LAUDE SAN PEDRO INTERNATIONAL COLLEGE

Política de seguridad electrónica

2025

Datos de contacto		
Principal	Mandy Palmer	m.palmer@laudesanpedro.com
Subdirector de Seguridad y Bienestar	Nicky de Comarmond	n.decomarmond@laudesanpedro.com
EYFS y Primaria	Arancha Barrasa	a.barrasa@laudesanpedro.com
Secundario	Joe Short	j.short@laudesanpedro.com
Director General Regional del ISP	Miguel Ángel Garrán	mgarran@ispschools.com

1.0 Introducción

En Laude San Pedro queremos que todos los miembros de nuestra comunidad tengan una comprensión compartida de nuestra visión, valores, estándares, políticas y procedimientos para que todos podamos trabajar para crear un entorno de aprendizaje positivo y ambicioso para los alumnos bajo nuestro cuidado:

Visión

"Seguro, feliz, aprendiendo"

Misiones

Inspiramos a nuestros estudiantes a convertirse en aprendices motivados y respetuosos en nuestra comunidad escolar internacional, inclusiva y dinámica. Los empoderamos para que alcancen su potencial individual mediante el desarrollo de relaciones positivas en un entorno seguro, feliz y enriquecedor.

Valores fundamentales

Resiliencia
Empatía
Aspiración
Coraje
Honestidad

2.0 Justificación

El propósito de esta declaración de política es:

- Garantizar la seguridad y el bienestar de los niños, jóvenes y personal es primordial cuando se utiliza Internet, redes sociales o dispositivos móviles.
- Proporcionar al personal y a los voluntarios los principios generales que guían nuestro enfoque de la seguridad en línea y que se respeten nuestros códigos de conducta.
- garantizar que, como organización, operamos de acuerdo con nuestros valores y dentro de la ley en términos de cómo usamos los dispositivos en línea
- Establecer mecanismos eficaces para identificar, intervenir y escalar incidentes cuando sea apropiado.

Creemos que:

- Los niños y jóvenes nunca deberían sufrir abusos de ningún tipo.
- Los niños deberían poder usar Internet para su educación y desarrollo personal, pero es necesario implementar medidas de seguridad para garantizar su seguridad en todo momento.

Reconocemos que:

- El mundo en línea ofrece a todos muchas oportunidades; sin embargo, también puede presentar riesgos y desafíos.

- Tenemos el deber de garantizar que todos los niños, jóvenes y adultos involucrados en nuestra organización estén protegidos de posibles daños en línea.
- Tenemos la responsabilidad de ayudar a mantener seguros a los niños y jóvenes en línea, ya sea que utilicen o no nuestra red y dispositivos.
- Trabajar en colaboración con niños, jóvenes, sus padres, cuidadores y otras agencias es esencial para promover el bienestar de los jóvenes y ayudarlos a ser responsables en su enfoque de la seguridad en línea.
- Todos los niños, independientemente de su edad, discapacidad, cambio de género, raza, religión o creencias, sexo u orientación sexual, tienen derecho a igual protección contra todo tipo de daño o abuso.

3.0 Rol y responsabilidades

Todo el personal

Buscaremos mantener seguros a los niños y jóvenes mediante:

- modelar el uso responsable de la tecnología y firmar su acuerdo de laPolítica de uso aceptable(ver Apéndice 1)
- impartir clases de seguridad electrónica y reforzar las buenas prácticas (EYFS, profesores de primaria y especialistas relevantes en secundaria)
- Informar rápidamente sobre problemas de seguridad electrónica
- Proporcionar instrucciones claras y específicas al personal y a los voluntarios sobre cómo comportarse en línea a través de nuestro Código de conducta del personal.
- Apoyar y alentar a los niños a usar Internet, las redes sociales y los teléfonos móviles de una manera que los mantenga seguros y muestre respeto por los demás.
- Apoyar y alentar a los padres y cuidadores a hacer todo lo posible para mantener a sus hijos seguros en línea.
- desarrollando unaacuerdo de seguridad en líneaPara usar con jóvenes y sus padres o cuidadores
- Desarrollar procedimientos claros y sólidos que nos permitan responder adecuadamente a cualquier incidente de comportamiento inapropiado en línea, ya sea por parte de un adulto, un niño o un joven.
- Revisar y actualizar periódicamente la seguridad de nuestros sistemas de información.
- garantizar que los nombres de usuario, los inicios de sesión, las cuentas de correo electrónico y las contraseñas se utilicen de forma eficaz
- garantizar que la información personal sobre los adultos y los niños que participan en nuestra organización se mantenga de forma segura y se comparta solo cuando sea apropiado
- garantizar que las imágenes de niños, jóvenes y familias se utilicen únicamente después de haber obtenido su permiso por escrito y únicamente para el propósito para el cual se ha otorgado el consentimiento
- Proporcionar supervisión, apoyo y capacitación al personal y voluntarios sobre seguridad en línea.
- Examinar y evaluar los riesgos de todas las plataformas de redes sociales y nuevas tecnologías antes de utilizarlas en la escuela.

El personal estará atento durante el uso de sitios web/tecnología y monitoreará los riesgos potenciales, incluidos:

- Acoso o intimidación en línea ("ciberacoso") por parte del estudiante u otros
- Publicar información sobre sí mismos que: a) podría usarse para avergonzarlos o manipularlos; b) podría causar daño psicológico; c) podría ser utilizada por delincuentes para robar su identidad o propiedad o, aunque es muy raro, determinar su ubicación física para causar daño físico
- Daños a la reputación o a las perspectivas futuras debido al propio comportamiento de los jóvenes o el de sus compañeros: publicaciones desagradables o enojadas, fotos o videos comprometedores o conflictos grupales representados en textos e imágenes.
- Pasar demasiado tiempo en línea, perdiendo el sentido del equilibrio en sus actividades.
- Exposición a contenido inapropiado
- Posibilidad de contacto inapropiado con adultos (los padres o tutores deben asegurarse de que las redes sociales no conduzcan a contactos fuera de línea no aprobados por ellos y otros adultos responsables en la vida de sus hijos).
- Explotación Sexual Infantil (ESI) y Explotación Criminal Infantil (ECI) que pueden comenzar en las Redes Sociales.

Padres/cuidadores

Pedimos a todas las familias que:

- sApoyar la política de seguridad electrónica de la escuela y discutir el uso seguro de Internet en casa.
- supervisar el uso que hacen sus hijos de las plataformas y aplicaciones en línea
- Informar a la escuela sobre problemas de seguridad electrónica

Estudiantes

Se espera que todos los estudiantes:

- Utilice la tecnología de manera responsable y respetuosa
- Mantener un buen comportamiento en línea y no hacer ni participar en nada que sea ilegal o delictivo o que implique una violación de las reglas de la escuela.
- Actuar con cautela y discreción en Internet, y adoptar y mantener en todo momento una actitud de precaución.
- Piensa antes de escribir, publicar y compartir algo, considerando la importancia y el significado si esto luego se comparte más ampliamente.
- Evite publicar comentarios o imágenes que puedan molestar, enojar, dañar o herir a otras personas.
- evitar utilizar cualquier tipo de lenguaje que pueda considerarse blasfemo, profano, obsceno o amenazante
- Mantengan sus contraseñas en secreto y seguras, sin compartirlas con nadie más que sus padres o tutores legales. Si alguien se apropia de su identidad en internet sin su conocimiento, podría ser considerado responsable.

- utilizar la cuenta de correo electrónico del colegio exclusivamente para fines académicos, entendiendo que es una herramienta de trabajo; el colegio se reserva el derecho de eliminar la cuenta de correo electrónico en los casos en que se detecte un uso indebido o inadecuado y se considere necesario
- Actuar con absoluta precaución al participar en juegos en línea, abrir correos electrónicos donde pueda haber sospechas, participar en encuestas e invitaciones de fuentes desconocidas, evitar páginas que soliciten dinero o información de tarjetas de crédito, mantener la integridad del colegio y proteger su información.
- No entrar en páginas web no confiables
- no chatear, enviar o consultar mensajes, jugar o ver vídeos a menos que se lo soliciten directamente, descargar música, comentar en blogs o foros, jugar o participar en juegos en línea, entrar en redes sociales, participar en concursos, crear eventos, contratar servicios o comprar productos en línea
- Entregar y mostrar el dispositivo al docente cuando lo considere apropiado o cuando exista preocupación por su mal uso.
- Informar sobre cualquier contenido o comportamiento inapropiado a un adulto de confianza.
- Siga las reglas de la escuela para el uso seguro de Internet.
    - Nunca acuerdes encontrarte con alguien que hayas conocido en la web.
    - Nunca proporcione información personal, por ejemplo, números de teléfono, dirección, fotos.
    - Si encuentras algo en la web que sea inapropiado u ofensivo, díselo a un adulto.
    - Nunca uses tu nombre real, siempre un apodo.
    - Mantenga su contraseña en secreto para los demás: solo comparta las contraseñas con sus padres o tutores para que puedan brindarle apoyo.
    - Si recibes un mensaje o una imagen desagradable, repórtalo a un adulto, bloquéalo y repórtalo al sitio en el que estás.
    - Asegúrese de que al usar sitios de redes sociales, la configuración de privacidad esté marcada para que no cualquiera pueda ver su página/fotos.
    - Utilice una cámara web únicamente con personas que conozca y haya conocido cara a cara.

No está permitido el uso de sitios de redes sociales en la escuela ni en los equipos escolares.

4.0 Uso de tecnologías

Ya sea utilizando material escolar o su propio dispositivo (como es el caso actualmente en el sexto curso), los usuarios no deberán visitar sitios de Internet, crear, publicar, descargar, transmitir, comentar o remarcar contenido relacionado con:

- pornografía (incluida la pornografía infantil)
- promover la discriminación de cualquier tipo
- promover el odio religioso
- promover actos ilegales

- armas
- mostrar cualquier otra información que pueda resultar ofensiva para otros estudiantes, personal, visitantes o cualquier miembro del público
- utilizar otras cuentas de usuario ni modificar ni eliminar ninguna de las cuentas, archivos o contraseñas
- instalar o intentar instalar programas de cualquier tipo

Es importante que los estudiantes comprendan

- Deben evitar utilizar el logotipo, uniforme, símbolos y otras imágenes asociadas a Laude International College en sus cuentas personales de redes sociales, sin la autorización expresa del Director.
- Deben actuar con corrección y cautela al publicar fotos e imágenes con el uniforme escolar. En este sentido, Laude International College se reserva el derecho de exigir la eliminación de internet de cualquier imagen o contenido relacionado con el colegio publicado sin el consentimiento del director.
- Se considera conducta extremadamente grave por parte del estudiante realizar bromas, burlas, comentarios hirientes, malintencionados u ofensivos en internet y redes sociales sobre otros estudiantes, padres, familias, tutores, profesorado, personal de administración y servicios o equipo directivo.
- que la ley castiga la fabricación o tenencia de herramientas, materiales, instrumentos, sustancias, máquinas o aparatos destinados a la comisión de delitos y, más específicamente, los destinados a la falsificación de documentos oficiales o privados con ánimo de engaño

En caso de sospecha u observación de contenido inapropiado, el personal deberá aplicar las normas escolares según corresponda. El contenido utilizado para intimidar a otros se tomará muy en serio, de acuerdo con la Política de Conducta y Antibullying.

Si el material se considera grave, se podrá confiscar el dispositivo y retenerlo como prueba (de un delito o de una infracción del reglamento escolar). Algunos ejemplos de actividades ilegales que podrían requerir la intervención policial son:

- Abuso sexual infantil e imágenes (incluidas imágenes de un niño en brazos de otro niño)
- Material para adultos que potencialmente infrinja la Ley de Publicaciones Obscenas
- Material criminalmente racista
- Otra conducta, actividad o material delictivo
- Grabaciones de actividad delictiva como testigo (esto incluye abuso infantil, incluido el "upskirting")
- El uso de armas para herir a alguien

Si parece que los estudiantes han estado enviando mensajes de texto sexuales entre ellos o a alguien fuera de la escuela, el personal informará de inmediato al DSL, quien realizará una investigación exhaustiva. Esto podría resultar en sanciones internas o en la remisión del caso a la Policía o a los Servicios Infantiles si una o más de las partes corren riesgo de sufrir daños.

Nota: Sextear significa enviar mensajes sexualmente explícitos o imágenes sugerentes, como desnudos. Aunque su nombre indica que se realiza mediante mensajes de texto, este tipo de mensajes puede enviarse a través de cualquier servicio de mensajería, incluyendo correos electrónicos y redes sociales. Es ilegal que un menor de 18 años se tome una foto de sí mismo o de un amigo desnudo, así como que la distribuya.

5.0 Monitoreo

La Escuela cuenta con sistemas de filtrado y monitoreo adecuados que utilizan**PARED LISA**Para proteger a los estudiantes en internet (incluyendo correos electrónicos, mensajes de texto y redes sociales) cuando se conectan a la red de la escuela. El sistema se revisa trimestralmente para garantizar su correcto funcionamiento.

Sin embargo, los dispositivos con suscripción de datos móviles pueden proporcionar a los estudiantes acceso ilimitado y sin restricciones a internet. Dado que la Escuela no puede brindar la protección adecuada a los estudiantes en estos casos, no se les permite usar estos dispositivos para conectarse a internet, incluyendo el acceso al correo electrónico, mensajes de texto o redes sociales, mientras estén bajo la custodia de la Escuela.

En ciertas circunstancias, como para el seguimiento de una afección médica, se puede autorizar a un estudiante a usar su propio dispositivo móvil para conectarse a internet a través de la red de la escuela. Dicha autorización debe solicitarse y otorgarse con antelación.

- Las normas del Colegio sobre el uso de dispositivos electrónicos móviles se establecen en elUso aceptablePolítica
- El uso de dispositivos electrónicos móviles por parte del personal está regulado en el Código de Conducta del Personal. Salvo acuerdo escrito en contrario, los dispositivos móviles personales, incluyendo computadoras portátiles y notebooks, no deben utilizarse para fines escolares, salvo en caso de emergencia.
- Las políticas de la Escuela se aplican al uso de la Tecnología por parte del personal y los estudiantes, ya sea dentro o fuera de las instalaciones de la Escuela, y se tomarán las medidas apropiadas cuando dicho uso afecte el bienestar de otros estudiantes o cualquier miembro de la comunidad escolar o cuando la cultura o la reputación de la Escuela se ponga en riesgo.

6.0 Acoso cibernético y amenazas

El ciberbullying o acoso a través de Internet se define como la utilización y difusión de información, real o ficticia, con intención lesiva o difamatoria y en formato electrónico.

Dicha difusión puede realizarse a través de diferentes medios digitales como el correo electrónico, mensajería instantánea, foros, chats, redes sociales, mensajería de texto a través de dispositivos móviles o la publicación de videos o fotografías en plataformas electrónicas de difusión de contenidos.

Esta forma de acoso o intimidación puede manifestarse de diversas maneras. En este sentido, los estudiantes tienen el deber de:

- mantener un comportamiento y actitud de vigilancia y responsabilidad en la defensa y protección de sus datos personales y los de sus compañeros
- No participar en conductas de acoso cibernético y, en caso de verse afectado o tener conocimiento/hechos al respecto, deberá informarlo inmediatamente a los docentes.
- Denunciar y no consentir actos de violencia psicológica o moral hacia otros estudiantes en cualquier foro, desde el momento en que tengan conocimiento de ello.
- evitar en todo momento hacer bromas sobre conductas que puedan definirse como acoso y ciberacoso
- Evitar el bullying, las trampas, las burlas, los rechazos y cualquier tipo de discriminación, exclusión y/o acoso a otros estudiantes con comentarios ofensivos en cualquier foro.
- No enviar, mostrar ni compartir ninguna fotografía o imagen de otro compañero de clase con la intención de burlarse de sus amigos.
- No publicar comentarios, fotos o vídeos que puedan dañar la reputación, difamar o herir los sentimientos de otro estudiante.
- no utilizar mensajes ofensivos, amenazantes o intimidantes o que contengan lenguaje o vocabulario agresivo y grosero, y tampoco deben utilizar mensajes que, directa o indirectamente, sean insultantes o impliquen acoso, exclusión o manipulación
- No compartir chismes ni rumores falsos de naturaleza cruel o que tengan la intención de dañar la reputación de otro estudiante.
- No grabar contenido íntimo ni imágenes privadas comprometedoras de otro estudiante
- No reenviar ni circular información personal sobre otros estudiantes y/o sus familias a otros estudiantes o personas fuera de la escuela
- No responder a amenazas, insultos, mensajes intimidatorios ni provocaciones que se hagan en ningún foro. En esta situación, el estudiante siempre debe informar a sus padres y profesores.

Situaciones que se consideran**factores agravantes**:

- amenazar con hacer público un asunto
- Amenazar con revelar o compartir hechos sobre la vida privada o las relaciones de otro estudiante en casos en que la reputación o los intereses personales de la persona puedan verse afectados si se lleva a cabo la amenaza.
- coerción: una amenaza que busca, por medio de la violencia de cualquier tipo, impedir que un estudiante haga algo legal o conforme a las reglas escolares, u obligar a un estudiante a hacer algo que no quiere hacer
- chantaje: amenaza con una condición, algo que se exige a cambio de no cumplirlo

Es una calumnia afirmar que otro estudiante ha actuado fuera o en contra de la política mientras se sabe que nunca ha cometido ninguna ofensa contra la política.

La calumnia es cualquier acción o expresión –humillación, insulto u ofensa– de carácter grave que lesiona la dignidad de otro estudiante, menoscaba su reputación o supone una afrenta a su autoestima.

7.0 Infracciones contra la privacidad

La infracción o violación del derecho a la privacidad puede tener consecuencias legales: la ley prohíbe acceder, apoderarse, utilizar, modificar y alterar los datos personales y la privacidad de otro individuo en su detrimento.

El secreto de las comunicaciones es un derecho fundamental de las personas y su incumplimiento puede acarrear graves consecuencias. El correo electrónico, la mensajería instantánea, los chats, los SMS, las redes sociales, etc., son medios de comunicación y, si se realizan de forma privada, están protegidos por la ley.

En este sentido, la difusión, revelación o cesión a terceros de datos ajenos sin consentimiento, por ejemplo, con su publicación en Internet, puede tener repercusiones jurídicas, especialmente graves si se refieren a un afectado menor de edad.

En relación a la intimidad personal, el artículo 18.4 de la Constitución Española garantiza la protección de los datos personales, de forma que no puedan ser utilizados sin el consentimiento informado de su titular y para fines específicos.

Es sumamente importante que los estudiantes sean conscientes de hasta qué punto su comportamiento puede ser apropiado o no y, sobre todo, que sepan y valoren la importancia de respetar la privacidad de los demás y las posibles consecuencias de actuar de otra manera.

- Al grabar y/o publicar imágenes y fotografías que incluyan a otros estudiantes, es deber del estudiante hacerlo con el consentimiento y permiso de los demás estudiantes.
- Es deber del estudiante abstenerse de subir, publicar o enlazar cualquier documento o imagen – fotografías, vídeos, páginas web, archivos de audio, foros, grupos, chats, etc., que puedan ser causa y motivo de daño, descrédito o perjuicio presente o futuro a la privacidad de otro estudiante.
- Es deber del estudiante evitar leer el correo electrónico de otro estudiante sin permiso, así como ingresar a la computadora o sistema de otro estudiante sin permiso, lo cual constituye una invasión a la privacidad de otro estudiante.

8.0 Plan de estudios

Como parte del plan de estudios de TIC/Informática y PSHE, todos los estudiantes tomarán lecciones de concientización sobre seguridad electrónica.Esto se refuerza en todas las demás áreas del currículo, especialmente al trabajar con tecnología. Los mensajes clave de estas lecciones son:

- Los peligros de usar Internet/aplicaciones tanto en casa como en la escuela
- Qué hacer si se encuentran con textos o imágenes inapropiados u ofensivos

- Cómo mantenerse seguro al comunicarse en línea
- Cómo tomar las medidas adecuadas cuando las cosas van mal
- Cómo mantenerse seguro al usar sitios de redes sociales
- Cómo mantenerse seguro en salas de chat/foros de discusión
- Qué hacer si son víctimas de ciberacoso
- Los peligros y las leyes del sexting y compartir imágenes y vídeos inapropiados

9.0 Informes

El personal, los estudiantes y los padres deben informar a la Escuela sobre cualquier incidente de uso indebido o sospecha de uso indebido, de acuerdo con esta política y las políticas y procedimientos disciplinarios y de protección de la Escuela. Consulte también**Apéndice 2.**

Mal uso por parte de los estudiantes

- Cualquier persona que tenga alguna inquietud sobre el uso indebido de la tecnología por parte de los estudiantes debe informarlo al responsable del KS en primera instancia, para que se pueda abordar de acuerdo con las políticas de conducta y disciplina del colegio, incluyendo la Política Antiacoso en caso de denuncia de ciberacoso. Esto también aplica a cualquier uso indebido fuera del colegio.
- Cualquier persona que tenga alguna inquietud sobre el bienestar y la seguridad de un alumno debe informarlo inmediatamente de acuerdo con los procedimientos de protección infantil de la escuela (consulte la Política de protección infantil y salvaguardia de la escuela).

Mal uso por parte del personal

- Cualquier persona que tenga alguna inquietud sobre el uso indebido de la tecnología por parte del personal debe informarlo de acuerdo con la Política de denuncia de irregularidades de la escuela directamente al director de la escuela, para que pueda tratarse de acuerdo con los procedimientos disciplinarios del personal.
- Si alguien tiene una inquietud relacionada con la protección, debe informarla inmediatamente al DSL para que pueda tratarse de acuerdo con los procedimientos para informar y tratar denuncias de abuso contra el personal establecidos en la Política de protección infantil y protección de la escuela.

Mal uso por parte de cualquier usuario

- Cualquier persona que tenga inquietudes sobre el mal uso de la Tecnología por parte de cualquier otro usuario debe informarlo inmediatamente al Jefe de Sección o al Director.
- La Escuela se reserva el derecho de retirar el acceso a la red de la Escuela a cualquier usuario en cualquier momento y de denunciar cualquier actividad ilegal sospechosa a la policía.

10.0 Respuesta al mal uso o abuso en línea

En caso de cualquier mal uso o abuso en línea, se seguirán los pasos descritos en la política de conducta de la escuela o en la política contra el acoso escolar, según corresponda.

Todos los casos de mal uso y abuso en línea se toman en serio para proteger al niño.

Las siguientes políticas, procedimientos y materiales de recursos también son relevantes para las prácticas de seguridad en línea de la Escuela:

- Política contra el acoso escolar
- Acuerdo de política de uso aceptable
- Política de salvaguardia y protección infantil
- Política sobre teléfonos móviles y cámaras

11.0 Interpretación

Cualquier consulta respecto a la aplicación de esta política deberá dirigirse al Director de Operaciones a:
33 Cavendish Square,
Londres,
W1G 0PW

12.0 Rastreador de políticas

Fecha de creación	Autor	Fecha de vencimiento de la revisión
Febrero de 2025	Subdirector: Seguridad y Bienestar	Febrero de 2026

Apéndice 1

LAUDE
SAN PEDRO
INTERNATIONAL COLLEGE

POLÍTICA DE USO ACEPTABLE - ACUERDO DEL PERSONAL

Esta política cubre el uso de tecnologías digitales en la escuela/emitidas para uso escolar: es decir, correo electrónico, Internet, intranet y recursos de red, plataforma de aprendizaje, software, equipos y sistemas.

Nombre:	
Cuenta de correo electrónico emitida por la escuela:	

Firme a continuación donde se indica para confirmar que ha leído y comprendido este documento.

1. Solo utilizaré los sistemas y recursos de tecnología digital de la escuela para fines profesionales o para usos que el director y el ISP consideren "razonables".
2. No revelaré mis contraseñas a nadie.
3. No permitiré que personas no autorizadas accedan al correo electrónico/Internet/intranet/red.
4. No participaré en ninguna actividad en línea que pueda comprometer mis responsabilidades profesionales.
5. Solo utilizaré los sistemas de correo electrónico seguros y aprobados para cualquier asunto escolar.
6. Solo utilizaré los sistemas de comunicación escolares aprobados con alumnos o padres/tutores, y solo me comunicaré con ellos para asuntos escolares apropiados.
7. No navegaré, descargaré ni enviaré material que pueda considerarse ofensivo o ilegal.
8. Informaré de cualquier acceso accidental o recepción de materiales inapropiados o de cualquier violación del filtrado.
9. No descargaré ningún software ni recurso de Internet que pueda comprometer la red o que no tenga la licencia adecuada.
10. No conectaré una computadora personal u otro dispositivo a la red / Internet a menos que el Director me autorice a hacerlo.
11. No utilizaré cámaras digitales ni teléfonos personales para tomar y transferir imágenes de alumnos o personal en el trabajo y no almacenaré imágenes en dispositivos personales.
12. Utilizaré la Plataforma de Aprendizaje de la escuela de acuerdo con la política escolar.
13. Me aseguraré de que cualquier sitio de redes sociales privado / blogs / vlogs / podcasts / publicaciones escritas, etc. que cree o en las que contribuya activamente no se confundan con mi rol profesional, y buscaré permiso del director de la escuela si tengo la intención de contribuir a cualquiera de dichas áreas.
14. Estoy de acuerdo y acepto que cualquier teléfono, computadora o portátil u otro dispositivo electrónico que me preste la escuela, se proporciona únicamente para apoyar mi profesión y puede ser auditado sin notificación, incluido el historial de búsqueda y los archivos.

15. Me aseguraré de que cualquier información confidencial que desee transportar de una ubicación a otra esté protegida mediante encriptación y de que seguiré los protocolos de seguridad de datos de la escuela cuando utilice dichos datos en cualquier ubicación.

16. Entiendo que la política de protección de datos de la escuela requiere que cualquier información que vea sobre el personal o los alumnos, almacenada dentro del sistema de gestión de información de la escuela, se mantendrá privada y confidencial, EXCEPTO cuando se considere necesario que la ley me exija revelar dicha información a una autoridad competente.

17. Entiendo que todo uso de Internet y de la red puede registrarse y que esta información puede ponerse a disposición de mi gerente si lo solicita.

18. Entiendo que la Escuela tiene la propiedad de todos los derechos de propiedad intelectual cuando creo un trabajo original durante el curso del empleo (ya sea durante las horas de trabajo o utilizando las instalaciones o recursos de la Escuela, y ya sea que esté grabado o no en forma material).

19. Cuando finalice mi contrato, acepto la transferencia de todos los archivos en las cuentas proporcionadas por la escuela, así como también cualquier copia impresa.

20. Entiendo que el incumplimiento de este acuerdo podría dar lugar a medidas disciplinarias.

21. Entiendo que es mi responsabilidad asegurarme de mantenerme actualizado y leer y comprender la Política de uso aceptable de la escuela.

22. Acepto cumplir todos los puntos anteriores.

Firma:

Nombre impreso:

Fecha:

Apéndice 2

Qué hacer si ocurre un incidente de acoso cibernético:

Si ocurre un incidente de acoso dirigido a un niño mediante el correo electrónico o la tecnología de las redes sociales, ya sea dentro o fuera del horario escolar, los maestros deben:

1. Aconseje al niño que no responda al mensaje.
2. Referir a través de Mi Preocupación como una preocupación de protección
3. Investigar, documentar y asegurar toda la evidencia de acuerdo con las políticas
4. Notificar a los padres de los niños involucrados.
5. Considere informar a la policía dependiendo de la gravedad o la naturaleza reiterada del delito.
6. Informar al responsable de protección escolar
7. Aplicar sanciones adecuadas

Si se publican comentarios maliciosos o amenazantes en un sitio de Internet sobre un alumno o miembro del personal.

1. Informar a los administradores del sitio y/o ISP y solicitar que se eliminen los comentarios si el sitio es administrado externamente
2. Asegure y preserve cualquier evidencia
3. Esforzarse por rastrear el origen e informar a la policía según corresponda.
4. Informe sobre mi preocupación como preocupación de protección

Los niños y el personal deben tener confianza en una cultura de no culpar a nadie cuando se trata de denunciar incidentes inapropiados relacionados con Internet o la tecnología móvil: deben poder hacerlo sin miedo, incluso si inicialmente han respondido al abuso.mi.