



## PROTOCOLO SOBRE USO DE REDES SOCIALES PARA LOS MIEMBROS DE LA COMUNIDAD SAN CARLOS DE ARAGÓN.

### **Introducción:**

A través del presente documento se busca promover una sana convivencia entre todos los miembros de la comunidad educativa.

Asimismo, tiene una función instructiva y preventiva, puesto que está orientado a educar acerca del uso adecuado de los medios digitales y prevenir situaciones que afecten y/o perjudiquen a miembros de la Comunidad Escolar, informando el tipo y grado de falta ante el uso indebido de medios electrónicos y redes sociales.

### **FUNDAMENTACIÓN Y MARCO LEGAL:**

El derecho a la privacidad y el derecho a la intimidad de los menores respectivamente esta reglamentados en la constitución de Chile y la carta fundamental de derechos humanos.

La protección de la privacidad está reconocida, con carácter general, en el artículo 12 de la Declaración Universal de los Derechos Humanos, «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques». Dos décadas después, se firmó en Nueva York el Pacto de Derechos Civiles y Políticos, cuyo artículo 17 determina: «Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. [...] Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

Se reconoce el derecho a la protección de la vida privada en el artículo 16 de Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989.

En particular, en su artículo sobre Derechos del Niño determina que:

«Todo niño tiene derecho a las medidas de protección que su condición de niño requiere por parte de su familia, de la sociedad y del Estado». La Constitución chilena no contiene una norma expresa en relación a la protección de datos personales, sin embargo, sigue en buena parte el modelo del artículo 12 de la Declaración Universal de Derechos Humanos, por lo que dicha protección constitucional se puede derivar de lo establecido en el artículo 19 número 4 que establece que la Constitución asegura el respeto y protección a la vida privada y a la honra de la persona y de su familia.

La Corte Suprema chilena se ha servido de dicho precepto para condenar casos donde se suben a internet fotos de terceras personas unidos a posibles comentarios denigrantes, siendo éste uno de los contenidos esenciales del derecho a la protección de datos (Figueroa García, 2013: 875). Chile fue el primer país de Latinoamérica que promulgó una ley de protección a la privacidad, la Ley 19.6289 sobre Protección de la Vida Privada, del 18 de agosto de 1999, que contiene los principios fundamentales de la protección de datos personales en este país andino (Chen Mok, 2010: 128).

En segundo lugar en el Capítulo XVII de la Ley General De derechos de niña, niño y adolescente.

Del Derecho a la Intimidad.

Artículo 76.

Niñas, niños y adolescentes tienen derecho a la intimidad personal y familiar, y a la protección de sus datos personales.

Niñas, niños y adolescentes no podrán ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia; tampoco de divulgaciones o difusiones

ilícitas de información o datos personales, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación.

Quienes ejerzan la patria potestad, tutela o guarda y custodia, deberán orientar, supervisar y, en su caso, restringir, las conductas y hábitos de niñas, niños y adolescentes, siempre que atiendan al interés superior de la niñez.

Artículo 77.

Se considerará violación a la intimidad de niñas, niños o adolescentes cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación que cuenten con concesión para prestar el servicio de radiodifusión y telecomunicaciones, así como medios impresos, o en medios electrónicos de los que tenga control el concesionario o medio impreso del que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.

### DESCRIPCIÓN:

Dando respuesta a las nuevas herramientas de comunicación y redes sociales que son parte del quehacer diario de nuestra comunidad, el Centro Educativo San Carlos de Aragón prohíbe el uso de imágenes de menores de edad en redes sociales privadas de los funcionarios, pues no podemos garantizar a sus padres y apoderados el buen uso de estas imágenes.

Como institución no podemos controlar el uso de la imagen, o si se mal usa para menoscabar, agredir, o dañar la reputación de un estudiante por un tercero.

Por tanto, reconocemos como vía de comunicación oficial entre apoderados y el colegio la agenda escolar o el cuaderno de comunicaciones, de no ser posible o dada la emergencia o la urgencia, dicha comunicación se realizará vía telefónica, no mediante redes sociales.

- Se solicita evitar la comunicación mediante correos o celulares personales. Dado que la vía de comunicación oficial entre estudiantes y profesores es personalmente durante la clase es el profesor quien deberá procurar que sea en esta instancia donde se fijen las fechas de pruebas, trabajos, materiales, etc. Si eventualmente se requiriera realizar algún cambio este será informado a los apoderados vía comunicación o agenda semanal.
- Ningún funcionario podrá referirse de manera grosera u ofensiva contra otro integrante de la comunidad escolar o contra la organización misma a través de las redes sociales.
- Se recomienda y se solicita a los profesores no incluir a los estudiantes en sus cuentas personales de Facebook, Twitter u otras redes sociales. Esto con la finalidad de proteger su privacidad y mantener una relación de probidad y vínculo de respeto entre estudiante y profesor.
- Se prohíbe la publicación de cualquier artículo u imagen que sea de exclusiva competencia del colegio, ya sea para entregar información o dar aviso acerca de algún estudiante o situación en la que estos se involucren, en ninguna red social.
- Se solicita no subir fotos de alumnos a WhatsApp, Facebook u otros medios o redes sociales, que comprometan el uso del uniforme del establecimiento, sala de clases o dependencias del establecimiento.
- Se prohíbe grabar a funcionarios o estudiantes sin su consentimiento o autorización.
- Se prohíbe subir imágenes de estudiantes o funcionarios del establecimiento a redes sociales sin su autorización y previo consentimiento.
- Solamente se autorizará subir imágenes a página web del colegio.
- El encargado de la administración de la página Web, ésta autorizado por la Dirección del establecimiento a subir imágenes que comprometan la imagen de la institución y sus participantes en actividades tales como actos, celebraciones, aniversario, etc.
- Entendiendo, que las imágenes que se exhibirán serán de actividades escolares, en contexto de colegio, por lo que no dañarán ni entregan comentarios respecto de los estudiantes, ni el ánimo de dañar su imagen u honra. Manteniendo su administración en manos de un adulto responsable representante del colegio, como órgano protector de los derechos de los niños.

## ALUMNOS

- El uso de internet en el interior del Colegio es de carácter estricto y restringido solo a la realización de trabajos, tareas o actividades pedagógicas debidamente establecidas por el profesor o el encargado de la sala de computación o biblioteca.
- Se prohíbe grabar a funcionarios o estudiantes sin su consentimiento o autorización.
- Se prohíbe subir imágenes de estudiantes o funcionarios del establecimiento a redes sociales sin su autorización y previo consentimiento.
- Está estrictamente prohibido visitar sitios con cualquier tipo de contenido de carácter erótico o pornográfico en el interior del colegio, utilizando para ello cualquier medio tecnológico posible.
- El almacenamiento de material pornográfico infantil y la visita de sitios con igual contenido, es un delito debidamente tipificado por la ley, por lo que el Colegio o su personal tienen la obligación imperativa, moral y legal de denunciarlo a las autoridades competentes.
- Se prohíbe el uso de internet en el interior del colegio para visitar sitios que inciten a la violencia, discriminación o que se dediquen a denigrar a las personas.
- La vía de comunicación oficial entre estudiantes y profesores durante la clase es en la sala de clases o en el establecimiento de manera formal y personal, utilizando los canales oficiales.
- Es esa la instancia en donde se fijarán fechas de pruebas, trabajos, materiales, etc. Si eventualmente se requiriera realizar algún cambio este será informado a los apoderados vía agenda escolar o página Web del establecimiento.
- Eventualmente y, por lo general, en cursos superiores se les podrá solicitar enviar sus trabajos por correo electrónico. Este correo será una cuenta creada para este objetivo y no personal de los docentes.
- Cada correo deberá tener claramente identificado quién lo emite.
- A ningún estudiante le está permitido insultar, denigrar, burlarse o maltratar a cualquier integrante de la comunidad educativa causando menoscabo o la ofensa a través de las redes sociales.
- Está terminantemente prohibido utilizar la imagen de otra persona sin su consentimiento subiendo a redes sociales fotos, videos o comentarios que sean irrespetuosos, burlescos u ofensivos, o que afecten psicológicamente.
- El Colegio no se hace responsable del uso indebido por parte de los alumnos y/o funcionarios de Facebook, Twitter, Whatsapps o cualquier otra red social, la responsabilidad de dichos actos recae única y exclusivamente sobre las familias, tutores o cuidadores que estén a cargo de los menores, especialmente cuando han mentido respecto de la información requerida y entregada para la obtención de una cuenta, o directamente en el funcionario como mayor de edad.
- El hacer caso omiso a lo anteriormente establecido puede acarrear sanciones de acuerdo a lo señalado en el manual de convivencia escolar.

## APODERADOS

- Si un apoderado lo requiere, puede solicitar las instalaciones del colegio para utilizar internet en la biblioteca, respetando el horario de atención y contrato de los funcionarios, después del horario de clases y previa cita vía agenda, informando a todos los involucrados. Esta acción podrá ser realizada siempre y cuando las dependencias no estén ocupadas o estén dispuestas para otra acción de la unidad educativa.
- El uso de internet solicitado por los apoderados debe ser para apoyar a su hijo o hija en las tareas o trabajos, o en alguna situación de emergencia, entendiéndose que los primeros beneficiarios de este instrumento de trabajo deben ser los estudiantes y funcionarios del establecimiento.
- En toda situación se debe hacer un uso correcto: está estrictamente prohibido visitar sitios con cualquier tipo de contenido de carácter erótico o pornográfico en el interior del colegio, se prohíbe el uso de internet en el interior del colegio para visitar sitios que inciten a la violencia, discriminación o que se dediquen a denigrar a las personas.
- Se prohíbe grabar a funcionarios o estudiantes sin su consentimiento o autorización.
- Se prohíbe subir imágenes de estudiantes o funcionarios del establecimiento a redes sociales sin su autorización y previo consentimiento.

- La vía de comunicación oficial entre apoderados y el colegio es la agenda escolar, los docentes no responderán llamados telefónicos para resolver situaciones pedagógicas de los estudiantes.
- Se enviará información del quehacer pedagógico vía agenda semanal o en la página Web del establecimiento.
- La información entregada a través de otras vías de comunicación y/o redes sociales entre distintos actores de la comunidad, no es la oficial y no reemplaza la comunicación por vías formales. Ningún apoderado podrá usar el correo electrónico, redes sociales u otro dispositivo para denigrar, insultar o perjudicar a otra persona sea en forma directa, por ejemplo, mediante insultos o apodos, ni de forma indirecta, como imágenes o cualquier otro tipo de forma de burla hacia algún miembro de la comunidad.
- Ningún apoderado podrá referirse de manera grosera u ofensiva a otro integrante de la comunidad escolar o contra la organización misma a través de las redes sociales.
- Para canalizar sus molestias o inquietudes se deberán utilizar las vías dispuestas para tal efecto (entrevista con el profesor, inspector, encargada de convivencia escolar, dirección, etc.). De no cumplirse lo dicho anteriormente el afectado podrá tomar las acciones legales que considere pertinentes y podrá solicitarse como última medida el cambio de apoderado.
- En caso de emergencia o en casos justificados el establecimiento podrá realizar contacto telefónico para resolver situaciones emergentes o accidentes.

El Colegio promueve el uso de TIC en el entendido que son insumos para mejorar la efectividad pedagógica de los educadores y potencian los aprendizajes significativos en los alumnos, posibilitando en los estudiantes la adquisición de conocimientos, habilidades y actitudes que les permitan tomar decisiones tecnológicas como usuarios, consumidores y creadores de tecnología.

Asimismo, las TIC contribuyen en una mejor gestión y administración más eficiente del sistema educativo.

El propósito de este protocolo es el de normar sobre las prácticas éticas que regulan el uso de los recursos tecnológicos de la información y comunicaciones.

Un ciudadano digital, en este caso quienes integran la comunidad escolar, se espera actúe con responsabilidad e integridad, acorde a los valores de nuestro Colegio.

### **1. Propiedad y privacidad**

Todos los dispositivos digitales, computadores y servidores del Colegio, son propiedad del establecimiento escolar. Como tal, el personal administrativo y académico podrá revisar archivos y comunicados para mantener el sistema íntegro y para asegurarse de que los estudiantes están usando estos recursos adecuadamente y con responsabilidad. No se garantiza la privacidad de los archivos guardados en los servidores del centro u otros equipos informáticos del Colegio.

### **2. Uso apropiado y aceptable de los Recursos Tecnológicos**

Todos los recursos tecnológicos de la información y comunicación del Colegio deberán utilizarse como medio de apoyo educacional con el fin de apoyar y maximizar los recursos disponibles para el aprendizaje y el conocimiento.

El uso correcto de estos medios implica educar en el estudiante las destrezas necesarias para acceder, seleccionar, usar, crear y publicar información. Asimismo, implica desarrollar el pensamiento crítico para analizar, reconocer y reflejar los valores, creencias, perspectivas y predisposiciones en diferentes fuentes de información.

### **El uso adecuado de las TIC contempla:**

- Tanto fuera como dentro del Colegio actuar con responsabilidad e integridad en la utilización de todo medio tecnológico, basada en los valores del Colegio y en las normas especificadas en este protocolo.
- Utilizar los medios tecnológicos bajo los valores de la convivencia y respeto mutuo, utilizando un lenguaje apropiado, sin ningún tipo de conducta constitutiva de maltrato escolar, usando medios tecnológicos de TIC o constitutivas de ciberbullying

(especificado más adelante). Por lo tanto, reflexionar cuidadosamente acerca de lo que publica en línea y sólo enviar información fidedigna.

- Respetar la privacidad y confidencialidad propia y ajena, utilizar con confidencialidad la información tal como nombre, edad, contraseñas, dirección, teléfonos, horarios y otros datos personales, excepto en casos especiales y aprobados por el Colegio. No utilizar nombres de usuario, información ni contraseñas ajenas, ni grabar a profesores y otro personal del Colegio sin previa autorización.
- Cuidar los sistemas de informática del Colegio, tanto en cuanto a los materiales y equipos, como a sus archivos. No instalar ni desinstalar archivos ni programas sin la debida autorización
- Reportar a un adulto responsable y/o profesor(a) cualquier caso de acoso, ciberbullying, amenaza, comentarios de odio o contenido inapropiado. También deberá reportar si es que ocurre acceso inadvertido a material inapropiado, sospecha de recepción de mensajes que posean contenido de virus, robo o pérdida de recursos informáticos o de equipo, robo de información personal (claves, etc.), intento de estafa, etc.

### 3. Consecuencias del mal uso

Cualquier acto intencional del estudiante donde se dañe la dignidad, integridad y/o privacidad de la persona o la propiedad del Colegio, tales como programas, computadores, tabletas, sistemas operativos, etc. se considerará como faltas y se tomarán las medidas disciplinarias correspondientes. Según el tipo de falta (leve, grave, muy grave) se aplicará una sanción de acuerdo a los procedimientos disciplinarios y formativos del Colegio.

Cualquier acto que implique hacer reparaciones, reemplazo o correcciones en la tecnología del Colegio o datos, también es considerado como falta y los costos económicos de la reparación serán asumidos por el padre, madre y/o apoderado.

### 4. Definiciones de situaciones de riesgo en el uso de TIC:

Para una mejor comprensión definiremos algunos de los ataques por medios virtuales, más comunes:

- a. Ciberbullying:** El ciberbullying es el acoso psicológico entre pares, a través de medios tecnológicos (por ejemplo en Internet y redes sociales, telefonía celular y videojuegos online). Puede manifestarse a través de amenazas, burlas, envío de mensajes ofensivos, provocación con vocabulario grosero, trato irrespetuoso, difamación, propagación de información personal.

#### El ciberbullying se caracteriza por:

- Ser una situación sostenida en el tiempo, excluyendo circunstancias puntuales.
- Constituir situaciones de hostigamiento psicológico, pero no necesariamente con una intención sexual. Sin embargo, podría contener algunos rasgos de esta naturaleza.
- Tanto víctimas como acosadores suelen tener edades similares (siempre menores de edad).

- Desarrollarse a través de medios digitales, especialmente a través de las redes sociales.
- Vincularse la mayoría de las veces a situaciones de acoso en la vida real.
- Llegar a una audiencia mayor al generarse en un ambiente virtual, donde existen muchísimas posibilidades de replicar los comentarios, burlas o situaciones de acoso.
- El acosador suele ampararse en el anonimato.
- Contar generalmente con testigos, que suelen estar al tanto de la situación que vive la víctima, pero no siempre actúan para denunciar o ayudan a solucionar el conflicto.
- Tener graves consecuencias.

### **El ciberbullying puede darse de las siguientes maneras:**

- **Acoso:** Es el envío constante y repetido de mensajes crueles, viciosos o amenazantes. Por ejemplo, organizar concursos de votaciones que promuevan la “marcada” de una persona, resaltando algún aspecto negativo de ella. Por ejemplo: “voten I LIKE quienes encuentran gorda a ...”
- **Denigración:** Consiste en crear o utilizar sitios webs, portales de Internet u otras plataformas tecnológicas o virtuales, con el propósito deliberado y directo de insultar, denostar o atacar a una persona. Como por ejemplo, publicar en Internet secretos, información o imágenes (reales o trucadas), con el objetivo de avergonzar, humillar o denigrar la honra de ésta.
- **Injurias y calumnias:** La calumnia es la imputación de un delito determinado, pero falso. La injuria es toda expresión proferida o acción ejecutada en deshonor, descrédito o menosprecio de otra persona. Estas acciones tienen el fin de denigrar, dañar la reputación, la honra y amistades de la persona afectada. Por ejemplo, hacer circular rumores en los cuales a la víctima se le atribuya un comportamiento reprochable, ofensivo o desleal.
- **Suplantación:** Suplantar la identidad de la víctima, creando un perfil falso en redes sociales u otros servicios webs, donde se escriben, a modo de confesiones, opiniones infundadas o de manera irrespetuosa respecto a una persona o un grupo en particular.
- **Usurpación de identidad:** Usurpar la clave de algún medio en redes sociales para utilizarla, enviando material vicioso o embarazoso para otros y para la víctima.
- **Exclusión:** intencionalmente excluir a alguien de un grupo en línea.
- **Pelears en línea** mediante mensajes electrónicos con lenguaje vulgar y denigrante.
- **Amenazas:** Se refiere al acto de causar temor al otro expresándole una intención de daño o riesgo serio hacia él o hacia su familia. En relación a su persona, honra o propiedad. Por ejemplo, enviar mensajes amenazantes en varios lugares de internet en los que se relaciona la víctima de manera habitual, provocándole una sensación de completo agobio.
- **Happy-slapping:** La acción de grabar, filmar o registrar agresiones y/o actos de violencia física, normalmente en el ámbito escolar, mediante teléfonos celulares, cámaras webs u otros aparatos o tecnologías, difundiendo tales agresiones para que circulen por la red o publicándolos en portales de Internet o servidores para videos.

- b. Grooming:** Se llama grooming a la acción premeditada de un adulto de acosar sexualmente a un niño mediante el uso de Internet. El grooming solo lo ejercen los adultos hacia los menores de edad.

**El grooming se caracteriza por:**

- **El acosador usa perfiles falsos:** Generalmente el acosador se hace pasar por jóvenes, niños o adultos muy atractivos.
- **Iniciarse a partir de una amistad:** El acosador se contacta a través de las redes sociales o videojuegos en línea con el menor para conocer sus intereses y gustos. Después de generar el contacto inicial y ganar su confianza, se profundiza el vínculo de amistad a lo largo del tiempo.
- **Establecerse a partir de una relación de confianza y amistad:** Una vez establecida la confianza en la relación de amistad entre el acosador y el menor, el adulto propone diálogos personales e íntimos. El acosador, con frecuencia, le pide al menor que participe de actos de naturaleza sexual, grabaciones de videos o toma de fotografías.
- **Es probablemente la más severa y peligrosa de los cyber-acosos.** El objetivo final del adulto es seducir, engañar y/o abusar sexualmente de la víctima. Es considerado un delito y está penado por ley. Si se sospecha de este tipo de cyber-acoso sexual, el adulto que reciba esta información debe realizar la denuncia ante Carabineros, Fiscalía o PDI dentro de las 24 horas de conocida la situación.

**c. Grabación y difusión de situaciones privadas.**

Es la acción en que se capta, intercepta, graba o reproduce conversaciones o comunicaciones, imágenes o hechos, todos de carácter privado, que ocurre en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio. Es un delito que se sanciona legalmente. También se sanciona a quien sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado.

**ACTUALIZADO DICIEMBRE 2019**