Versión: Final
Fecha de aprobación: 27.10.2022
Fecha de revisión: septiembre 2024

The British School of Gran Canaria

Seguridad en Línea

Protocolo

Índice

THE BRITISH SCHOOL OF GRAN CANARIA

PROTOCOLO DE SEGURIDAD EN LÍNEA

1. Definiciones

Las siguientes palabras, términos o frases presentan los siguientes significados a lo largo de todo el documento:

BSGC – The British School of Gran Canaria, también denominado *el colegio*.

Colegio – engloba tanto la sede de Tafira como la del Sur.

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.

Director – la persona que cuenta con responsabilidad estratégica y diaria, junto con

Coordinador de Seguridad Electrónica – la persona asignada del centro educativo que dispone de tal responsabilidad.

Personal – incluye a todos los empleados del colegio como, por ejemplo, los profesores, y el personal de Administración, Cocina y Mantenimiento.

Responsable de Redes – Técnico informático superior contratado por la escuela

Responsable de Datos – Responsable contratado, actualmente *Prodat*.

2. Fundamentos

El Protocolo de Seguridad Electrónica explica cómo el BSGC contribuirá a que los alumnos y el personal del colegio constituyan usuarios responsables y cuenten con la seguridad necesaria cuando utilizan Internet y otras tecnologías de la comunicación para el uso educativo, personal o de ocio.

Este protocolo:

- Clarificará las expectativas de comportamiento y los códigos de práctica para el uso responsable y para emplear las tecnologías, así como para acceder a Internet.

- Proporcionará protección y salvaguarda a los alumnos del BSGC y al personal cuando trabajan a través de Internet al establecer directrices clarificadas para reducir las posibilidades de sufrir daños y el procedimiento de actuación ante un abuso en línea.

- Garantizará que todos los miembros del BSGC son conscientes de que los comportamientos ilegales e inseguros son inaceptables y establecerá las consecuencias que acarrean acciones indebidas.

3. Objetivo del Protocolo

Este protocolo establece el papel que desempeña el colegio al garantizar que los alumnos disponen de la seguridad virtual en el centro educativo. Si bien el colegio adoptará medidas preventivas para evitar que los alumnos se vean en riesgo mientras utilizan Internet durante la jornada escolar, reconocemos la extensión y la omnipresencia del Internet fuera del centro. Por lo tanto, los alumnos recibirán formación sobre los posibles riesgos que conlleva y la necesidad de adquirir habilidades y estrategias para mantenerlos a salvo.

Asimismo, este documento:

- Identifica las personas clave, así como sus funciones y responsabilidades.
- Subraya la estrategia que desarrollará el colegio para que sus alumnos
- Identifica el procedimiento que debe cumplirse en caso de un incidente.

4. Roles y responsabilidades

Miembro del Consejo Rector responsable de la Seguridad en Línea

El miembro del Consejo Rector designado como responsable de la Seguridad en Línea. Entre sus funciones, se incluye:

- Reunirse regularmente con el Coordinador de Seguridad en Línea.
- Realizar una visita trimestral de supervisión, con una revisión de los registros de incidentes de seguridad en línea.
- Supervisión periódica de los registros de filtrado/control de cambios.
- Presentar actualizaciones, información y problemas en las reuniones mensuales de los miembros del Consejo.

Coordinador de Seguridad en Línea

El coordinador de Seguridad en Línea es Ryan Hannah. Entre sus funciones más destacadas, se encuentran:

- La responsabilidad diaria de asesoramiento y orientación sobre cuestiones de seguridad en línea, y ejercer el rol de liderazgo en el establecimiento y revisión de los protocolos de seguridad en línea del colegio con su correspondiente documentación.
- Garantizar que todo el personal conozca el protocolo y los procedimientos que deben llevarse a cabo en caso de que se produzca un incidente relacionado con la seguridad en línea.
- Proporcionar formación y asesoramiento al personal.
- Colaborar con *Inspección educativa* y otros organismos cuando sea necesario.
- Colaborar con el personal de apoyo TIC del BSGC en lo que respecta a la seguridad en línea.
- Recibir informes de incidentes de seguridad en línea y mantener un registro de incidentes para informar sobre futuros protocolos y prácticas de seguridad en línea.

- Mantener un contacto estrecho con el miembro del Consejo Rector responsable de la seguridad en línea.

Director
El Director cuenta con la responsabilidad general de garantizar la seguridad de la comunidad educativa, si bien responsabilidad diaria queda relegada al equipo de seguridad en línea.
El Director trabajará con el Coordinador de Seguridad en Línea para garantizar la seguridad de los alumnos y concienciarlos sobre la posibilidad de que acontezcan problemas graves relacionados con la protección del menor:

- el intercambio de datos personales
- el acceso a materiales ilegales o inapropiados
- contactos inapropiados en línea con adultos/desconocidos
- incidentes posibles o reales de *grooming*;
- ciberacoso.

Responsable de Redes
Cuenta con las siguientes funciones:

- supervisar, adaptar y controlar los sistemas TIC del colegio, los servidores, el hardware, el software y las barreras de protección para garantizar la seguridad de los usuarios, así como de los sistemas y los equipos.
- controlar, filtrar y supervisar el acceso de los usuarios del colegio a Internet.
- controlar e impedir el acceso no deseado y no autorizado al sistema escolar desde el exterior.
- garantizar que el centro educativo cuenta con la suficiente protección para hacer frente a cualquier amenaza indeseada.
- informar y actualizar con regularidad al miembro del Consejo Rector de Seguridad en Línea, al equipo de seguridad en línea y al Director sobre las situaciones problemáticas y las medidas necesarias para preservar la seguridad y plena información en lo relativo a la escuela y a todos sus usuarios.

5. Educación de los menores

Mantener la seguridad de los niños en Internet es crucial y fundamental en todos los aspectos de la educación. Aunque existen filtros para proteger a los alumnos mientras se encuentran en el centro educativo, esto es sólo un pequeño porcentaje del tiempo que un menor navega a través de Internet. Los colegios deben desempeñar su papel en la educación de sus alumnos al negociar el Internet sin los filtros y los cortafuegos del centro. El BSGC hará todo lo posible para desarrollar las estrategias de riesgo de los alumnos y las respuestas a las amenazas, bien sean reales o posibles.

El BSGC proporcionará una educación sobre la seguridad en línea a través de las siguientes medidas:

- Un programa planificado de seguridad en línea como parte de las clases de *Computer Science,* PHSE y otras asignaturas, con temas fundamentales que se repasarán con periodicidad en el plan de estudios y en el que todo el personal desempeñará un papel de relevancia.
- Se reforzarán los mensajes clave sobre la seguridad en línea a través de un programa planificado de asambleas.
- En todas las clases, se enseñará a los niños a ser críticamente conscientes de que el contenido al que acceden de forma virtual no es completamente veraz o válido. Asimismo, se les enseñará a comprobar la veracidad de la información.
- Se fomentará en el alumnado la promoción y adopción de un uso seguro y responsable de las TIC, el Internet y los dispositivos móviles, no solo en el entorno escolar sino también fuera de él.
- Se enseñará a reconocer las fuentes de la información empleadas y a respetar los derechos de autor cuando los alumnos dispongan del material al que hayan accedido a través de Internet.
- Las normas de uso de los sistemas TIC y de Internet se expondrán en todas las aulas, ya que la utilización de los dispositivos móviles implica que se puede acceder a Internet en cualquier área del colegio.
- El personal servirá de modelos positivos de gran arraigo al utilizar las TIC, el Internet y los dispositivos móviles.

6. Educación de las familias y los tutores

La educación de las familias resulta fundamental para que los niños desarrollen estrategias orientadas a afrontar los posibles riesgos que acarrea el Internet. La percepción de dicha amenaza por parte de los padres puede ser limitada o carecer de la información suficiente. Los diferentes casos que se divulgan en los medios de comunicación no solo pueden provocar ciertas preocupaciones innecesarias en las familias, sino que también ocultan problemas y riesgos reales. El objetivo del centro consistirá en proporcionar la máxima información útil posible para contribuir a que las familias dispongan de la seguridad en línea cuando los menores se encuentran fuera del entorno escolar. Esta información también podrá transmitirse a otros familiares como, por ejemplo, los abuelos.

Este objetivo se logrará a través de:

- las redes sociales.
- las circulares informativas, los boletines y la página web.
- las reuniones o talleres para padres.

Todos los miembros del personal pueden ayudar a las familias, si bien tienen la obligación de remitir cualquier información ante indicios de que se produzcan problemas de seguridad en línea.

7. Educación y formación del personal

Resulta esencial que todo el personal reciba formación sobre seguridad en línea y comprenda sus responsabilidades, tal y como se describen en este protocolo. La formación incluirá:

- Un programa planificado de formación formal sobre la seguridad en línea.
- Presentación y debate anual de este protocolo.
- El colegio tendrá como objetivo proporcionar el mejor asesoramiento actualizado para apoyar las prácticas de seguridad en línea para miembros de la comunidad educativa y grupos.

8. Seguridad electrónica

El colegio adoptará todas las medidas debidas para mantener un entorno seguro y protegido. Para ello, se tomarán en consideración los siguientes aspectos:

- Los sistemas TIC se gestionarán de forma que se garantice que el colegio cumple con los requisitos técnicos de seguridad en línea indicados por las correspondientes autoridades españolas y las recomendaciones establecidas en las guías del Reino Unido.

- Se revisará y auditará periódicamente la seguridad de los sistemas TIC del centro.

- Los servidores, los sistemas inalámbricos y el cableado se ubicarán de forma segura y el acceso físico a estos quedará restringido.

- Todos los usuarios tendrán derechos de acceso a los sistemas TIC del centro educativo claramente definidos.

- Todos los usuarios firmarán el documento *Expectativas de uso aceptable de las TIC* del colegio antes de utilizar Internet.

- Las contraseñas gestionadas por el responsable del sistema TIC del centro también deben estar a disposición del Director o de otro miembro designado que forme parte del Equipo Directivo. Estas deberán custodiarse en un lugar seguro.

- En el caso de que el personal de apoyo TIC (u otros individuos) necesiten desactivar el filtrado por cualquier motivo, deberá registrarse debidamente y llevarse a cabo mediante un procedimiento acordado con el Director.

- Cualquier problema sobre tal irregularidad debe comunicarse inmediatamente al Director.

- Las solicitudes del personal para que se eliminen sitios web de la lista de filtrados se someterán a la consideración del Director.

- El personal del Departamento de TIC controlará y registrará periódicamente la actividad de los usuarios en los sistemas informáticos del colegio. Asimismo, se informará a los usuarios de este control en las *Expectativas de uso aceptable de las TIC*.

- Cualquier incidente, posible o real, relacionado con la seguridad en línea debe comunicarse al responsable o departamento pertinente. En la mayoría de los casos, será el Coordinador de Seguridad en Línea, salvo que dichos miembros responsables se encuentren involucrados, en cuyo caso deberá tomar parte el Director o Equipo Directivo.

- La infraestructura del colegio y las zonas de trabajo individuales se protegerán con un software antivirus actualizado.

- Los datos personales no deben difundirse a través de Internet ni exponerse en un entorno externo al colegio sin la debida autorización previa; en estos casos, solamente se llevará a cabo de forma segura y encriptada.

El uso de tecnologías sobre imagen digital implica ciertas ventajas relevantes para el aprendizaje, ya que permite que tanto el personal como el alumnado utilicen de forma instantánea imágenes grabadas por ellos mismos o descargadas a través de Internet. Sin embargo, dichos miembros de la comunidad educativa deben ser conscientes de los riesgos que conlleva el hecho de compartir fotografías y de publicarlas en Internet, pues estas pueden quedar accesibles en Internet como parte de la huella digital y pueden perjudicar o avergonzar a tales personas a corto o largo plazo. En este caso, cabe destacar que se ha tenido conocimiento de muchas situaciones en las que determinadas empresas realizan búsquedas en Internet para obtener información sobre sus empleados actuales y aquellos que aspiran a trabajar en el futuro.

El personal debe no solo conocer sino también comprender el protocolo del colegio en lo que respecta al uso de las redes sociales por su parte, tal y como se indica a continuación:

- Al utilizar imágenes digitales, el personal debe educar a los alumnos sobre los riesgos asociados a la realización, el uso, el intercambio, la publicación y la difusión de fotografías. Por ejemplo, al identificar los riesgos asociados a su publicación en Internet, como en las redes sociales.

- El personal puede realizar imágenes digitalmente o grabar vídeos como material de apoyo a los objetivos educativos, si bien debe cumplir con los protocolos del centro educativo vinculados a compartir, distribuir y publicar dicho contenido (autorización GDPR). Tal material solamente podrá obtenerse a partir de la utilización de dispositivos en propiedad del centro educativo, de modo que los medios personales no podrán emplearse para dicho fin.

- Cuando se tomen fotografías o se graben vídeos, los menores deben vestir adecuadamente y no participar en actividades que puedan desacreditar a dichos miembros de la comunidad escolar o el centro educativo, en sí mismo.

- Los menores no deben realizar, utilizar, compartir, publicar ni distribuir imágenes realizadas en el entorno escolar en las que aparezcan otras personas sin la autorización explícita del profesor correspondiente y del colegio.

- Las fotografías publicadas en la página web, o en cualquier otro entorno, en las que se incluya a menores se seleccionarán con la debida atención y cumplirán con las directrices de prácticas positivas sobre el uso de dichas imágenes. Del mismo modo, la autorización GDPR quedará garantizada.

- No se hará uso de los nombres completos de los alumnos en ningún espacio de la página web, las redes sociales o blog, especialmente cuando se publican junto con fotografías.

- Se obtendrá la autorización GDPR de los padres o tutores legales antes de publicar cualquier imagen del menor en cuestión a través de la página web o de las redes sociales del centro.

9. Protección de Datos

Los datos personales se registrarán, tratarán, cederán y pondrán a disposición conforme a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos (*juridicas.com*) en la que se establece que los datos personales deben ser:

- tratados de manera leal y lícita,
- tratados con fines determinados,
- adecuados, pertinentes y no excesivos
- exactos
- no almacenados por un periodo de tiempo mayor del necesario
- tratados de conformidad con los derechos del interesado,
- seguros,
- únicamente transferidos a terceros con la seguridad pertinente.

Los miembros del personal deben velar en todo momento por la custodia de los datos críticos, al minimizar el riesgo de pérdida o de uso indebido. Deben almacenar los datos personales o más vulnerables únicamente en ordenadores y otros dispositivos del BSGC seguros y protegidos por contraseña, al asegurarse de que se "desconectan" correctamente al final de cualquier sesión en la que hayan empleado dicha información.

10. Gestión de la infraestructura TIC

El acceso a Internet, la seguridad, la protección antivirus y el filtrado

El BSGC gestiona la infraestructura TIC al aplicar una serie de medidas de seguridad. El Responsable de Redes y el Coordinador de Seguridad en Línea cuentan con la responsabilidad de mantenerla actualizada.

Todos los usuarios también tienen la responsabilidad de utilizar Internet y los sistemas de la escuela de forma segura, de modo de que deben informar al Responsable de Redes si identifican contenido

susceptible de spam, fraude virtual, malware, ciberataque de datos y archivos con virus, o si observan indicios de su existencia.

El correo electrónico del BSGC

El colegio proporciona a todo el personal una cuenta de correo electrónico para que se utilice de acuerdo con sus funciones. Se espera que los usuarios del correo reconozcan que representan al centro educativo en cualquier correspondencia que mantengan a través de este sistema y, por lo tanto, deben actuar con el cierto cuidado y consideración en sus acciones.

- Los usuarios del correo electrónico del BSGC deben ser conscientes de lo siguiente:

- El sistema de correo electrónico del colegio puede considerarse seguro, pues se comprueban y controlan los virus. Asimismo, debe utilizarse en todas las comunicaciones relacionadas con el centro.

- Las cuentas de correo electrónico del colegio no deben utilizarse para comunicaciones a título privado.

- Las comunicaciones por correo electrónico e Internet pueden quedar sujetas al correspondiente control.

- Todos los usuarios deben informar inmediatamente a la persona designada, identificada en este protocolo, de la recepción de cualquier correo electrónico que les haga sentir incómodos, sea ofensivo, o de carácter amenazante y/o de naturaleza intimidatoria - los usuarios no deben responder a ningún correo electrónico de este tipo.

- Cualquier comunicación digital entre el personal y los alumnos o padres/tutores legales debe ser profesional en cuanto al tono y al contenido se refiere. Estas comunicaciones solamente pueden llevarse a cabo a través de los sistemas oficiales del colegio sujetos a un control.

- Las direcciones de correo electrónico personales, los mensajes de texto o las aplicaciones públicas de chat / redes sociales no deben emplearse para este tipo de comunicaciones.

- A los alumnos se les enseñará prácticas positivas en las redes sociales y el correo electrónico, así como cuestiones de seguridad y una hoja de ruta para responder a los riesgos que conlleva el uso de estos medios.

- Al dejar el colegio, el personal dejará de tener acceso a la cuenta de correo electrónico y a las bases de datos del centro.

- BSGC se reserva el derecho de ponerse en contacto con la Policía si uno de nuestros empleados o alumnos recibe un correo electrónico que consideremos especialmente perturbador o que infrinja la ley;

Protocolo de contraseñas

- Los alumnos deben mantener siempre su contraseña en secreto, de forma que no deben compartirla con otros ni dejarla explícitamente visible donde otros puedan encontrarla.

- Todo el personal dispone de un nombre de usuario propio y una contraseña privada para acceder a los sistemas del centro educativo; es su responsabilidad mantener su contraseña en secreto.

Página web del BSGC

- El Director asume la responsabilidad general de garantizar que el contenido de la página web sea preciso y que se mantenga la calidad de la presentación, si bien delega la responsabilidad diaria en el responsable de la página web del colegio.

- La mayor parte del material debe ser fruto del BSGC de manera que, cuando se publica o se comparte el trabajo de otros, deben explicitarse las fuentes utilizadas e indicarse claramente la identidad o la posición que ostenta el autor.

- Los puntos de contacto en la página web son la dirección del BSGC, el número de teléfono y la dirección de correo electrónico. No se publican ni los datos del domicilio ni la identidad de los correos electrónicos personales.

- Las fotografías publicadas en la página web no se presentan con nombres y cuentan con los permisos parentales pertinentes y con la GDPR.

Redes sociales

- Sólo se utilizarán las cuentas oficiales de BSGC en las redes sociales para promocionar el colegio, compartir información y resaltar los logros dentro de la comunidad del BSGC.

- Cualquier fotografía o información no debe incluir detalles que puedan permitir la identificación por parte de personas desconocidas.

- Para publicar y compartir información en las redes sociales del BSGC se necesitan todos los permisos pertinentes de la GDPR y de las familias.

- Un miembro del personal designado será responsable de recopilar información y realizar las publicaciones diarias en estas cuentas de redes sociales.

11. Acciones ilegales e inaceptables en Internet

Las acciones que se indican a continuación son ilegales o se consideran inaceptables en el entorno escolar y, por consiguiente, los usuarios de los sistemas escolares no deben involucrarse en ellas. En este sentido, los protocolos y sistemas escolares no solamente restringen, sino que también prohíben determinados usos de Internet. Los usuarios no deben visitar sitios de Internet, realizar, publicar,

descargar, subir, transferir, comunicar o transmitir material, observaciones, propuestas o comentarios que contengan o se vinculen a:

- Imágenes de abuso sexual infantil.
- Fomento o realización de actos ilegales como, por ejemplo, en virtud de la legislación sobre protección de menores, obscenidad, uso indebido de ordenadores y fraude.
- Material para adultos que infrinja la legislación/normativa española o británica sobre publicaciones obscenas;
- Contenido racista
- Pornografía;
- Fomento de cualquier tipo de discriminación
- Promoción del odio racial o religioso.
- Comportamientos de carácter amenazante, incluido el fomento de la violencia física o psicológica.
- Cualquier otra información que pueda resultar ofensiva o atente contra la integridad o el espíritu del centro educativo.
- El uso de sistemas escolares para gestionar un negocio privado.
- La utilización de sistemas, aplicaciones, páginas web u otros mecanismos que eludan filtros, cortafuegos u otras salvaguardias.
- Subir, descargar o transmitir software comercial u otros materiales protegidos por derechos de autor pertenecientes a terceros, sin los permisos de licencia correspondientes.
- Revelar o divulgar información confidencial o sujeta a derechos de propiedad como, por ejemplo, información financiera o personal, bases de datos, códigos de acceso a ordenadores o redes y contraseñas.
- Crear o difundir virus informáticos u otros archivos dañinos.
- Realizar un tráfico de red prolongado o instantáneo de gran volumen; por ejemplo, descargar/subir archivos que provoquen la congestión de la red y dificulten a otros el uso de Internet;
- *Streaming* o descarga en portales o aplicaciones como Netflix y Spotify.
- Juegos en línea no educativos.
- Juegos de azar virtuales.
- Publicar en YouTube o sitios similares, a menos que sea por razones educativas y con el permiso previo del Jefe de Departamento y del Responsable de GDPR.

12. Respuesta a incidentes de uso indebido

Todos los miembros de la comunidad escolar están comprometidos con el uso responsable de las TIC y cumplen este protocolo. Si acontece una infracción del protocolo por descuido, irresponsabilidad o uso indebido deliberado, la conducta indebida del usuario en cuestión debe comunicarse al

responsable de seguridad en línea. Del mismo modo, debe llevarse a cabo el proceso de notificación de incidentes, al igual que con cualquier aspecto relacionado con la seguridad, el bienestar de los niños o la conducta indebida del personal.

Conducta esperada

Se espera que los miembros de la comunidad del BSGC:

- Utilicen los sistemas TIC del colegio de acuerdo con el Protocolo de Uso Aceptable.
- Comprendan la importancia de adoptar buenas prácticas de seguridad virtual en todo momento.
- Reconozcan y comprendan las consecuencias del uso indebido o de acceder a materiales inapropiados.
- Reconozcan y denuncien los casos de tratamiento indebido de la información, el uso indebido o el acceso a materiales inapropiados.
- Reconozcan y respeten el protocolo sobre el uso de dispositivos portátiles, así como comprendan el modo en que se relacionan estos protocolos con la toma/uso de imágenes y el ciberacoso.

Además, el personal debe leer el protocolo de seguridad en línea del centro, aceptarlo y cumplirlo. Así pues, no solo se orientará a todos los alumnos sobre el uso seguro y responsable de Internet y los dispositivos electrónicos, sino que también se espera que los alumnos de Year 5 y de cursos superiores firmen cada año el *Acuerdo de uso aceptable de las TIC.* Asimismo, comprenderán adecuadamente tanto las técnicas de investigación como la necesidad de evitar el plagio y de respetar las normas sobre los derechos de autor.

Los padres/tutores recibirán información sobre el uso seguro de Internet, las expectativas de la escuela acerca del "uso aceptable" y las sanciones que podrían acarrear su uso indebido.

Gestión de incidentes

El BSGC:

- Vigilará exhaustivamente y aplicará el Protocolo de Seguridad en Línea, con las consecuentes sanciones diferenciadas, en caso necesario.
- Fomentará que los miembros de la comunidad muestren especial atención al informar de ciertas problemáticas, con la confianza de que estas se gestionarán con rapidez y sensibilidad; del mismo modo, se garantizará que el personal conoce el Protocolo de Denuncia de Irregularidades.
- Pondrá en marcha un ciclo continuo para la mejora del protocolo con el fin de garantizar que actualiza conforme a los avances tecnológicos;
- Informará a los padres/tutores de las personas implicadas en incidentes de seguridad en línea.

- Se pondrá en contacto con la Policía si un miembro de nuestro personal o un alumno recibe o envía comunicaciones en línea que consideremos especialmente alarmantes o que supongan una infracción de la ley.

Tratamiento de inquietudes

El centro educativo tomará las debidas precauciones para garantizar la seguridad en línea. Resulta imposible garantizar que jamás pueda aparecer un determinado material inadecuado en un ordenador o dispositivo móvil del colegio, ni que los incidentes o interacciones negativas sean inexistentes. El colegio no podrá aceptar responsabilidad alguna por el material al que se acceda, ni por las consecuencias del acceso a Internet si ha actuado para garantizar la seguridad y minimizar los riesgos.

La Comunidad Escolar recibe información sobre el uso inaceptable y las posibles sanciones, entre las que se incluyen:

- Una entrevista/consejo por parte de un miembro del personal;
- Transmisión de información a los padres o tutores
- Sanción de acuerdo con el protocolo de disciplina y sanciones del BSGC;
- Eliminación del acceso a Internet o al ordenador durante un cierto periodo de tiempo;
- Remisión a la policía.
- El Coordinador de Seguridad en Línea representa la primera referencia de contacto para cualquier denuncia. Cualquier inquietud sobre un uso indebido por parte del personal se remite directamente al Director, tal y como se establece en el Protocolo de Denuncia de Irregularidades.
- Las denuncias de ciberacoso se abordarán de acuerdo con nuestro Protocolo Contra el Acoso.

Anexo A - Gestión de la infraestructura TIC

Este colegio:

- dispone de conectividad de banda ancha educativa, filtrada y segura a Internet.
- garantiza la buena salud de la red mediante el uso de un software antivirus.
- bloquea todas las salas de chat y páginas web de redes sociales, excepto las que forman parte de una red educativa o plataforma de aprendizaje que cuente con la debida aprobación.
- bloquea el acceso de los alumnos a páginas web de descarga de música o de compras, excepto aquellas autorizadas que cuenten con fines educativos.
- vigila el uso de las TIC por parte de los alumnos en todo momento, en la medida de lo posible, y utiliza estrategias de sentido común en las áreas de recursos de aprendizaje donde los alumnos mayores disponen de un acceso más flexible.
- se asegura de que todo el personal y los alumnos de Year 5 y cursos superiores hayan firmado un formulario de acuerdo de uso aceptable y comprendan que deben informar de cualquier problemática.
- exige al personal que compruebe previamente las páginas web antes de emplearlas; fomenta el uso de la plataforma de aprendizaje del colegio como un recurso fundamental para remitir a los alumnos a páginas web apropiadas para su edad y de acuerdo con la asignatura.
- se encuentra alerta cuando realiza búsquedas de imágenes con los alumnos como, por ejemplo, aquellas llevadas a cabo a través de Google.
- informa a todos los usuarios de que el uso de Internet cuenta con la vigilancia correspondiente.
- informa al personal y a los alumnos de que deben comunicar directamente cualquier fallo de los sistemas de filtrado al correspondiente responsable.
- clarifica, a través de las reuniones de personal y los programas de enseñanza, que todos los usuarios conocen y comprenden las "normas de uso adecuado" y las sanciones que implican un uso indebido.
- Proporciona a los alumnos, al personal y a los padres asesoramiento e información sobre cómo denunciar materiales ofensivos, maltrato/acoso, etc;
- se reserva el derecho de remitir a las autoridades competentes como, por ejemplo, la Policía, cualquier material que muestre indicios de ilegalidad.

Anexo B - Compromisos de Uso Aceptable de las TICs

1. Expectativas de Uso Aceptable sobre las TICs (Padres)

Introducción

El BSGC es consciente de que el uso de las nuevas tecnologías contribuye a que los alumnos dispongan de mejores oportunidades de aprendizaje, compromiso, comunicación y desarrollo de habilidades que les prepararán para el trabajo, la vida y la ciudadanía global. Nos comprometemos a ayudar a los alumnos a acceder y utilizar las nuevas tecnologías de forma adecuada, al incluir su responsabilidad personal.

Los recursos tecnológicos del centro educativo, entre los que se incluyen el correo electrónico y el acceso a Internet, se proporcionan con fines educativos. Se espera que sus usuarios cumplan las normas del BSGC, actúen con responsabilidad y respeten los términos y condiciones establecidos por el personal docente e identificados en el Protocolo de Uso Aceptable acordado con cada alumno. Este protocolo describe las directrices y los comportamientos que se esperan de la totalidad de tales usuarios de dispositivos del centro o en situaciones en las que empleen sus dispositivos personales en las dependencias del centro:

- La red del BSGC se destina a fines educativos.
- Las tecnologías y dispositivos de este protocolo incluyen el acceso a Internet, los ordenadores de sobremesa, los ordenadores portátiles o móviles, las videoconferencias, las aplicaciones de colaboración en línea, los tablones de anuncios, las redes sociales y el correo electrónico.
- La actividad en la red del colegio puede quedar sujeta a su monitorización y retención.
- El acceso a contenidos virtuales a través de la red queda restringido de acuerdo con los protocolos del colegio y los cortafuegos.
- Se espera que los alumnos se comporten de forma adecuada y respetuosa en la red, al igual que actuarían físicamente.
- El uso indebido de los recursos del colegio puede conllevar medidas disciplinarias.
- Todos los usuarios son responsables de su uso de la tecnología y se comprometen a evitar, al máximo posible, contenidos inapropiados.
- Los usuarios deben informar al personal del BSGC inmediatamente ante cualquier inquietud relativa a la seguridad.
- Este Protocolo de Uso Aceptable se aplica a los dispositivos tecnológicos en propiedad del colegio y a aquellos de propiedad privada que accedan a la red del colegio, siempre y cuando se encuentren en sus instalaciones, en el transporte, viajes o eventos.

Con el fin de ser eficaces en la aplicación de nuestras expectativas y para garantizar que se implementen de forma similar en casa y en el centro educativo, compartimos la siguiente hoja de ruta con todas las familias del BSGC.

El BSGC busca el apoyo de las familias con las siguientes expectativas:

1. Apoyar el uso positivo de la tecnología como parte de la vida escolar diaria y como una herramienta integral para la enseñanza y el aprendizaje.

2. Fomentar y modelar el uso seguro de las nuevas tecnologías e Internet.

3. Supervisar el uso de las redes sociales del menor y mostrar su apoyo a las expectativas sobre redes sociales del colegio.

4. Apoyar las expectativas de seguridad en línea del centro y el Protocolo de Uso Aceptable.

Este acuerdo se ha establecido para garantizar que todos los niños matriculados en el BSGC cuenten con la debida seguridad en Internet. Ante cualquier otra consulta, o si desea asesoramiento adicional, no dude en ponerse en contacto con el Responsable de Etapa (*Head of Sector*) de su hijo o hija.

2. Compromiso de Uso Aceptable de las TICs del BSGC (Secundaria)

Todos los usuarios deben leer y firmar que están de acuerdo con el Protocolo de Uso Aceptable y que lo cumplirán firmemente.

Uso Aceptable - Yo:

- Utilizaré las TICs escolares para actividades relacionadas con el colegio.
- Seguiré unas expectativas de comportamiento respetuoso y responsable en línea de la misma manera que en acciones no virtuales.
- Trataré con cuidado los recursos escolares y avisaré al personal si percibo algún problema.
- Fomentaré debates positivos y constructivos al permitirme la utilización de las tecnologías comunicativas o colaborativas.
- Informaré a un miembro del personal si observo contenido de carácter amenazante, inapropiado o perjudicial (imágenes, mensajes y publicaciones) en línea.
- Utilizar las TICs escolares en los momentos adecuados, en los lugares autorizados y con fines educativos.
- Citaré las fuentes cuando utilice páginas web y recursos en línea para desarrollar investigaciones.
- Seré prudente en la protección de la seguridad propia y ajena.
- Ayudaré a proteger la seguridad de los recursos escolares.

Uso inaceptable – No podré:

- Utilizar las TICs escolares de una manera que pueda ser personal o físicamente perjudicial.
- Buscar imágenes o contenidos inapropiados. (Se trata de un incumplimiento del Protocolo de Uso Aceptable).
- Participar en acoso cibernético, acoso o conducta irrespetuosa hacia los demás.
- Encontrar formas de eludir los cortafuegos y filtros del colegio. (El intento de sortear las medidas de seguridad supone un incumplimiento del Protocolo de Uso Aceptable).
- Utilizar las TICs del centro educativo para enviar *spam* o correos masivos.
- Publicar o divulgar de cualquier otro modo cierta información de identificación personal sobre mí mismo o sobre los demás.
- Quedar físicamente con alguien que he conocido a través de Internet.
- Utilizar un lenguaje en línea que sería inaceptable dentro del aula.
- Utilizar las TICs escolares para actividades ilegales o inapropiadas.
- Intentar piratear o acceder a páginas web, servidores o contenidos que no estén destinados al uso correspondiente.

Esta lista no resulta demasiado exhaustiva; todos los usuarios deben usar el sentido común cuando utilicen las TICs escolares.

Incumplimiento del Protocolo de Uso Aceptable – Los incumplimientos pueden tener consecuencias disciplinarias, entre las que se incluyen lo siguiente:

- Suspensión de privilegios de red, TICs o ordenador.
- Notificación a los padres.
- *Detention* tras la jornada escolar o expulsión temporal del colegio o de actividades relacionadas con el centro educativo.
- Acciones legales y/o procedimiento judicial.

Reconozco la política, los puntos identificados en esta declaración, y estoy de acuerdo en seguir y defender el espíritu y las directrices específicas detalladas.

Firmado Fecha

3. Compromiso de Uso Aceptable de las TICs del BSGC (Primaria)

Todos los alumnos deben leer y firmar que comprenden la información explicitada a continuación y se comprometen a cumplir con tales reglas.

Uso Aceptable - Yo:

- Usaré el ordenador o la tableta solamente para tareas escolares.
- Cuidaré todos los recursos tecnológicos.
- Solamente visitaré las páginas web y las aplicaciones que me solicite mi profesor.
- Informaré a un profesor si no estoy satisfecho con cualquier material que vea o si recibo mensajes que me desagradan.
- Pediré ayuda si no estoy seguro.

Uso inaceptable – No podré:

- Involucrarme en el ciberacoso.
- Utilizar el ordenador o la tableta para chatear o enviar mensajes.
- Compartir información personal en Internet.
- Utilizar palabras malsonantes.
- Conocer a extraños a través de Internet o hablar virtualmente con personas que no conozco.

Comprendo que, cuando empleo el ordenador o la tableta, debo adoptar buenas decisiones.

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

Firmado Fecha

4. Compromiso de Uso Aceptable de las TICs del BSGC (Personal y Visitantes)

Todos los alumnos deben leer y firmar que comprenden la información explicitada a continuación y se comprometen a cumplir con tales reglas.

Uso Aceptable - Yo:

- Utilizaré las TICs escolares para actividades relacionadas con el colegio.
- Seguiré unas expectativas de comportamiento respetuoso y responsable en línea de la misma manera que en acciones no virtuales.
- Trataré con cuidado los recursos escolares y avisaré al personal si percibo algún problema.
- Fomentaré debates positivos y constructivos al permitirme la utilización de las tecnologías comunicativas o colaborativas.
- Informaré a un miembro del personal si observo contenido de carácter amenazante, inapropiado o perjudicial (imágenes, mensajes y publicaciones) en línea.
- Utilizar las TICs escolares en los momentos adecuados, en los lugares autorizados y con fines educativos.
- Citaré las fuentes cuando utilice páginas web y recursos en línea para desarrollar investigaciones.
- Seré prudente en la protección de la seguridad propia y ajena.
- Ayudaré a proteger la seguridad de los recursos escolares.

Uso inaceptable – No podré:

- Utilizar las TICs escolares de una manera que pueda ser personal o físicamente perjudicial.
- Buscar imágenes o contenidos inapropiados. (Se trata de un incumplimiento del Protocolo de Uso Aceptable).
- Participar en acoso cibernético, acoso o conducta irrespetuosa hacia los demás.
- Encontrar formas de eludir los cortafuegos y filtros del colegio. (El intento de sortear las medidas de seguridad supone un incumplimiento del Protocolo de Uso Aceptable).
- Utilizar las TICs del centro educativo para enviar *spam* o correos masivos.
- Publicar o divulgar de cualquier otro modo cierta información de identificación personal sobre mí mismo o sobre los demás.
- Quedar físicamente con alguien que he conocido a través de Internet.
- Utilizar un lenguaje en línea que sería inaceptable dentro del aula.
- Utilizar las TICs escolares para actividades ilegales o inapropiadas.
- Intentar piratear o acceder a páginas web, servidores o contenidos que no estén destinados al uso correspondiente.

Esta lista no resulta demasiado exhaustiva; todos los usuarios deben usar el sentido común cuando utilicen las TICs escolares.

Incumplimiento del Protocolo de Uso Aceptable – Los incumplimientos pueden provocar consecuencias disciplinarias, entre las que se incluyen:

- Suspensión de privilegios de red, TICs u ordenador.
- Medidas disciplinarias laborales.
- Acciones legales y/o procedimiento judicial.

Soy consciente de este protocolo, los aspectos identificados en este compromiso y acepto tanto seguir como defender el espíritu y las directrices específicas detalladas.

Firmado Fecha