Política de seguridad de TIC

Titular de la póliza: The British School of Almería

Ámbito de actuación: Salvaguarda

Revisado: julio de 2025

Próxima revisión: julio de 2026

JUSTIFICACIÓN Y ORIENTACIÓN

THE BRITISH SCHOOL OF ALMERÍA. espera que todo el personal y voluntarios de nuestro colegio y cualquier contratista o personal de agencia asociada utilizada por el colegio, reconozcan dónde un alumno está en riesgo, o realmente está siendo perjudicado y hacen todo lo posible para reducir el riesgo o daño adicional.

El colegio reconoce que la seguridad electrónica es un elemento esencial para proteger a niños y adultos en el mundo digital. Internet y las tecnologías de la información y la comunicación son ahora una parte importante de la vida cotidiana. Este documento destaca las diferentes áreas de las TIC y la seguridad electrónica y los procedimientos que se espera que sigan todos los miembros del personal y el alumnado dentro del colegio.

DEFINICIÓN

El término TIC incluye, pero no se limita a:

- Cualquier ordenador, tablet o portátil
- Cualquier dispositivo que tenga acceso, ya sea fijo o móvil, a salas de chat, redes sociales, podcasts, servicios de mensajería instantánea, tecnologías de seguimiento de ubicación y/o GPS.
- Dispositivos y acceso inalámbricos y de banda ancha
- Teléfonos móviles
- Consolas y dispositivos de juego
- La descarga y difusión de música
- Cámaras digitales
- Dispositivos de visualización como pizarras
- Impresoras o fotocopiadoras
- Software utilizado con fines comerciales o educativos

IMÁGENES DIGITALES Y VÍDEO

El uso de video e imágenes digitales juega un papel importante en las actividades de aprendizaje. El alumnado y los miembros del personal pueden usar una variedad de dispositivos para registrar

evidencia de actividades en las clases y fuera del colegio. Estas imágenes se pueden utilizar para una variedad de propósitos educativos. También se reconoce que el mayor uso de la tecnología ha aumentado la posibilidad de que los dispositivos y las imágenes se utilicen indebidamente. Para garantizar la seguridad de todo el alumnado dentro del colegio, se deben seguir las siguientes pautas en todo momento:

Directrices para el personal:

1. Las fotos y videos del alumnado deben tomarse con una cámara del colegio. Los dispositivos personales sólo deben usarse como último recurso cuando no haya una cámara escolar disponible.
2. Las fotos / videos de cualquier niño/a en el colegio solo se pueden tomar por razones académicas, para ser utilizadas sólo dentro del colegio (evaluaciones, exhibiciones, etc.)
3. Cualquier imagen/video tomado con un dispositivo personal de cualquier niño/a en edad escolar durante el día escolar, ya sea dentro o fuera del edificio escolar por razones académicas (incluidos los viajes) **DEBE** descargarse lo antes posible a la carpeta de fotos del colegio y las imágenes/videos deben eliminarse inmediatamente del dispositivo personal.
4. No se permite compartir en una cuenta personal de redes sociales (Twitter, Facebook, Instagram, etc.) fotos / videos tomados por un miembro del personal durante el día escolar en una cuenta personal de redes sociales (Twitter, Facebook, Instagram, etc.) sin la aprobación previa por escrito de la dirección del colegio y / o las familias.
5. Cualquier foto / video de cualquier niño/a del colegio compartida entre miembros del personal por razones académicas **DEBE** descargarse a la carpeta oficial de Fotos del colegio **Y** debe eliminarse inmediatamente de ambos dispositivos después de recibirse.
6. No se permite compartir imágenes con personas que no sean miembros del personal (por ejemplo, fotos o vídeos de niños/as en edad escolar tomados con un dispositivo personal durante la jornada escolar (enviados a amigos o familiares mediante Messenger o Whatsapp) sin **la aprobación previa por escrito** de la dirección del colegio y/o de las familias.
7. Cuando la **dirección y/o las familias hayan otorgado la aprobación previa por escrito** de las pautas mencionadas anteriormente, la cara del niño/a o niños/as debe estar cubierta/borrosa y NO se permite compartir datos personales del niño/a (niños/as) (nombre, edad, etc.)
8. Las pautas anteriores también se aplican a los miembros del personal que también son padres/madres. Se espera que los profesores sean profesionales durante el día escolar. Por lo tanto, se espera que un miembro del personal solicite la aprobación previa de la directora antes de tomar fotografías de sus hijos durante el día escolar, para eventos escolares especiales cuando otras familias no están en el colegio.

NOTA: Cuando el **responsable** haya otorgado la aprobación previa por escrito de lo mencionado anteriormente, se debe seguir la pauta 7.

PÁGINA WEB Y REDES SOCIALES

El colegio obtendrá el consentimiento por escrito de las familias o tutores al comienzo del año académico antes de publicar una imagen de ellos o de su(s) hijo(s) en la página web del colegio o en las cuentas de redes sociales.

REDES SOCIALES

Profesores, alumnado y familias interactúan con las aplicaciones de redes sociales. Estas aplicaciones incluyen, entre otras, Facebook, Snapchat, Instagram, Twitter, blogs y otras herramientas online a través de las cuales las personas se conectan y comparten información. Se espera que todos los miembros de la comunidad escolar defiendan los valores del colegio en todas las interacciones en las redes sociales. El personal, el alumnado y las familias no actuarán de manera que se desacredite la imagen del colegio ni de una manera que perjudique a los miembros de la comunidad escolar.

Directrices para el personal y el profesor

1. Las redes sociales en relación con el personal y los profesores se relacionan con blogs, wikis, podcasts, imágenes y videos digitales, mensajería instantánea y dispositivos móviles.
2. Las aplicaciones de redes sociales como Facebook o Instagram no deben ser utilizadas por el personal como una plataforma para actividades de aprendizaje con el alumnado.
3. El personal no debe aceptar el alumnado como "amigos" en sus propias redes sociales ni interactuar con el alumnado.
4. La interacción online entre el personal y el alumnado debe ocurrir sólo en un contexto educativo.
5. Se aconseja a los miembros del personal que **NO** acepten a ex alumnos o familias del alumnado actual como amigos en redes sociales personales.
6. El personal no debe hablar sobre el alumnado o compañeros ni criticar públicamente las políticas del colegio o el personal en las redes sociales.
7. El personal debe evitar publicar comentarios en las redes sociales que puedan considerarse ofensivos o irrespetuosos para una persona u organización, especialmente en foros abiertos.
8. Los miembros del personal no tienen permiso para publicar fotos o detalles que identifiquen a ningún niño/a en sus redes sociales.
9. Los miembros del personal son personalmente responsables del contenido que publican online. Los miembros del personal deben ser conscientes de que lo que publiquen será público durante mucho tiempo.
10. El personal no debe participar en la difusión de rumores falsos o infundados o información falsa con respecto a la comunidad escolar y sus miembros.
11. Al conectarse online, el personal no debe publicar información confidencial del alumnado.
12. El personal debe visitar la configuración de seguridad y privacidad de su perfil en las páginas de redes sociales. Como mínimo, el personal debe tener todas las configuraciones de privacidad configuradas como "privado" y "solo amigos".

SEGURIDAD ELECTRÓNICA Y PROTECCIÓN ONLINE

Internet es ahora un recurso invaluable para el aprendizaje de todo nuestro alumnado y, como colegio, lo usamos en todo el plan de estudios para buscar información y como fuente de

materiales de aprendizaje digitales. Sin embargo, Internet puede ser inseguro cuando no se implementan y no se siguen los procedimientos adecuados. Se deben cumplir los siguientes principios para garantizar la seguridad online de todo el alumnado y del personal:

1. **Personal del colegio**

- Todos los miembros del personal son responsables de promover y apoyar comportamientos seguros en el colegio y de seguir los procedimientos de seguridad electrónica del colegio.
- Todos los miembros del personal deben fomentar una cultura de "No culpar" para que el alumnado se sienta capaz de denunciar cualquier acoso, abuso o contacto con materiales inapropiados online.
- Los profesores de clase deben asegurarse de que el alumnado conozca las reglas de seguridad electrónica, introducidas al comienzo de cada nuevo año escolar.
- Los profesores de clase deben planificar cuidadosamente toda la enseñanza basada en Internet para asegurarse de que el alumnado no acceda accidentalmente a contenidos inapropiados.
- Se espera que los miembros del personal firmen anualmente el Acuerdo de **Uso Aceptable de Internet** para el Personal.

2. **Alumnado**

- Se le debe enseñar a comprender la importancia de denunciar el abuso, el uso indebido o el acceso a materiales inapropiados y saber cómo hacerlo.
- Se debe enseñar la importancia de adoptar buenas prácticas de seguridad online cuando se utilizan tecnologías digitales dentro y fuera del colegio.
- Se le debe enseñar a tener una buena comprensión de las habilidades de investigación y la necesidad de evitar sitios peligrosos / dañinos, plagio y cumplir con las regulaciones de derechos de autor.
- Se debe enseñar a usar los motores de búsqueda y a evaluar la información basada en Internet como parte del currículo de Informática, y en otras áreas del currículo donde sea necesario. () Se debe enseñar a reconocer la diferencia entre páginas web comerciales y no comerciales.
- Se debe enseñar a llevar a cabo comprobaciones sencillas de riesgos y desinformación.
- Todo el alumnado es responsable de usar los sistemas de TIC del colegio de acuerdo con **la Política de Uso Aceptable para el alumnado**, que se espera que cumplan/acepten antes de que se les dé acceso a los sistemas escolares.
-

3. Familias/Tutores

Las familias/tutores desempeñan un papel crucial para garantizar que sus hijos/as comprendan la necesidad de utilizar Internet / dispositivos móviles de manera adecuada. Muchas familias y cuidadores no comprenden completamente los problemas y tienen menos experiencia en el uso de las TIC que sus hijos/as. Por lo tanto, el colegio aprovechará todas las oportunidades para ayudar a las familias a comprender estos temas a través de la información en las tutorías, apoyo y reuniones informativos con la policía nacional; boletines informativos, correos electrónicos, la página web del colegio e información sobre campañas de seguridad online/ literatura nacional / local.

Los padres y cuidadores serán responsables de:

- Respaldar y aceptar la Política de Uso Aceptable para el alumnado
- Enseñar a sus hijos/as la importancia de adoptar buenas prácticas de seguridad online al usar tecnologías digitales dentro y fuera del colegio.

4. Medios de almacenamiento portátiles

Los miembros del personal pueden usar dispositivos portátiles de almacenamiento como (USB y discos duros externos) solo con fines académicos. Si el uso de un dispositivo de este tipo da como resultado un mensaje antivirus, el dispositivo debe retirarse inmediatamente y se debe enviar un informe al administrador de informática del colegio / técnico de TI. El personal y el alumnado deben evitar el uso de cualquier dispositivo USB si no conocen previamente la fuente y / o el contenido almacenado.

5. Descarga de archivos y aplicaciones

Internet es una rica fuente de archivos, aplicaciones, software, juegos y otros materiales gratuitos que se pueden descargar e instalar en un ordenador. Si bien parte de este material puede ser útil, gran parte es inapropiado y puede afectar negativamente el rendimiento y la confiabilidad del equipo escolar.

- Los miembros del personal deben asegurarse de verificar la confiabilidad de la página web y el contenido antes de descargar material en un ordenador escolar.
- Al alumnado NO se les permite descargar ningún material de Internet a menos que se lo indique un miembro del profesorado apropiado.

6. Filtro de contenido

El colegio utiliza un sofisticado filtro de contenido para garantizar que, en la medida de lo posible, solo el contenido apropiado de Internet llegue al colegio. Si bien esta tecnología de filtrado es robusta y generalmente efectiva para bloquear material inadecuado, aún es posible que el material inadecuado pase ocasionalmente por el filtro.

- Todo el alumnado y el personal deben seguir las pautas de presentación de informes que se describen a continuación si esto sucede, y las familias/tutores serán informados cuando sea necesario.
- El alumnado o el personal que intenten deliberadamente acceder a materiales inadecuados serán tratados de acuerdo con los procedimientos que se describen a continuación.

* Se enviarán alertas automáticas al director si los alumnos o el personal intentan acceder a materiales inapropiados en un dispositivo escolar

7. Smoothwall

El colegio utiliza un sistema llamado Smoothwall que detecta cualquier comentario/comportamiento irresponsable o preocupante del alumnado y del personal al acceder a la red del colegio. En caso de que surja algún problema, se envía automáticamente una notificación a la Directora/Líder Designada de Salvaguarda (DSL). Estas inquietudes serán objeto de seguimiento por parte de la Directora/DSL o de un miembro del Equipo de Salvaguarda.

8. Acoso online

El acoso online se refiere al "**uso repetido de la comunicación electrónica en cualquier forma, en cualquier plataforma, que causaría daño o angustia a otra persona**".

El colegio tiene un enfoque de tolerancia cero al acoso y se toma muy en serio cualquier incidente de acoso online. Cualquier acoso online será tratado por el colegio siguiendo los procedimientos que se describen a continuación.

NOTIFICACIÓN DE INCIDENTES DE TIC O SEGURIDAD ELECTRÓNICA

1. Cualquier preocupación sobre la protección o el uso indebido de cualquier TIC dentro o fuera del colegio debe informarse utilizando el proceso normal de Motivo de preocupación de la escuela "MyConcern". Se debe enviar un informe al Líder Designado de Salvaguarda. Por otra parte, si se considera que puede producirse un conflicto de intereses, el miembro del personal debe informar del incidente a cualquier otro miembro del Equipo de Salvaguarda. Si se sospecha que en algún momento un alumno/a puede haber sido o se considera que es objeto de abuso, el colegio debe seguir inmediatamente la política y los procedimientos de salvaguarda. No se debe intentar descargar, imprimir o enviar ningún material inapropiado que se encuentre, ya que al hacerlo se podrían cometer más delitos.
2. El personal puede confiscar los teléfonos móviles como sanción de acuerdo con el reglamento interno del colegio y las directivas de la Junta de Andalucía. Sin embargo, el personal no puede registrar un dispositivo móvil sin el consentimiento de los padres del alumnado. Este sigue siendo el caso, incluso si sospechan que el teléfono contiene una imagen ilegal. Si un alumno o un familiar se niega a divulgar el contenido de material ofensivo en su teléfono, el problema será reportado al DSL y / o a la dirección del colegio, quien puede involucrar a la policía, quienes pueden usar sus propias herramientas de búsqueda.
3. Cualquier denuncia sobre el uso indebido de las tecnologías de la información y las comunicaciones se tratará de manera rápida, justa y sensible. La prioridad fundamental debe ser garantizar la seguridad y el bienestar de los niños y los jóvenes en todo momento. El colegio se ocupará de las incidencias de forma individual, caso por caso. El colegio tendrá en cuenta:
   - El contexto
   - La intención
   - El impacto del incidente
4. Los siguientes incidentes siempre serán denunciados a la Policía y/o a la Asistencia Social Infantil:
   - Descubrimiento de imágenes indecentes de niños y jóvenes.
   - Comportamiento considerado como grooming.
   - Envío de materiales obscenos.
5. Si el incidente se relaciona con un acceso involuntario a una página web inapropiada.
   - Se debe enviar un informe escrito al técnico de TI del colegio y los detalles de la página web se agregarán a la lista filtrada.
   - Un problema de protección debe registrarse y compartirse con el DSL para una investigación más detallada.
   - Es importante que el personal informe de cualquier incumplimiento involuntario de la política para evitar que se escale un evento no informado.

6. Si se hace una acusación de uso indebido contra un niño o joven, se informará a las familias o tutores y se les informará de las acciones que tomará el colegio.

Política creada por: Gillian Greaves

Revisada por: Gillian Greaves

Fecha: julio de 2025

A revisar: julio de 2026