Política de Seguridad Digital (E-Safety Policy)

A. ALCANCE

La escuela está comprometida a promover y salvaguardar el bienestar de todos los estudiantes, y para ello es indispensable contar con una estrategia efectiva de seguridad en línea.

Los objetivos de la estrategia de seguridad en línea de la escuela son tres:

- Proteger a toda la comunidad escolar de contenido o contacto ilegal, inapropiado o dañino.
- Educar a toda la comunidad escolar sobre su acceso y uso responsable de la tecnología.
- Establecer mecanismos efectivos para identificar, intervenir y escalar incidentes cuando corresponda.

Al considerar el alcance de la estrategia de seguridad en línea, la escuela adoptará una visión amplia y deliberada acerca del significado de tecnología, redes y dispositivos utilizados para visualizar o intercambiar información, incluyendo tecnología de comunicación (de manera colectiva denominada en esta política como tecnología).

Esta política aplica a todos los miembros de la comunidad escolar, incluyendo colaboradores, voluntarios, estudiantes, padres de familia y visitantes que tengan acceso a la tecnología de la escuela, ya sea dentro o fuera de las instalaciones, o que utilicen tecnología de una manera que afecte el bienestar de otros estudiantes o cualquier miembro de la comunidad escolar, o cuando se ponga en riesgo la cultura o reputación de la escuela.

Las siguientes políticas, procedimientos y materiales de referencia también son relevantes para las prácticas de seguridad en línea de la escuela: Política Anti-Bullying, Código de Conducta del Personal, Política de Uso Aceptable para Estudiantes (Manual del Estudiante) y Política de Salvaguarda.

B. ROLES Y RESPONSABILIDADES

1. Dirección General y ISP

La Dirección General tiene responsabilidad general sobre los mecanismos de protección dentro de la escuela, incluyendo la estrategia de seguridad en línea y el uso de tecnología.

La Dirección General deberá garantizar que todos aquellos con responsabilidades de liderazgo y gestión promuevan activamente el bienestar de los estudiantes. La adopción de esta política forma parte de dicha responsabilidad.

La Dirección General llevará a cabo una revisión anual de los procedimientos de protección y su implementación, incluyendo la efectividad de esta política y las relacionadas, en función de los objetivos establecidos.

2. Dirección General y Equipo Directivo

La Dirección General tiene responsabilidad ejecutiva sobre la seguridad y el bienestar de los miembros de la comunidad escolar.

Los Designados de Salvaguarda (DSL) son miembros del Equipo Directivo con responsabilidad en protección y bienestar infantil. Su responsabilidad incluye la gestión de incidentes de protección relacionados con el uso de tecnología, conforme a la Política de Salvaguarda de la Escuela.

El Equipo Directivo trabajará con el Coordinador de IT y el Departamento de IT para monitorear el uso y las prácticas tecnológicas dentro de la escuela, y evaluar posibles mejoras que aseguren el bienestar digital de los estudiantes.

El Equipo Directivo revisará de forma regular el Registro de Incidentes Tecnológicos.

Los DSL actualizarán al equipo directivo regularmente sobre la operación de los mecanismos de salvaguarda, incluyendo las prácticas de seguridad en línea.

3. Coordinación de IT

El Coordinador de IT, junto con su equipo, es responsable del funcionamiento y efectividad del sistema de filtrado de la escuela con el fin de prevenir el acceso a material que represente riesgos, incluyendo material extremista o terrorista.

El Coordinador de IT deberá asegurar que:

- La infraestructura tecnológica de la escuela sea segura y no vulnerable a mal uso o ataques.
- Solo usuarios autenticados y autorizados puedan acceder a la tecnología de la escuela.
- El sistema de filtrado esté vigente, sea efectivo y se actualice regularmente.
- Se minimice el riesgo de que estudiantes o personal evadan los sistemas de protección implementados por la escuela.
- El uso de la tecnología sea monitoreado regularmente para asegurar el cumplimiento de esta política.
- El software de monitoreo se mantenga actualizado y permita rastrear el uso de correo e internet.

El Coordinador de IT reportará al Equipo Directivo sobre el funcionamiento de los sistemas tecnológicos y escalará cualquier preocupación de manera inmediata.

Asimismo, mantendrá el Registro de Incidentes Tecnológicos e informará cualquier situación de riesgo al DSL, conforme a la Política de Salvaguarda.

4. Todo el Personal

El personal deberá actuar como modelo de conducta responsable en el uso de tecnología y compartir con los estudiantes las políticas y prácticas seguras del colegio.

El personal deberá reportar cualquier preocupación relacionada con el bienestar o seguridad de los estudiantes, conforme a la política de Salvaguarda.

5. Padres de Familia

El rol de los padres es clave para asegurar que los estudiantes comprendan cómo mantenerse seguros en el entorno digital. La escuela espera que los padres:

- Apoyen la implementación de esta política y reporten inquietudes.
- Conversen con sus hijos sobre el uso de redes, dispositivos y medios digitales.
- Alienten a sus hijos a reportar situaciones de acoso o riesgo digital.

C. EDUCACIÓN Y CAPACITACIÓN

1. Estudiantes

El uso seguro de la tecnología forma parte integral del currículo de IT. Los estudiantes reciben orientación sobre el uso seguro de internet, redes sociales y dispositivos móviles.

En Early Years, la tecnología se integra a través de exploración, juego y reconocimiento de su uso en contextos cotidianos tanto en el hogar como en la escuela.

Asimismo, los mensajes de seguridad digital se refuerzan mediante clases, asambleas y sesiones de tutoría para enseñar:

- Riesgos asociados al uso de tecnología.
- Validación de información digital.
- Identificación de conductas sospechosas, acoso, radicalización y extremismo.
- Concepto y efectos del ciberacoso.
- Consecuencias de conductas negativas en línea.

2. Personal

La escuela brinda capacitación para asegurar que el personal comprenda riesgos digitales y sepa actuar ante incidentes.

La inducción incluye formación en Política de Seguridad Digital, Código de Conducta, Política de Correo y Redes, y lineamientos de uso profesional de redes sociales.

3. Padres

Se invita a los padres a revisar la Política de Uso Aceptable incluida en el Manual del Estudiante con sus hijos.

D. ACCESO A LA TECNOLOGÍA DE LA ESCUELA

Todo acceso requiere usuario y contraseña personal que no deberán compartirse. Visitantes cuentan con red Wi-Fi separada y acceso controlado.

E. USO DE DISPOSITIVOS MÓVILES

La escuela cuenta con sistemas de filtrado y monitoreo; sin embargo, reconoce que los datos móviles pueden permitir acceso no regulado.

El uso de dispositivos personales deberá contar con autorización previa.

F. PROCEDIMIENTOS ANTE MAL USO

Todo incidente debe ser reportado conforme a políticas de disciplina, salvaguarda y conducta.

G. MONITOREO Y REVISIÓN

Todo incidente grave quedará registrado y será evaluado dentro de revisiones de seguridad digital, con el fin de mejorar mecanismos de protección.

• Prepared by:	• Reviewed by:	• Approved by:
• ISP • Eustolia Martínez Rodríguez Melissa Ceulemans • Isaías Molina Carrillo Melina Estrella Morales	• Lucía Chavero Vallejo Melody Martín del Campo • María José Valencia González • Jennifer Barbour Martínez • Amanda Martín del Campo Jensen	• Melody Martín del Campo

September 2025