Versión: Octubre 2025
Fecha de revisión: Octubre 2027

The British School of Gran Canaria

Seguridad en Línea

Protocolo

Índice

1. Definiciones

En este protocolo:

- **BSGC** – The British School of Gran Canaria, también denominado *el colegio* (incluye tanto el campus de Tafira como el del Sur).
- **Estudiantes / Alumnos / Niños** - todos los matriculados en el colegio.
- **Comunidad escolar** – incluye a la totalidad de los alumnos y de los empleados.
- **Miembro del Consejo Rector** – se encuentra entre los representantes elegidos que se encargan de supervisar el centro educativo.
- **Equipo directivo superior (SMT)** - el equipo directivo del colegio.
- **Director** – la persona que cuenta con responsabilidad definitiva de las gestiones del colegio.
- **Coordinador / Líder de la Seguridad en Línea** – miembro del personal responsable de implementar este protocolo.
- **Personal** – todos los empleados del colegio (los profesores, personal de Administración, Cocina y Mantenimiento)
- **Responsable de redes / Técnico de TIC** - personal responsable de los sistemas de TIC, el filtrado, la seguridad y el acceso.
- **Administrador de datos/delegado de protección de datos** - persona o servicio responsable del cumplimiento de la normativa de protección de datos.
- **IA/medios sintéticos/herramientas generativas** - software que utiliza inteligencia artificial para producir o alterar audio, vídeo, imágenes o texto (por ejemplo, *deepfakes*, chatbots, generadores de vídeo con IA).

2. Fundamentos y Finalidad

En BSGC, reconocemos que internet y las tecnologías digitales son fundamentales para el aprendizaje, la vida y el futuro profesional de los alumnos. Sin embargo, estas mismas herramientas acarrean riesgos consigo. Este protocolo pretende:

- Definir conductas seguras y responsables para el uso de tecnologías digitales e internet.
- Proveer protección a los alumnos, personal y colegio, ante riesgo online y abuso.
- Promover conciencia en nuestra comunidad sobre las amenazas, uso indebido y ciudadanía digital responsable.
- Incorporar recursos de tecnologías emergentes (Ej: multimedia generada por IA), en nuestro marco de protección.
- Establecer procedimientos para el reporte, respuesta y recuperación de incidentes de seguridad online.

3. Ámbitos y Aplicación

Este protocolo contempla:

- El uso de dispositivos propios del colegio o de uso personal (portátiles, tablets, móviles)
- El uso de comunicación digital, servicios en la nube, herramientas de IA, redes sociales, aplicaciones y plataformas online.

- Actividades realizadas durante o fuera del horario escolar que pudieran relacionarse con la seguridad online, o se reflejen en la comunidad educativa.

Aunque no podamos controlar todo el comportamiento digital fuera de los sitios web, nos comprometemos a educar a los estudiantes y proveerles de estrategias para mantenerse seguros en todos los entornos digitales.

4. Roles y Responsabilidades

Miembro del Consejo Rector / Responsable de la Seguridad en Línea

- Asegurarse de que este protocolo es vigente, renovado anualmente e implementado completamente.
- Recibir informes regularmente de parte del Coordinador / Líder de la Seguridad en Línea sobre incidentes, tendencias y cumplimiento del protocolo.
- Apoyar la asignación de recursos para la formación, monitoreo e infraestructura.

Líder designado de Salvaguarda y Líder de IA

- Supervisar la implementación diaria y reseñas de este protocolo.
- Proveer formación al personal y fomentar la conciencia sobre el asunto.
- Mantener un registro de incidencias, elevar los problemas graves y analizar patrones.
- Servir de enlace con equipo de TIC, pastoral, líderes de salvaguarda y miembros del consejo rector.
- Supervisar nuevas tecnologías, riesgos y actualizar las directrices en consecuencia.

Director

- Asegurar que la seguridad online está integrada en la cultura, planes de estudios y prácticas.
- Colaborar con el Coordinador de Seguridad en Línea y SMT para gestionar incidentes, sanciones y comunicaciones.
- Ser consciente de los riesgos de seguridad derivados de los medios digitales, el uso indebido de datos personales, la captación de menores, el ciberacoso y los medios sintéticos.

Responsable de Redes / Técnico de TIC

- Gestionar el filtrado, el cortafuegos, la seguridad de los dispositivos, las actualizaciones y la supervisión.
- Ayudar al personal con herramientas, controles de acceso y asistencia técnica.
- Registrar los cambios, las excepciones de filtrado e informar a la alta dirección según sea necesario.

Personal

- Ser modelo de un comportamiento digital responsable.

- Utilizar herramientas de IA/sintéticas en clase solo con planificación, supervisión y aprobación.
- Informar inmediatamente al Responsable de Seguridad en Línea o al Líder designado de Salvaguarda sobre cualquier inquietud o uso indebido de los medios digitales.
- Respetar las directrices de privacidad, protección de datos y consentimiento al publicar o utilizar imágenes, vídeos o trabajos de los alumnos.

Alumnos

- Utilizar la tecnología siguiendo la línea del Protocolo de uso aceptable y de este protocolo de seguridad.
- Informar inmediatamente a un adulto de su confianza, cualquier situación de incomodidad, acoso o uso indebido.
- Ser formados sobre el uso responsable de las herramientas de IA en el colegio, analizar contenido críticamente y proteger su identidad digital.

Padres / Cuidadores

- Apoyar el protocolo de seguridad online del colegio y las expectativas de uso aceptable.
- Trabajar junto con el colegio para reforzar el uso responsable de la tecnología en la casa.
- Asistir a cursos de formación o sesiones informativas sobre nuevos temas digitales o de protección (Ej: Inteligencia Artificial)

5. Educación digital e integración curricular

Nos comprometemos a integrar la seguridad online y la alfabetización digital en nuestro currículo:

- Un programa planificado de seguridad en línea como parte de las clases de *Computer Science* (Ciencias Informáticas), *PHSE –Personal, Health and Economic Education*- y otras asignaturas trasversales.
- Se reforzarán los mensajes clave sobre la seguridad en línea (información, verificación de datos, consentimiento) a través de un programa planificado de asambleas.
- Talleres o clases explícitas sobre IA, medios sintéticos *deepfakes* (videos falsos generados por inteligencia artificial) y desinformación. Los alumnos aprenderán cómo se crean estos medios, cómo detectar la manipulación y la ética que conlleva.
- Habilidades de pensamiento crítico y verificación enseñadas en todas las materias (ejemplo: evaluar fuentes, detectar *deepfakes*).
- Métodos y escenarios seguros para el uso de herramientas de IA por parte de los alumnos en el aprendizaje, con la supervisión del profesor.

6. Formación y concienciación del personal

- Formación anual obligatoria en seguridad online para todo el personal (incluidos los riesgos de la IA, los medios sintéticos y las nuevas herramientas).

- Sesiones específicas durante la formación interna sobre el uso responsable de la IA, actualizaciones de políticas y gestión de incidentes.
- Actualizaciones continuas, sesiones informativas y recursos compartidos para mantener al personal informado sobre las amenazas emergentes.

7. Medidas de seguridad técnicas y de infraestructura

El BSGC mantendrá sólidas medidas de seguridad en materia de TIC para defenderse contra el uso indebido:

- Banda ancha segura, filtrado, cortafuegos, antimalware, detección de intrusiones.
- Auditorías y revisiones periódicas de los sistemas, registros de filtrado, derechos de acceso y vulnerabilidades.
- Dispositivos, servidores y cableado protegidos físicamente y nombres de usuario/contraseñas protegidos.
- Permisos y derechos de acceso definidos según las funciones de los usuarios; derechos elevados limitados.
- Procedimientos para la desactivación controlada de los filtros (solo bajo supervisión y con registro).
- Se informa a los usuarios de que se puede realizar un seguimiento del uso de la red.
- Las solicitudes de desbloqueo o cambios deben seguir los procesos de aprobación formales.
- Transmisión de datos personales solo a través de canales seguros y cifrados.

8. Uso Aceptable y Conducción Digital

Todos los usuarios deben adherirse al Protocolo de Uso Aceptable (AUP). Expectativas claves:

Uso permitido:

- Utilizar la tecnología del colegio para la educación, comunicación y tareas creativas aprobadas.
- Citar fuentes y respetar derechos de autor.
- Utilizar herramientas de IA responsablemente cuando se autorice y supervise.

Uso inaceptable:

- Acceder o distribuir contenido ilegal (ejemplo: imágenes indecentes, discursos de odio, piratería).
- Eludir los filtros o las medidas de seguridad.
- Crear o compartir medios generados por IA que representen a personas reales sin su consentimiento, o que se utilicen para engañar o causar daño.
- Acoso cibernético, acoso, suplantación de identidad.
- Divulgación no autorizada de datos personales o confidenciales.
- Utilizar dispositivos o cuentas personales para realizar trabajos digitales relacionados con la escuela en violación de la política.

Las infracciones pueden dar lugar a medidas disciplinarias, restricciones o remisiones legales.

9. Gestión y Respuesta de Incidentes

Informe y registro:

- Todos los incidentes sobre la seguridad en línea (uso indebido, acoso, problemas con medios sintéticos) deben enviarse al registro de seguridad en línea, e informados al Coordinador de Seguridad en Línea.
- Preservar la evidencia (capturas de pantalla y enlaces) sin reenviar o alterar contenido.

Respuesta:

- El Responsable de Seguridad en Línea, el Coordinador de Seguridad en Línea, el departamento de TIC, y la Dirección evalúan la gravedad y el riesgo.
- Seguir protocolos de protección al menor si fuera necesario, involucrando a los padres y a organismos externos (policía) para incidentes graves (ejemplo: *deepfakes* que involucren a menores).
- Apoyo a el/los alumno/s afectado/s con cuidado pastoral, asesoramiento y medidas correctivas.
- Revisión y perfeccionamiento de protocolos y prácticas par aprevenir que se repitan.

10. Consecuencias legales según la Legislación Española por uso indebido de IA y Medios Sintéticos

En el Anexo B se encuentra una sección sobre el contexto legal que resume las consecuencias del uso indebido, para que el personal, los alumnos y los padres entiendan que el uso indebido no va solamente en contra del protocolo escolar, sino que también pueden acarrear riesgos y consecuencias legales (criminales, civiles y administrativas).

El colegio proveerá guía y promoverá la conciencia en los alumnos, el personal y los padres, sobre las responsabilidades y consecuencias, a fin de desarrollar actitudes y uso positivos y responsables. (Ver Anexo C)

11. Iniciativa sobre Dispositivos Electrónicos

Se espera que todos los dispositivos móviles que los alumnos traigan al colegio para uso personal, tengan instalada una aplicación de control parental. El colegio supervisará y recordará a los padres sobre el cumplimiento de esta norma.

Los teléfonos móviles de los alumnos, así como otras tecnologías que permitan la comunicación con terceros, serán recogidos al comienzo del día escolar, almacenados y devueltos a los alumnos al finalizar el día. El incumplimiento de esta norma, podría suponer la pérdida del derecho a traer el teléfono u otro dispositivo similar al colegio.

12. Comunicación y Participación de los Padres

- Se publicarán guías, actualizaciones y alertas sobre la seguridad en línea en la página web escolar, en el boletín informativo y a través de talleres para padres.
- Ofreceremos sesiones dedicadas a la IA, medios sintéticos y protección, disponibles para padres, cuidadores y a la comunidad.
- Fomentaremos las conversaciones familiares en casa sobre las tecnologías emergentes, el consentimiento y el intercambio respetuoso de contenido en los medios de comunicación.

13. Anexos y Documentos Adicionales

- **Anexo A:** Herramientas para Videos Generados con IA. Resumen y Guía.
- **Anexo B:** Consecuencias Legales bajo la Legislación Española para el uso de IA y Uso Indebido de Medios Sintéticos.
- **Anexo C:** Estrategias para la toma de Conciencia en los Alumnos.
- **Anexo D:** Guía práctica en el aula, para docentes (Uso seguro de herramientas de IA).
- **Anexo E:** Acuerdos de Uso Aceptable (Alumnos, Personal, Padres).
- **Anexo F:** Formularios de notificación de incidentes, Diagramas de Flujo de Elevación.
- **Anexo G:** Diagramas de Flujo de Incidentes de Seguridad en Línea.
- **Anexo H:** Anexo sobre Incidentes relacionados a la IA y a Medios Sintéticos.

14. Revisión y actualizaciones de protocolo.

- Este protocolo será revisado al menos anualmente, o antes en caso de que surjan nuevas tecnologías o riesgos.
- Las opiniones del personal, miembros del Consejo Rector y los servirán de base para las actualizaciones.
- Cualquier cambio será publicado, y se impartirá formación para garantizar el conocimiento.

15. Anexos

Anexo A: Herramientas para Videos Generados con IA. Resumen y Guía

Tema	Resumen y Guía
¿Qué son las Herramientas de Medios generadas por IA?	Las plataformas de generación de videos, imágenes y voz (Ejemplo: Sora, Runway, Pika Labs, Synthesia, DeepBrain, y D-ID) pueden crear contenido realista desde indicadores de texto o materiales de referencia, incluyendo imágenes o voces de personas.
Potencial Uso Indebido	Se han denunciado casos de tergiversación ("*deepfakes*"), acoso en línea, daño a la reputación, desinformación y creación de contenidos nocivos o inapropiados en muchas de estas plataformas.
Salvaguardas y Limitaciones Actuales	Aunque muchas herramientas incluyen filtros de moderación, restricciones de edad y verificación de contenido, estas no son infalibles. El uso indebido todavía puede ocurrir, especialmente en plataformas de terceros o no reguladas.
Riesgos para los Alumnos y Colegios	Angustia emocional provocada por la manipulación de los medios de comunicación o la suplantación de identidad. Erosión de la confianza en los contenidos digitales. Exposición a contenidos inapropiados o sexualizados generados por la IA. Uso indebido en el acoso escolar o la exclusión social. Dependencia excesiva de la IA para el aprendizaje o la creatividad.
¿Qué deberían hacer los Colegios?	Incorporar la concienciación sobre la IA en la educación sobre seguridad en línea. Mantener políticas claras sobre el uso ético. Incluir la IA en la formación del personal sobre protección. Proporcionar vías seguras para denunciar el uso indebido de la IA. Colaborar con los padres para reforzar expectativas coherentes.
Guía para Padres	Debatir con los niños sobre cómo funciona el contenido generado por IA y cómo éste puede ser engañoso. Promover la pregunta: *¿Puede ser esto Inteligencia Artificial?,* antes de compartirlo. Establecer límites en el uso de herramientas de IA en el hogar. Dar ejemplo sobre el compromiso ético y responsable con la tecnología.

Tema	Resumen y Guía
Cuándo involucrar a las Autoridades	Si el contenido generado por IA involucra a menores en cualquier forma indecente, amenazante o de acoso, debe ser elevado inmediatamente a la policía u oficina de protección al menor correspondiente. Esto incluye imágenes sexuales sintéticas y suplantación de identidades.
Marco de Referencia	Orientación basada en la Alianza para una IA segura para los niños, el Centro para una Internet más segura del Reino Unido y el Informe sobre seguridad de la IA de la NSPCC (2025) - *Safe AI for Children Alliance, UK Safer Internet Centre, and NSPCC AI Safety Briefing (2025).*

Anexo B: Consecuencias Legales bajo la Legislación Española para el uso de IA y Uso Indebido de Medios Sintéticos

Uso Indebido / Escenario	Ley Pertinente / Artículo	Posibles Consecuencias Legales
Contenido *Deepfake* con material sexual, pornográfico o degradante	Propuesta de modificación del **Código Penal español, artículo 173 bis**: tipifica como delito la creación o difusión sin consentimiento de *deepfakes* sexuales o gravemente degradantes generados por IA. (Fuente: merlin.obs.coe.int)	• **Delito penal** punible con pena de prisión (normalmente de 1 a 4 años) y/o multas. • **Antecedentes penales permanentes** y posible inscripción en el Registro de Delincuentes Sexuales. • **Responsabilidad civil** por daños morales y reputacionales a la víctima. • **Órdenes obligatorias de eliminación** y retirada del contenido infractor.
Difusión de material pornográfico a menores	**Código Penal español, Título VIII** (Delitos contra la libertad sexual), en especial los **artículos 183-189**. Las reformas de 2024/25 amplían estos delitos al contenido generado por IA o sintético. (Fuente: La Moncloa)	• **Delito grave** con penas de 2 a 6 años de prisión. • **Remisión automática** a las autoridades policiales y de protección infantil. • **Prohibición de trabajar con menores** o en entornos educativos. • **Confiscación de los dispositivos digitales implicados** y eliminación obligatoria de los materiales.
Uso no consensuado de imagen o voz de un otro en medios manipulados (Uso indebido de identidad, Daño al Honor, Dignidad o Imagen)	**Constitución española, artículo 18** (derecho al honor, a la intimidad y a la propia imagen). **Ley Orgánica 1/1982, artículos 7-9** (protección civil de estos derechos). (Fuente: LetsLaw)	• **Posibilidad de demanda** civil por parte de la persona afectada. • **Indemnización** por daños morales o perjuicio a la reputación (puede superar los 30 000 €). • **Retirada del material ofensivo** por orden judicial. • **Posible investigación** penal si el uso indebido va acompañado de difamación o acoso.
Falsificación de Identidad o	**Código Penal español, artículos 390-399 ter y artículo 392** (falsificación de documentos públicos o	• **Encarcelamiento** de 6 meses a 3 años por uso de identidad falsa o materiales falsificados.

Uso Indebido / Escenario	Ley Pertinente / Artículo	Posibles Consecuencias Legales
Manipulación de Documentos	privados; suplantación de identidad). (Fuente: Ministerio de Justicia)	• **Aumento de las penas** si se utiliza para defraudar, suplantar a funcionarios o causar daño a la reputación. • **Registro permanente** y posible restricción de futuros viajes o acceso a visados.
Violación de la protección de datos / publicación de imágenes de menores sin consentimiento	**RGPD**, en especial el **artículo 6.1** (base jurídica para el tratamiento). **LOPDGDD (Ley Orgánica 3/2018), artículos 93-94** (derechos digitales y consentimiento para menores de 14 años). (Fuente: LetsLaw)	• **Sanciones administrativas** de la Agencia Española de Protección de Datos (AEPD) de hasta 20 millones de euros o el 4 % de la facturación. • **Responsabilidad civil** por daños y perjuicios y daño a la reputación. • **Órdenes de retirada** inmediata y supervisión del cumplimiento. • **Medidas educativas** o servicios comunitarios para los menores implicados.
No etiquetar el contenido generado por IA o sintético (incumplimiento de la transparencia)	**Proyecto de ley española** sobre regulación de la IA (2025) en consonancia con la **Ley de IA de la UE.** Exige un etiquetado claro del material de audio, imagen y vídeo generado por IA. (Fuente: Olive Press News Spain)	• **Multa reglamentaria** de hasta 35 millones de euros o el 7 % de la facturación global por infracciones graves. • **Prohibición del uso** o la publicación del sistema de IA. • **Rectificación obligatoria** (etiquetado, descargo de responsabilidad o retirada).

Anexo C: Estrategias para la toma de Conciencia en los Alumnos

Estrategia	Descripción
Integración Curricular	Lecciones en PSHE / Ciudadanía Digital, que incluye el estudio de casos legales reales (Ejemplo: Uso indebido de *Deepfake*), cómo la legislación trata los medios sintéticos, etc.
Talleres	Talleres escolares especiales impartido por expertos jurídicos o especialistas en seguridad digital, enfocándose en las consecuencias del uso indebido de la IA, la privacidad y el contenido.
Asambleas / Sesiones de Tutoría	Sesiones breves para explicar: Qué es la IA / Medios sintéticos; Qué es legal vs Ilegal; Enfatización en el respeto, el consentimiento y la honestidad.
Escenarios y Juegos de Roles	Llevar a cabo escenarios de juegos de roles donde los alumnos consideren: “Si alguien realiza un *deepfake* sin tu consentimiento, ¿qué consecuencias habrán legal y personalmente?”
Contratos / Compromisos con los alumnos	Incorporar la comprensión de las responsabilidades legales en los acuerdos de uso aceptable o en los compromisos de seguridad digital.
Participación de los padres	Informar a los padres sobre situaciones legales; proveer orientación. Proporcionar orientación para que el hogar respalde los valores promovidos por la escuela y la concienciación jurídica.
Ayudas Visuales y Carteles	Infografías alrededor del colegio mostrando “Los Riesgos Legales por el Uso Indebido de IA y Medios Sintéticos” con puntos clave y qué es lo que los alumnos deberían evitar.
Supervisión e Información de Mecanismos	Fomentar que los estudiantes informen usos indebidos mediante rutas claras, seguras y confidenciales; reforzar que el uso indebido puede traer consecuencias graves.

Anexo D: Guía práctica en el aula, para docentes (Uso seguro de herramientas de IA)

1. Propósito

Este anexo provee una guía práctica y clara para los docentes y el personal del British School of Gran Canaria (BSGC) sobre el uso seguro, ético y efectivo de las herramientas de videos, imágenes y adiós generados por IA en entornos educativos.

Asegura que la innovación mejora el aprendizaje, mientras que mantiene los más altos estándares de protección, privacidad y ética digital.

2. Definición y Ámbitos

Las "herramientas generadas por IA" se refieren a plataformas que utilizan inteligencia artificial para crear o manipular contenido digital, incluyendo, entre otras:

- Herramientas de síntesis de vídeo: Sora 2, Runway Gen-3, Pika Labs, HeyGen, Synthesia, DeepBrain, Veed.io, etc.
- Herramientas de generación de imágenes: DALL-E, Midjourney, Leonardo AI, Adobe Firefly, Canva Magic Media.
- Herramientas de audio y voz: ElevenLabs, PlayHT, Resemble AI y similares.

Esta guía se aplica a todo el personal, todos los cursos y todos los dispositivos o cuentas de BSGC.

3. Principios Orientativos

a) **La seguridad es lo primero**: el bienestar y la protección de los alumnos prevalecen sobre cualquier objetivo creativo o educativo.
b) **Transparencia**: informar siempre a los alumnos cuando se utilice la IA y debatir sus limitaciones o implicaciones éticas.
c) **Consentimiento**: no se podrá tomar ni reproducir la imagen, el parecido o la voz de ningún alumno utilizando herramientas de IA sin el consentimiento explícito de los padres/cuidadores y del alumno (cuando sea apropiado para su edad).
d) **Idoneidad para la edad**: sólo se pueden utilizar plataformas que cumplan con el RGPD y las restricciones de edad.
e) **Supervisión**: todas las actividades relacionadas con la IA deben ser supervisadas directamente por el personal.
f) **Fines educativos**: las herramientas de IA solo deben utilizarse para mejorar los resultados de la enseñanza y el aprendizaje, nunca para entretenimiento o experimentación personal.

4. **Uso Aprobado en el Aula**

El personal podría utilizar herramientas de IA para:

- Demostrar conceptos (ejemplo: visualizar procesos científicos, reconstrucciones históricas, guiones gráficos creativos).
- Apoyar el aprendizaje diferenciado mediante recursos accesibles o multilingües.
- Fomentar la alfabetización digital crítica, explorando cómo se crean y verifican los medios sintéticos.
- Estimular el debate sobre los prejuicios, la verdad y el uso responsable de la tecnología.

Todos los usos deben planificarse previamente, evaluarse en cuanto a riesgos y ser aprobados por el jefe de departamento o el responsable de aprendizaje digital correspondiente.

5. **Uso Prohibido**

Los docentes y alumnos **no podrán**:

- Generar o compartir contenido de IA relacionado a personas reales (personal, alumnos o figuras públicas) sin su previo consentimiento informado.
- Crear o reproducir contenido generado por IA que pueda resultar engañoso, ofensivo, discriminatorio o perjudicial.
- Uso de avatares, rostros o voces de menores creados por IA en cualquier proyecto de medios sintéticos.
- Subir fotos, nombres o identificaciones de alumnos en sitios de IA de terceros, a menos que esté autorizado por el Responsable de Protección de Datos del colegio.
- Uso de cuentas personales de IA (no escolares) para actividades educativas.

6. **Protección de Datos y Cumplimiento de RGPD (Reglamento General de Protección de Datos)**

- Todas las plataformas de IA deberán someterse a una evaluación de protección de datos antes de ser utilizada en clase.
- Cualquier información compartida con sistemas de IA deben ser anonimizados y minimizados.
- La información personal nunca debe ser utilizada para “entrenar” herramientas de IA.
- El personal debe utilizar cuentas oficiales del colegio y almacenar la totalidad del contenido generado en los discos aprobados por el colegio.
- Las infracciones o inquietudes deben comunicarse inmediatamente al jefe del sector, al Líder Designado de Salvaguarda y al Administrador de Datos.

7. **Enseñar la Alfabetización Digital**

El BSGC se compromete a desarrollar la alfabetización de IA como un componente clave de la educación de la seguridad en línea.

Se anima a los profesores a:

- Ayudar a los alumnos a identificar los medios generados por IA frente a los auténticos.
- Debatir las consecuencias reales de los *deepfakes* y la desinformación.
- Reforzar la empatía, el respeto y el consentimiento en la creación digital.
- Utilizar el lema de la escuela: *Be kind, Be brave, Be you* (Sé amable, sé valiente, sé tú mismo) para enmarcar el uso responsable y la curiosidad.

8. Formación y Apoyo al Personal

El colegio proporciona:

- Sesiones periódicas sobre herramientas educativas de IA y protocolos de protección.
- Actualizaciones del responsable de IA sobre plataformas emergentes y riesgos.
- Acceso a comunidades de aprendizaje profesional para compartir las mejores prácticas.
- Asistencia bajo demanda para la planificación de clases, dilemas éticos y cuestiones técnicas.

Se anima al personal a solicitar asesoramiento al responsable de IA, al coordinador de TIC o al Líder Designado de Salvaguarda antes de introducir nuevas herramientas de IA.

9. Informes y Elevación

Si se hiciera uso indebido de herramientas de IA, el personal debe:

- Detener la actividad inmediatamente.
- Preservar cualquier evidencia (capturas de pantalla, enlaces).
- **Informar al Líder Designado de Salvaguarda y al Responsable de IA de inmediato.**
- Registrar el incidente utilizando el sistema de notificación de protección de la escuela (ejemplo: CPOMS).
- Seguir las instrucciones o los procedimientos de investigación posteriores.

10. Revisión y evaluación

Esta guía se revisará anualmente, o antes si se producen cambios importantes en la normativa o la tecnología de la IA.

Las opiniones del personal y los alumnos servirán de base para las actualizaciones, con el fin de garantizar que BSGC siga siendo una escuela segura, con visión de futuro y responsable en el ámbito digital.

11. Políticas relacionadas

- Protocolo de Salvaguarda y Protección de Menores
- Protocolo de seguridad online
- Protocolo de uso aceptable de la tecnología
- Protocolo de protección de datos y RGPD
- Estrategia de aprendizaje digital

Anexo E: Acuerdos de Uso Aceptable

1. Expectativas del Uso Aceptable de la Tecnología (Padres)

Introducción

BSGC reconoce que el uso de la tecnología mejora las oportunidades de los alumnos para aprender, participar, comunicarse y desarrollar habilidades que los prepararán para el trabajo, la vida y la ciudadanía global. Nos comprometemos a ayudar a los alumnos a acceder y utilizar la tecnología de forma adecuada, incluyendo su responsabilidad personal.

Los recursos tecnológicos de la escuela, incluyendo el correo electrónico y el acceso a Internet, se proporcionan con fines educativos. Se espera que los usuarios de la tecnología cumplan con las normas de BSGC, actúen de manera responsable y respeten los términos y condiciones establecidos por el personal docente, y que se identifican en la Política de Uso Aceptable acordada con cada alumno. La Política de Uso Aceptable describe las pautas y los comportamientos que se esperan de todos los usuarios de las tecnologías de la escuela o cuando se utilizan dispositivos personales en los campus del colegio:

- La red BSGC tiene fines educativos.
- Las tecnologías y dispositivos cubiertos por la política incluyen acceso a Internet, computadoras de escritorio, portátiles, dispositivos móviles, videoconferencias, aplicaciones de colaboración en línea, foros de mensajes, redes sociales y correo electrónico.
- Las actividades realizadas a través de la red de la escuela pueden ser supervisadas y conservadas.
- El acceso a contenidos en línea a través de la red está restringido de acuerdo con las políticas de la escuela y los cortafuegos.
- Se espera que los alumnos se comporten de forma adecuada y respetuosa en línea, tal y como lo harían en persona.
- El uso indebido de los recursos de la escuela puede dar lugar a medidas disciplinarias.

En función de ser efectivos en la aplicación de nuestras expectativas, y para asegurar que las mismas expectativas se aplican en el hogar como en el colegio, se comparten la siguiente guía para los padres:

El BSGC espera que los padres apoyen con las siguientes expectativas:

a) Apoyar el uso positivo de la tecnología como parte de la vida diaria escolar, como una herramienta integral para la enseñanza y el aprendizaje.
b) Promover y demostrar el uso seguro de la tecnología y del Internet.
c) Supervisar el uso de redes sociales del niño y apoyar las expectativas de redes sociales del colegio.
d) Apoyar las expectativas de seguridad en línea de la escuela y la Política de uso aceptable.

Este acuerdo se ha establecido para garantizar la seguridad de todos los niños matriculados en BSGC mientras están conectados a Internet. Si tiene alguna pregunta o desea recibir asesoramiento adicional, póngase en contacto con el director del sector de su hijo.

2. Acuerdo del Uso Aceptable de la Tecnología (Secundaria)

Todos los usuarios deberán leer y firmar que están de acuerdo con el Uso de Políticas Aceptables de la Tecnología, y seguir el mismo.

Uso Aceptable – Me comprometo a:

- Hacer uso de las tecnologías del colegio para actividades escolares.
- Seguir las mismas normas de comportamiento respetuoso y responsable en Internet que se espera de mí fuera de Internet.
- Tratar con cuidado los recursos del centro educativo y avisar al personal si hay algún problema con ellos.
- Fomentar el debate positivo y constructivo si se me permite utilizar tecnologías comunicativas o colaborativas.
- Alertaré a un miembro del personal si veo contenido amenazante, inapropiado o dañino (imágenes, mensajes y publicaciones) en línea.
- Utilizaré las tecnologías de la escuela en momentos apropiados, en lugares aprobados y con fines educativos.
- Citaré las fuentes cuando utilice sitios y recursos en línea para investigar.
- Seré cauteloso en la protección de mi propia seguridad y la de los demás.
- Ayudaré a proteger la seguridad de los recursos escolares.

Uso Inaceptable – Me comprometo a no:

- Utilizar tecnologías del colegio en formas que puedan resultar dañinas personal o físicamente.
- Atentar a encontrar imágenes o contenido inapropiado. (La intención de buscar imágenes o contenido inapropiado es una violación a este Protocolo de Uso Aceptable)
- Participar en acoso cibernético, hostigamiento o conducta irrespetuosa hacia otros.
- Intentar encontrar formas de eludir los cortafuegos y filtros de la escuela. (La intención de eludir las medidas de seguridad constituye una violación de esta Política de uso aceptable)
- Utilizar las tecnologías de la escuela para enviar spam o cadenas de correos electrónicos.
- Publicar o divulgar información de identificación personal sobre mí mismo o sobre otras personas.
- Acordar reunirme en persona con alguien que haya conocido en Internet.
- Utilizar en Internet un lenguaje que sería inaceptable en el aula.
- Utilizar las tecnologías de la escuela para actividades ilegales o inapropiadas.
- Intentar piratear o acceder a sitios, servidores o contenidos que no estén destinados a mi uso.

Esta lista no es exhaustiva. Todos los usuarios deben utilizar su propio criterio al utilizar las tecnologías de la escuela.

Infracciones de la Política de uso aceptable: las infracciones pueden tener consecuencias disciplinarias, entre las que se incluyen:

- Suspensión de los privilegios de red, tecnología o informáticos.
- Notificación a los padres.
- Detención o suspensión de la escuela y de las actividades relacionadas con la escuela.
- Acciones legales y/o enjuiciamiento.

Reconozco el protocolo, los puntos identificados en esta declaración, y acepto seguir y respetar el espíritu y las directrices específicas detalladas.

Firmado Fecha

3. Acuerdo del Uso Aceptable de la Tecnología (Primaria)

Todos los alumnos deben leer y firmar que entienden la información descrita debajo y aceptan seguir las reglas.

Uso Aceptable – Me comprometo a:

- Utilizar la computadora o Tablet únicamente para tareas escolares.
- Cuidar todo el equipo.
- Visitar únicamente los sitios web y aplicaciones que me indica mi docente.
- Decirle a la profesora si no estoy a gusto con algo que veo, o recibo un mensaje que no me gusta.
- Pedir ayuda si no me siento seguro/a.

Uso Inaceptable – Me comprometo a no:

- Formar parte del Cyber acoso.
- Utilizar la computadora o Tablet para chatear o enviar mensajes.
- Compartir información personal en línea.
- Utilizar malas palabras o amables.
- Conocer extraños por Internet o hablar en línea con personas que no conozco.

Entiendo que cuando utilizo una computadora o Tablet, debo tomar buenas decisiones.

Entiendo que, si incumplo deliberadamente estas normas, se me podría prohibir el uso de Internet, ordenadores y tabletas, y se contactaría con mis padres.

Firmado Fecha

4. Acuerdo del Uso Aceptable de la Tecnología (Personal y Visitantes)

Todos los usuarios deben leer y firmar que están de acuerdo con la Política de uso aceptable y que la cumplirán.

Uso Aceptable – Me comprometo a:

- Hacer uso de las tecnologías del colegio para actividades escolares.
- Seguiré las mismas expectativas de comportamiento respetuoso y responsable en línea que se espera que siga fuera de línea.
- Trataré los recursos escolares con cuidado y alertaré al Departamento de TIC si hay algún problema con ellos.
- Fomentaré el debate positivo y constructivo si se me permite utilizar tecnologías comunicativas o colaborativas.
- Alertaré al responsable de seguridad en línea si veo contenido amenazante, inapropiado o perjudicial (imágenes, mensajes y publicaciones) en línea.
- Utilizar las tecnologías escolares en los momentos adecuados, en los lugares autorizados y con fines educativos.
- Citar las fuentes cuando utilice sitios y recursos en línea para investigar.
- Ser prudente en la protección de mi propia seguridad y la de los demás.
- Ayudar a proteger la seguridad de los recursos escolares.

Uso Inaceptable – Me comprometo a no:

- Utilizar las tecnologías escolares de forma que pueda resultar perjudicial a nivel personal o físico.
- Intentar buscar imágenes o contenidos inapropiados. (La intención de buscar imágenes o contenidos inapropiados constituye una infracción de la presente Política de uso aceptable)
- Participar en acoso cibernético, hostigamiento o conducta irrespetuosa hacia otros.
- Intentar encontrar formas de eludir los cortafuegos y filtros de la escuela. (La intención de eludir las medidas de seguridad constituye una violación de esta Política de uso aceptable)
- Utilizar las tecnologías de la escuela para enviar spam o correos en cadena.
- Publicar o divulgar de cualquier otra forma información de identificación personal sobre mí mismo o sobre otros.
- Utilizar en Internet un lenguaje que sería inaceptable en el aula.
- Utilizar las tecnologías de la escuela para actividades ilegales o inapropiadas.
- Intentar piratear o acceder a sitios, servidores o contenidos que no estén destinados a mi uso.

Esta lista no es exhaustiva. Todos los usuarios deben utilizar su propio criterio al utilizar las tecnologías de la escuela.

Infracciones de la Política de uso aceptable: las violaciones pueden tener consecuencias disciplinarias, entre las que se incluyen:

- Suspensión de los privilegios de red, tecnología o informáticos.
- Medidas disciplinarias laborales.
- Acciones legales y/o procesamiento judicial.

Reconozco la política y los puntos identificados en esta declaración, y acepto seguir y respetar el espíritu y las directrices específicas detalladas.

Firmado Fecha

Anexo F: Formulario de notificación de incidentes de Seguridad en Línea. (Plantilla)

The British School of Gran Canaria

Formulario de Notificación de Incidentes de Seguridad en Línea y Salvaguarda Digital

Sección	Detalles
Fecha y Hora del Informe:	
Notificado por:	Nombre, Rol, Contacto
Fecha y Hora del Incidente (si se conoce):	
Personas involucradas:	Alumno(s) / Personal / Padre o Madre / Otro (indicar nombres, clases, roles)
Tipos de Incidente (Marcar todas las que correspondan):	☐ Cyberacoso ☐ Contenido inapropiado ☐ Sexting / Imagen indecente ☐ IA / Uso indebido de Deepfake ☐ Violación de Datos ☐ Uso indebido de dispositivo ☐ Captación de menores ☐ Amenaza / Intimidación ☐ Otro (Especificar): _____
Breve descripción del Incidente:	(Incluir lo que se vio / dijo / compartió, por quién, y cómo se hizo notar. Adjuntar capturas de pantalla, enlaces, etc. si corresponde)
Acciones tomadas inmediatamente:	(Ej: dispositivo confiscado, restricción de acceso a internet, Líder Designado de Salvaguarda (LDS) informado, padres contactados).
Quién fue informado:	☐ LDS ☐ Director ☐ Líder de Seguridad Digital ☐ Técnico de TIC ☐ Padres / Tutores ☐ Policía ☐ Organismo externo
Evaluación Inicial de Riesgo	☐ Bajo ☐ Moderado ☐ Alto (razonamiento breve)
Próximos pasos / Plan a Seguir	(Ej: Investigación, Orientación, Medidas disciplinarias, Reunión de padres, Derivación externa)
Completado por:	Nombre / Firma / Fecha
Revisado por (LDS / Director):	Nombre / Firma / Fecha
Conclusión / Resultado:	(Acciones completadas, apoyo brindado, fecha de revisión, lecciones aprendidas)

Confidencial: Este formulario debe almacenarse de forma segura de acuerdo con el RGPD y los procedimientos de conservación de registros de protección escolar.

Anexo G: Diagramas de Flujo de Incidentes de Seguridad en Línea

1. Identificación

- Miembro del personal, alumno, o padre identifican un potencial problema de seguridad online o recibe un informe al respecto.

- NO INVESTIGAR de forma independiente, más allá de la recolección de pruebas (ej: capturas de pantalla, enlaces).

2. Informarlo Inmediatamente

- Informarlo al Líder Designado de Salvaguarda (LDS).
- Si no estuviera disponible, contactar al Director o al Líder de Salvaguarda adjunto.
- Registrar los detalles iniciales en el Formulario de notificación de Incidentes.

3. Evaluación Inicial realizada por el LDS / Líder de Seguridad en Línea.

- Evaluación del riesgo: bajo, moderado, o alto.
- Considerar: ¿Se encuentra alguien en riesgo inmediato? ¿Es esto ilegal? ¿Involucra contenido sintético o sexual?
- Decidir acciones inmediatas protectoras (ej: aislación del dispositivo, retirar contenido, contactar a los padres).

4. Elevación de la Decisión

Nivel de Riesgo	Ejemplo	Acción / Elevación
Bajo	Uso inadecuado leve, no implica daños, se necesita un recordatorio del protocolo	Anotar en el registro, informar al tutor, seguimiento al alumno
Medio	Uso indebido reiterado, acoso, manipulación de imágenes con IA, filtración de datos	Investigación del LDS, reunión con los padres, posible medida disciplinaria
Alto / Ilegal	Imágenes sexuales de menores, captación de menores, amenazas, explotación de *deepfakes*, discurso de odio	Contactar a la Policía inmediatamente. Informar al Director y Miembros del Consejo Rector. Preservar la evidencia de forma segura

5. Respuesta y Apoyo

- LDS coordina la respuesta de protección.
- Se ofrece apoyo pastoral y asesoramiento a los alumnos afectados.
- Comunicación con los padres (a menos que ello aumente el riesgo).
- Se aplica el proceso disciplinario cuando procede.

- Actualización del registro de seguridad en línea y registro de los resultados.

6. Revisión y aprendizaje

- El responsable de seguridad LDS/en línea revisa el incidente para extraer lecciones.
- Actualizar la evaluación de riesgos, la formación del personal o la política cuando sea necesario.
- Informar de forma resumida (anonimizada) a los gobernadores en la revisión trimestral de protección.

Anexo H: Anexo sobre Incidentes relacionados a la IA y a Medios Sintéticos

Cuando un incidente involucra contenido generado por IA (ej: video deepfake, imagen sintética, voz falsa o uso indebido de un chatbot):

1) Asegure y conserve las pruebas digitales (capturas de pantalla, enlaces, metadatos si es posible).
2) Evalúe la posible ilegalidad: si el contenido es sexual, amenazante o difamatorio, póngase en contacto con la policía inmediatamente.
3) No comparta ni reenvíe el contenido, solo consérvelo para salvaguardar el registro.
4) Notifique a los padres y a las personas afectadas con sensibilidad; explique qué son los medios sintéticos y las medidas que se están tomando.
5) Ofrecer sesiones educativas y de apoyo a los alumnos implicados para evitar que se repita.
6) Revisar los materiales de filtrado, supervisión y enseñanza para incluir conocimientos relevantes sobre inteligencia artificial.