SEGURIDAD ONLINE

COLEGIO CEDES
DESDE 1932

Aprobado por :	**Fecha:**
Última revisión:	
Próxima revisión:	

1. Introducción

El Colegio CEDES reconoce que las tecnologías digitales y el acceso a internet forman parte esencial del proceso educativo y de la vida cotidiana del alumnado.

El centro se compromete a garantizar que el uso de internet y de las tecnologías digitales se realice de forma **segura, responsable y educativa**, protegiendo al alumnado frente a los riesgos asociados al entorno digital.

La seguridad online constituye una parte fundamental del marco de **Safeguarding and Child Protection** del centro y forma parte del compromiso institucional de proteger el bienestar y el desarrollo del alumnado.

Esta política establece:

- Normas para el uso seguro de internet y de las tecnologías digitales.
- Responsabilidades de los miembros de la comunidad educativa.
- Procedimientos de actuación ante incidentes online.
- Medidas preventivas y educativas para la protección del alumnado.

La política se aplica a todos los miembros de la comunidad educativa:

- Alumnado.
- Profesorado.
- Personal del centro.
- Familias.
- Visitantes.

2. Marco normativo

Normativa internacional

Esta política se basa en estándares internacionales de protección infantil y seguridad digital:

- Keeping Children Safe in Education (KCSIE).
- UK Safer Internet Centre Guidance.
- Education for a Connected World Framework.
- Prevent Duty Guidance.
- Working Together to Safeguard Children.

Estas normativas consideran la **seguridad online como una parte esencial de la protección del menor**.

Normativa española

El centro cumple con la legislación española aplicable:

- Ley Orgánica 8/2021 de Protección Integral a la Infancia y la Adolescencia frente a la Violencia (LOPIVI).
- Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

3. Alcance de la política

Esta política regula el uso de:

- Dispositivos tecnológicos del centro.
- Dispositivos personales utilizados en el colegio.
- Plataformas educativas digitales.
- Redes sociales.
- Comunicaciones digitales.

El centro podrá intervenir en incidentes ocurridos **fuera del entorno escolar** cuando estos tengan impacto en el bienestar del alumnado o en la convivencia escolar.

4. Riesgos online (Modelo 4C)

El colegio reconoce cuatro categorías principales de riesgos online.

Contenido

Acceso a contenidos inapropiados o perjudiciales:

- Pornografía.
- Violencia extrema.
- Discursos de odio.
- Desinformación.
- Contenidos que promuevan autolesión.
- Propaganda extremista.

Contacto

Interacciones peligrosas con terceros:

- Grooming.
- Manipulación online.
- Contacto con adultos desconocidos.

Conducta

Comportamientos inadecuados del alumnado:

- Ciberacoso.
- Sexting.
- Difusión de imágenes sin consentimiento.

- Uso irrespetuoso de redes sociales.

Riesgos comerciales

- Publicidad engañosa.
- Juegos con micropagos.
- Explotación de datos personales.

5. Roles y responsabilidades

Dirección del centro

- Garantizar la seguridad del alumnado.
- Supervisar la implementación de esta política.

DSL (Designated Safeguarding Lead)

- Gestionar incidentes online relacionados con safeguarding.
- Coordinar la respuesta ante riesgos digitales.
- Colaborar con autoridades externas cuando sea necesario.

Coordinador de Seguridad Online

- Supervisar la aplicación diaria de la política.
- Registrar incidentes online.
- Proporcionar formación al personal.

Equipo técnico

- Garantizar la seguridad de la red del centro.
- Implementar sistemas de filtrado y monitorización.
- Proteger la infraestructura tecnológica.

Profesorado

- Promover el uso responsable de internet.
- Supervisar el uso de dispositivos en el aula.
- Informar de incidentes online.

Alumnado

- Utilizar la tecnología de forma responsable.
- Respetar la privacidad de los demás.
- Informar de situaciones de riesgo online.

Familias

- Apoyar al centro en la promoción de la seguridad digital.
- Supervisar el uso de internet en el hogar.

6. Educación en seguridad online

El colegio integrará la educación digital en el currículo escolar.

El alumnado recibirá formación sobre:

- Identidad digital.
- Privacidad online.
- Prevención del ciberacoso.
- Uso responsable de redes sociales.
- Pensamiento crítico frente a la información digital.

7. Filtrado y monitorización

El centro implementa sistemas de filtrado y monitorización para proteger al alumnado frente a contenidos inapropiados.

Las medidas incluyen:

- Filtrado de contenidos online.
- Control de accesos a internet.
- Monitorización de actividad digital.
- Software antivirus y medidas de ciberseguridad.

8. Uso de dispositivos móviles

El uso de teléfonos móviles en el centro está regulado por la **Mobile Phone Policy**.

En general:

- Los estudiantes no podrán utilizar teléfonos móviles durante el horario escolar salvo autorización.
- Las comunicaciones urgentes con las familias se realizarán a través de recepción.

9. Uso de imágenes digitales

El uso de imágenes digitales debe respetar la privacidad y dignidad del alumnado.

Se aplicarán las siguientes normas:

- Consentimiento previo por escrito de las familias para publicar imágenes del alumnado.
- No publicar nombres completos junto a fotografías.
- El personal no utilizará dispositivos personales para tomar imágenes del alumnado.
- Las imágenes deberán captarse únicamente con dispositivos autorizados del centro.

- El alumnado no podrá grabar ni fotografiar a otras personas sin autorización.
- Las familias podrán tomar fotografías en eventos escolares únicamente para uso personal.
- Las imágenes no deberán publicarse en redes sociales si aparecen otros alumnos.

10. Protección de datos

El tratamiento de datos personales se realizará conforme a:

- **RGPD.**
- **LOPDGDD.**
- **LOPIVI.**

El centro garantizará:

- Almacenamiento seguro de la información.
- Acceso restringido a datos personales.
- Eliminación segura de datos.

Las comunicaciones digitales deberán realizarse exclusivamente a través de **plataformas oficiales del centro**.

11. Uso profesional de redes sociales

El personal deberá mantener una conducta profesional en redes sociales.

No está permitido:

- Comunicarse con estudiantes mediante redes sociales personales.
- Publicar información confidencial.
- Hacer referencia a estudiantes o familias en redes sociales personales.

El uso inapropiado de redes sociales podrá tratarse conforme al **Código de conducta del Staff**

12. Supervisión de redes sociales públicas

El centro podrá realizar supervisión razonable de contenidos públicos en internet relacionados con el colegio con el objetivo de proteger el bienestar del alumnado y de la comunidad educativa.

13. Riesgos específicos en el entorno digital

Sexting / Youth Produced Sexual Imagery

Se entiende por sexting la creación o difusión de imágenes sexuales producidas por menores.

Cuando el centro tenga conocimiento de un incidente:

1. El personal no compartirá ni reenviará las imágenes.
2. Se informará inmediatamente al DSL.
3. Se evaluará el incidente desde la perspectiva de safeguarding.
4. Se preservarán evidencias cuando sea necesario.
5. Se informará a las familias cuando proceda.
6. En situaciones graves se podrá informar a las autoridades competentes.

Inteligencia artificial y deepfakes

Las nuevas tecnologías de inteligencia artificial pueden generar nuevos riesgos.

Entre ellos:

- Manipulación de imágenes.
- Creación de deepfakes.
- Generación de contenido ofensivo mediante IA.
- Uso de herramientas de IA para el acoso digital.

Cualquier uso de estas tecnologías que afecte a la dignidad o reputación de otras personas será considerado **una conducta grave**.

14. Respuesta a incidentes de seguridad online

Cuando se detecte un incidente online:

1. Se informará al Coordinador de Seguridad Online
2. Se informará al DSL.
3. Se registrará el incidente.
4. Se evaluará la gravedad del caso.
5. Se aplicarán medidas educativas o disciplinarias.

Cuando exista sospecha de actividad ilegal:

- Se preservarán evidencias.
- Se podrá informar a las autoridades competentes.

15. Clasificación de incidentes online

Tipo de incidente	Ejemplos
Acceso a contenido inapropiado	Pornografía, violencia extrema
Uso indebido de redes sociales	Comentarios ofensivos
Ciberacoso	Insultos o amenazas
Difusión de imágenes	Compartir fotos sin consentimiento
Evasión de filtrado	Uso de VPN
Manipulación digital	Deepfakes
Sexting	Intercambio de imágenes sexuales
Conductas ilegales	Grooming

16. Acciones y medidas disciplinarias

El uso inadecuado de tecnologías digitales se gestionará conforme a la **Behaviour Policy del centro**.

Niveles de actuación

Nivel	Tipo de conducta	Medida disciplinaria	Reincidencia tras la medida
Nivel 1	Uso no autorizado de internet	Advertencia	Retirada del dispositivo
Nivel 2	Uso indebido de redes sociales	Comunicación a familias	Restricción de dispositivos
Nivel 3	Compartir contraseñas o evadir filtros	Intervención del coordinador	Medidas disciplinarias adicionales
Nivel 4	Difusión de imágenes o ciberacoso	Activación del protocolo de acoso	Medidas disciplinarias graves
Nivel 5	Conductas ilegales online	Intervención inmediata del DSL	Posible comunicación a autoridades

Reincidencia

Cuando un alumno repita una conducta tras una medida disciplinaria, el centro podrá:

- Aumentar el nivel disciplinario.
- Limitar el acceso a dispositivos o internet.
- Establecer medidas educativas específicas.
- Realizar seguimiento por parte del tutor.

17. Relación con otras políticas del centro

Esta política debe leerse junto con:

• Política de Salvaguarda y Protección del Menor.
• Política de Conducta.
• Política de Abuso entre Iguales (Peer on Peer Abuse).
• Código de Conducta del Personal.
• Política de Uso de Teléfonos Móviles.
• Política de Protección de Datos.

18. Revisión de la política

Esta política será revisada periódicamente para garantizar su actualización conforme a cambios legislativos y tecnológicos.

ANEXOS

- Anexo 1 – Compromiso del alumnado sobre el uso responsable de las tecnologías (Student Acceptable Use Agreement)
- Anexo 2 – Compromiso del personal sobre el uso profesional de las tecnologías (Staff Acceptable Use Agreement)
- Anexo 3 – Compromiso de las familias sobre el uso responsable de internet (Parent Acceptable Use Agreement)
- Anexo 4 – Protocolo de actuación ante incidentes de seguridad online
- Anexo 5 – Registro de incidentes de seguridad online

ANEXO 1 Acuerdo del alumnado sobre el uso responsable de las tecnologías *(Student Acceptable Use Agreement)*

El uso de internet y de las tecnologías digitales forma parte del aprendizaje en el Colegio CEDES. Para garantizar un entorno seguro y respetuoso, el alumnado se compromete a utilizar los recursos tecnológicos del centro de manera responsable.

Compromisos del alumnado

El alumnado se compromete a:

- Utilizar internet y los dispositivos digitales únicamente con fines educativos cuando esté en el centro.
- Seguir las indicaciones del profesorado sobre el uso adecuado de la tecnología en el aula.
- Respetar a los demás en los entornos digitales y comunicarse de forma adecuada y respetuosa.
- No participar en conductas de ciberacoso, insultos, amenazas o humillaciones a través de medios digitales.
- No compartir información personal propia ni de otros compañeros en internet.
- No publicar ni difundir imágenes, vídeos o información de otros estudiantes o miembros del personal sin autorización.
- No acceder a contenidos inapropiados o dañinos.
- No intentar eludir los sistemas de seguridad o filtrado del centro.
- No utilizar las tecnologías para engañar, suplantar identidades o difundir información falsa.
- Informar a un profesor o a un adulto del centro si se encuentra con contenido inapropiado o si observa una situación de riesgo online.

Uso responsable de dispositivos

El alumnado deberá:

- Utilizar los dispositivos y recursos tecnológicos del centro con cuidado y responsabilidad.
- No compartir contraseñas ni acceder a cuentas de otros usuarios.
- Respetar las normas establecidas en la Mobile Phone Policy del centro**.**

Seguridad online

El alumnado deberá recordar que:

- No todo lo que aparece en internet es fiable.
- Las acciones en internet pueden tener consecuencias reales.
- La información personal debe protegerse.

Incumplimiento de las normas

El incumplimiento de este acuerdo podrá dar lugar a:

- Medidas educativas.
- Restricciones en el uso de tecnología.
- Medidas disciplinarias conforme a la Behaviour Policy del centro.

Declaración del alumno/a. Declaro que he leído y comprendido las normas sobre el uso responsable de internet y de las tecnologías digitales en el Colegio CEDES y me comprometo a cumplirlas.

Nombre del alumno/a: _____

Curso: _____

Firma del alumno/a: _____

Fecha: _____

ANEXO 2 Acuerdo del personal sobre el uso profesional de las tecnologías *(Staff Acceptable Use Agreement)*

El personal del Colegio CEDES tiene la responsabilidad de utilizar las tecnologías digitales de forma profesional, segura y ética, contribuyendo a la protección y bienestar del alumnado.

Este acuerdo establece las normas para el uso adecuado de internet, dispositivos digitales y plataformas tecnológicas por parte del personal del centro.

Uso profesional de las tecnologías

El personal se compromete a:

- Utilizar las tecnologías del centro únicamente con fines profesionales y educativos.
- Mantener una conducta profesional en todos los entornos digitales.
- Respetar la privacidad y confidencialidad de la información del alumnado.
- Proteger los datos personales de estudiantes, familias y compañeros.
- Utilizar únicamente las plataformas oficiales del centro para la comunicación educativa.
- Informar de cualquier incidente relacionado con la seguridad online.
- Comunicarse con los estudiantes únicamente a través de los canales oficiales del centro.
- No utilizar redes sociales personales para comunicarse con el alumnado.
- Evitar cualquier contacto digital que pueda interpretarse como inapropiado o no profesional.
- Mantener siempre límites profesionales claros en las comunicaciones digitales.
- Mantener una conducta profesional en redes sociales.
- Revisar la configuración de privacidad de sus perfiles personales.
- Evitar publicar información que pueda afectar a la reputación del centro o de la comunidad educativa.
- Publicar información confidencial relacionada con el centro.
- Hacer referencia a estudiantes o familias en redes sociales personales.
- Compartir imágenes o información del alumnado sin autorización.
- Utilizar únicamente dispositivos autorizados por el centro para tomar fotografías o grabaciones del alumnado.
- No utilizar teléfonos móviles personales u otros dispositivos privados para captar imágenes o vídeos de estudiantes.
- Almacenar las imágenes o vídeos del alumnado únicamente en los sistemas seguros del centro.
- Utilizar contraseñas seguras y no compartirlas con terceros.
- Cerrar sesión en dispositivos compartidos.
- Evitar el almacenamiento de datos personales en dispositivos personales no autorizados.
- Seguir las normas establecidas en la política de protección de datos del centro.

Incidentes de seguridad online

El personal deberá informar inmediatamente al Coordinador de Seguridad Online o al DSL cuando detecte:

- Contenido inapropiado.
- Situaciones de ciberacoso.
- Difusión de imágenes sin consentimiento.
- Posibles riesgos de grooming u otras conductas online peligrosas.

Incumplimiento de las normas

El incumplimiento de este acuerdo podrá ser tratado conforme a:

- Staff Code of Conduct.
- Safeguarding and Child Protection Policy.
- Procedimientos disciplinarios del centro.

Declaración del miembro del personal Declaro que he leído y comprendido las normas sobre el uso profesional de las tecnologías digitales en el Colegio CEDES y me comprometo a cumplirlas.

Nombre , firma y fecha _____

ANEXO 3 Compromiso de las familias sobre el uso responsable de internet *Parent Acceptable Use Agreement)*

El Colegio CEDES considera fundamental la colaboración entre el centro educativo y las familias para promover un uso seguro, responsable y saludable de las tecnologías digitales. Las familias desempeñan un papel clave en la educación digital de los menores y en la prevención de riesgos en el entorno online. Este acuerdo tiene como objetivo fomentar la cooperación entre el centro y las familias para garantizar la seguridad del alumnado en el uso de internet y de las tecnologías digitales.

Compromisos de las familias

Las familias se comprometen a:

- Apoyar al centro en la promoción de un uso responsable y seguro de las tecnologías digitales.
- Supervisar el uso de internet de sus hijos en el hogar en la medida de lo posible.
- Hablar con sus hijos sobre los riesgos asociados al uso de internet y de las redes sociales.
- Fomentar un comportamiento respetuoso y responsable en los entornos digitales.
- Recordar a sus hijos la importancia de no compartir información personal en internet.

Seguridad digital en el hogar

Se recomienda a las familias:

- Establecer normas claras sobre el uso de dispositivos y redes sociales.
- Supervisar el tiempo de uso de dispositivos digitales.
- Conocer las plataformas digitales que utilizan sus hijos.
- Promover un uso equilibrado de la tecnología.

Comunicación con el centro

Las familias deberán informar al centro cuando detecten situaciones que puedan afectar al bienestar del alumnado relacionadas con:

- Ciberacoso.
- Difusión de imágenes sin consentimiento.
- Situaciones de riesgo en redes sociales.
- Cualquier incidente digital que implique a estudiantes del centro.

Uso de imágenes en eventos escolares

Las familias podrán realizar fotografías o vídeos durante eventos escolares públicos, como celebraciones o actuaciones, siempre que:

- Las imágenes se utilicen únicamente para uso personal y privado.
- No se publiquen en redes sociales si aparecen otros estudiantes sin consentimiento de sus familias.
- Se respete la privacidad del alumnado y del personal del centro.

Colaboración con el centro

El Colegio CEDES trabajará en colaboración con las familias para promover una cultura digital segura y responsable que contribuya al bienestar del alumnado.

Declaración de la familia

Declaro que he leído y comprendido el compromiso sobre el uso responsable de internet y de las tecnologías digitales del Colegio CEDES y me comprometo a colaborar con el centro en su aplicación.

Nombre del padre, madre o tutor legal: _____

Nombre del alumno/a: _____

Firma y fecha :_____

ANEXO 4 Procedimiento de actuación ante incidentes de seguridad online

El Colegio CEDES reconoce que el uso de internet y de las tecnologías digitales puede dar lugar a situaciones de riesgo para el alumnado. Este procedimiento establece las actuaciones que deben seguir los miembros del personal del centro cuando se detecte un incidente relacionado con la seguridad online.

1. Detección del incidente

Un incidente de seguridad online puede ser detectado por:

- Un miembro del personal del centro.
- Un estudiante.
- Una familia.
- Un tercero que informe al centro.

Entre los incidentes más comunes se incluyen:

- Acceso a contenidos inapropiados.
- Ciberacoso entre estudiantes.
- Difusión de imágenes sin consentimiento.
- Uso indebido de redes sociales relacionado con el centro.
- Intentos de eludir los sistemas de filtrado de internet.
- Situaciones relacionadas con sexting o intercambio de imágenes íntimas.

2. Comunicación del incidente

Cuando un miembro del personal detecte o tenga conocimiento de un incidente deberá:

- Informar inmediatamente al Coordinador de Seguridad Online o al DSL (Designated Safeguarding Lead).
- Evitar investigar el incidente por su cuenta sin la supervisión del responsable correspondiente.
- Evitar compartir la información con personas no implicadas en la gestión del caso.

3. Registro del incidente

El incidente deberá registrarse en el registro de incidentes de seguridad online del centro.

El registro incluirá:

- Fecha y hora del incidente.
- Descripción de los hechos.
- Personas implicadas.
- Evidencias disponibles (por ejemplo capturas de pantalla o enlaces).
- Medidas adoptadas.

4. Evaluación del incidente

El Coordinador de Seguridad Online o el DSL evaluará:

- La gravedad del incidente.
- El posible impacto en el bienestar del alumnado.
- Si se trata de un incidente disciplinario o de safeguarding.
- Si es necesario aplicar protocolos específicos del centro.

5. Aplicación de medidas

Dependiendo de la naturaleza del incidente, el centro podrá:

- Aplicar medidas educativas.
- Aplicar medidas disciplinarias conforme a la Behaviour Policy.
- Activar el protocolo de acoso escolar.
- Informar a las familias del alumnado implicado.

6. Preservación de evidencias

Cuando el incidente implique contenido digital relevante:

- Se procurará preservar las evidencias sin alterar los dispositivos.
- No se compartirán ni reenviarán imágenes o contenidos sensibles.
- Se seguirá el asesoramiento del DSL.

7. Comunicación con autoridades externas

En situaciones graves o cuando exista sospecha de actividad ilegal, el centro podrá:

- Consultar o informar a las autoridades competentes.
- Seguir las recomendaciones de los organismos de protección del menor.

8. Seguimiento del caso

Una vez gestionado el incidente, el centro podrá:

- Realizar seguimiento del bienestar del alumnado implicado.
- Aplicar medidas educativas relacionadas con la seguridad digital.
- Revisar las medidas preventivas del centro.

9. Confidencialidad

Todos los incidentes de seguridad online deberán tratarse con confidencialidad, respetando en todo momento la protección de datos y el bienestar de los menores implicados.

Registro de incidentes de seguridad online / safeguarding

Todos los incidentes relacionados con la seguridad online o con posibles riesgos para el bienestar del alumnado deberán registrarse de forma inmediata y precisa.

El registro deberá incluir, como mínimo, la siguiente información:

Fecha y hora del incidente.

Nombre del alumno o alumnos implicados.

Curso o grupo al que pertenecen.

Nombre del miembro del personal que detecta o recibe la información.

Descripción detallada del incidente, incluyendo el contexto en el que se produjo y las circunstancias relevantes.

Tipo de incidente, especificando si se trata, por ejemplo, de:

- Ciberacoso.
- Acceso a contenido inapropiado.
- Uso indebido de dispositivos.
- Compartición de imágenes íntimas.
- Conductas de riesgo en internet.

Medidas inmediatas adoptadas por el centro para garantizar la seguridad del alumnado.

Personas informadas, incluyendo:

- Tutor o responsable del grupo.
- Designated Safeguarding Lead (DSL).
- Equipo directivo.

Comunicación con las familias, cuando proceda.

Decisiones adoptadas por el centro, incluyendo medidas educativas, disciplinarias o de protección.

Seguimiento del caso, indicando si se requieren acciones adicionales o monitorización posterior.