sociales / mensajería instantánea / mensajes de texto para llevar a cabo comunicaciones digitales con estudiantes								
Acciones que podrían comprometer la reputación profesional del miembro del personal								
Acciones que podrían dañar la reputación del colegio o vulnerar la integridad de su ethos								
Uso de sitios proxy u otros medios para eludir el sistema de filtrado del colegio								
Acceder accidentalmente a material ofensivo o pornográfico y no informar del incidente								
Acceder deliberadamente o intentar acceder a material ofensivo o pornográfico								
Vulnerar las normativas de derechos de autor o de licencias								
Infracciones continuadas de lo anterior, tras advertencias o sanciones previas								