



Caja de Recursos para Padres de Familia sobre la Privacidad del Estudiante



PARENT COALITION FOR
STUDENT PRIVACY



Campaign for a Commercial-Free Childhood

SEPTIEMBRE 2017

INDICE DE CONTENIDOS

INTRODUCCIÓN	1
SECCIÓN I: ¿Qué son los datos del estudiante?	3
SECCIÓN II: Los derechos que tienen los padres para proteger la privacidad de sus hijos ante la ley federal .	7
SECCIÓN III: Consejos para padres que quieren proteger la privacidad de su estudiante	15
SECCIÓN IV: Buenas prácticas de protección de la privacidad de los estudiantes para maestros, escuelas, distritos y estados	21
SECCIÓN V: Hablando con los maestros, las escuelas y los distritos sobre la privacidad del estudiante	25
SECCIÓN VI: Abogando por la privacidad del estudiante en las escuelas, los distritos y más allá	27
SECCIÓN VII: Preguntas frecuentes sobre la privacidad del estudiante	31
ANEXO A: Solicitud para inspeccionar los archivos educativos que están en posesión de la escuela, el distrito o el estado	
ANEXO B: Modelo de carta para optar por negarse a revelar información de la "información de directorio"	
ANEXO C: Modelo de carta para optar por no ser reclutado por el ejército	
ANEXO D: Preguntas adicionales para hacer al maestro o al director	
ANEXO E: Modelo de petición	
ANEXO F: Consejos para llegar a los medios de comunicación y ejemplos de materiales dirigidos a la prensa	

RECURSOS ADICIONALES

INTRODUCCIÓN

¿Por qué se deben preocupar los padres de familia?

Para los padres de familia es difícil imaginar la gran cantidad de información que se recopila actualmente en las escuelas acerca de los estudiantes, y cómo dicha información se usa, se almacena y se comparte con otros. Durante el transcurso de un día normal en la escuela –y a lo largo de la vida del niño, desde pre-escolar hasta la graduación de la escuela preparatoria (high school)– una gran cantidad de información, incluyendo información muy sensible, se comparte sin el conocimiento o consentimiento de los padres, con los vendedores que proporcionan servicios operacionales o compañías que ofrecen programas educativos. A menudo, en lugar de que la información se asegure en la escuela en un archivo bajo llave, o que se almacene en los servidores de las computadoras de la escuela, la información personal de los estudiantes se almacena y se transmite hacia la “Nube” para facilitar su acceso y para ser usada por terceros. Las leyes federales, destinadas a proteger los datos de los estudiantes contenidos en las escuelas, son simplemente inadecuadas para abordar los retos de la actual era digital.

Puede ser que los padres nunca sepan por completo cómo es que la información personal de sus hijos pudo haber sido compartida, usada, mal utilizada, vendida, “pirateada” o intervenida cibernéticamente en el transcurso de su paso por las escuelas. Si a sus hijos se les niega la entrada al colegio que eligieron, los padres pueden preguntarse ¿si los perfiles de los estudiantes fueron vendidos a las universidades por el Consejo Directivo de Colegios y ACT (College Board and ACT) y que luego hayan sido usados como base para rechazar su aplicación? Si a sus hijos se les rechaza de los trabajos ideales para ellos, uno se pregunta ¿si el empleador los examinó usando un perfil en línea de su historia de búsquedas en Internet, que fue recopilado por el dispositivo otorgado por la escuela y comprado por los agentes/vendedores de datos? Si las identidades de sus hijos son robadas, ¿fue eso el resultado de una violación cibernética a los datos de la escuela primaria sucedida muchos años atrás?

Si a sus hijos se les negara algún servicio estatal cuando sean adultos, ¿podría ser a causa de alguna información disciplinaria o incriminatoria, incluida en sus archivos acumulados que están en posesión del departamento de educación estatal u otras agencias?

Esta caja de recursos está diseñada para ayudar a padres de familia como usted, en la navegación de dichas cuestiones, y proporcionar información sobre sus derechos y los pasos que puede seguir para maximizar la privacidad y seguridad de sus hijos. Todo padre o madre entiende intuitivamente que su objetivo es proteger a sus hijos y tratar de asegurar el éxito en su escuela y en su vida. Esperamos entonces, que esta caja de recursos le ayude en lograr dicho objetivo.

Reconocimientos

Este esfuerzo es un proyecto en conjunto de la Coalición de Padres para la Privacidad del Estudiante (Parent Coalition for Student Privacy) y la Campaña por una Infancia Sin Comerciales (Campaign for a Commercial-Free Childhood) y fue posible gracias a una subvención financiera del Fondo para los Derechos de Privacidad de los Consumidores de la Fundación Rose por las Comunidades y el Ambiente (Rose Foundation for Communities and the Environmental's Consumer Privacy Rights Fund).

Los autores de esta Caja de Recursos para la Privacidad del Estudiante son Rachael Stickland, Melissa Campbell, Josh Golin, Leonie Haimson, y David Monahan. Traducción realizada por Alma R. Galván. Un agradecimiento especial a los miembros del Consejo Kris Alman, Oregon Education Advocate; Faith Boninger, Centro de Política Educativa Nacional (National Education Policy Center), Universidad de Colorado en Boulder (University of Colorado Boulder); Laura Bowman, Padres a Través de América (Parents Across America); Phyllis Bush, Co-fundador de Amigos de la Educación Pública del Noreste de Indiana (Northeast Indiana Friends of Public Education), y miembro del Consejo Red para la Educación Pública (Network for Public Education); Tim Farley, Alianza para

la Educación Pública del Estado de Nueva York (*New York State Alliance for Public Education*); Jennifer Jacobson, Alianza por la Privacidad en la Educación de Connecticut (*Connecticut Alliance for Privacy in Education*)*; Cheri Kiesecker, Coalición de Padres para la Privacidad del Estudiante (*Parent Coalition for Student Privacy*); Chad Marlow, Unión Americana para las Libertades Civiles (*American Civil Liberties Union*)*; Abg. Francesca Miceli; Mark B. Miller, Director de la Escuela Centennial, Distrito Escolar de Pensilvania (*Centennial, Pennsylvania School District*), y miembro del Consejo, Red para la Educación Pública (*Network for Public Education*); y Abg. Sarah Petrie.

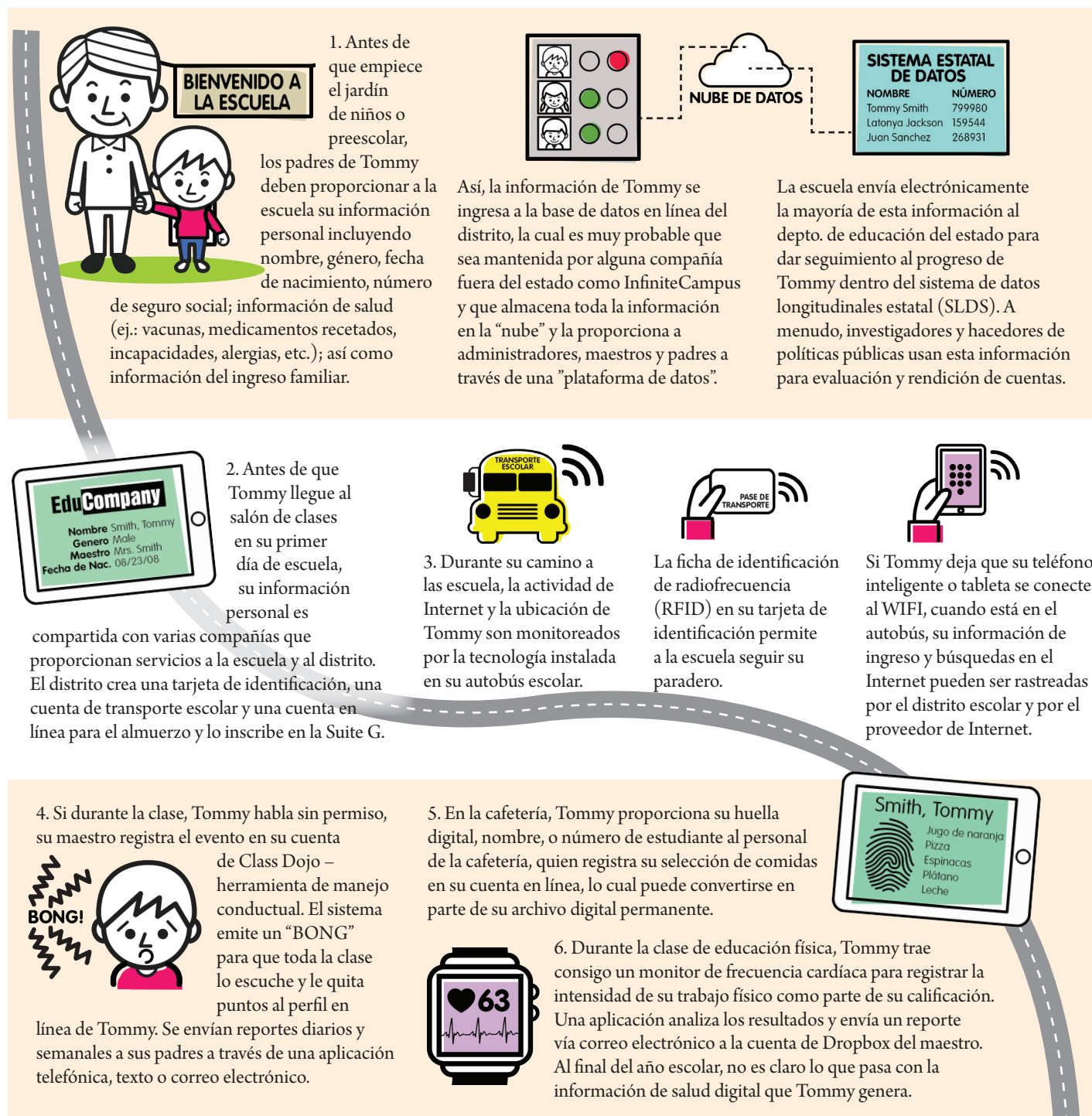
**Afiliación, únicamente con propósitos de identificación*

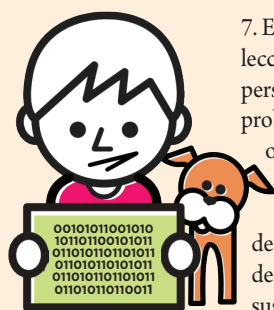
¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

SECCIÓN I.

¿Qué son los datos del estudiante?

Para entender completamente los tipos y la cantidad de información personal que un estudiante genera en el mundo digital de la actualidad, y como ésta información se usa y se comparte, vamos a examinar la vida de un niño ficticio al que llamaremos Tommy.





7. En casa y en la escuela Tommy recibe lecciones en línea de “aprendizaje personalizado”. Si está resolviendo problemas matemáticos en un video juego o haciendo pruebas después de leer historias, las compañías de tecnología lucrativas –no sus maestros– determinan contenido y nivel de dificultad de la actividad, recogiendo datos y usando sus propios algoritmos para analizar las habilidades de Tommy, perfilar sus intereses y predecir resultados. Este proceso es conocido como “extracción de datos”.



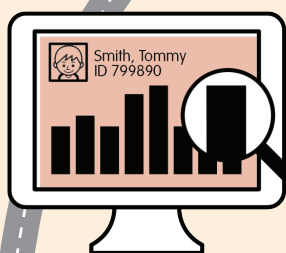
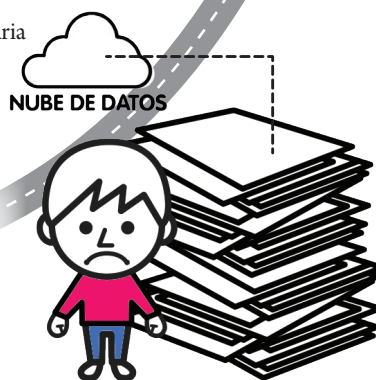
8. Desde el jardín de niños o Preescolar, a Tommy le asignan evaluaciones intermedias (pruebas de preparación) como requisito estatal y del distrito. Desde 3° hasta 8° grado Tommy hace exámenes anuales estandarizados en matemáticas y

Lenguaje en Inglés (ELA) de acuerdo a la ley federal y también puede estar sujeto a realizar evaluaciones estandarizadas locales y periódicas en esos y otros temas más. Las compañías que administran esas pruebas a menudo recogen información estudiantil personal y sensible, y otros datos como el tiempo que tardan en responder una pregunta específica. A menudo los ensayos son calificados por máquinas y no por personas.

9. En ocasiones en la escuela primaria, le pedirán a Tommy que complete encuestas sobre el “clima escolar” y sus creencias personales, sus puntos de vista políticos, o habilidades emocionales y sociales, usando a menudo, una cuenta en línea que contiene su nombre y otra información personal.



10. Conforme Tommy avanza en la escuela primaria (elementary school) y en sus años de escuela secundaria (middle school), su archivo educativo crece incluyendo calificaciones, horarios de cursos, resultados de pruebas estandarizadas, disciplina, archivos de consejería, discapacidades y Planes de Educación Individualizada (504), y cualquier condición de salud que tenga y que requiere medicamentos o tratamiento especial en la escuela. El archivo puede incluir su información de historia familiar, antecedentes étnicos y raciales, país donde nació, estado migratorio o si no tiene casa, y servicios especiales que recibe.



11. Cuando Tommy llega a 6to. grado o antes, su distrito puede implementar programas 1:1, donde el distrito entrega al alumno dispositivos con una configuración predeterminada que permite a compañías como Google seguir y extraer información del estudiante, incluyendo sitios de Internet que visita, términos usados en búsquedas, videos, libros y artículos en línea que vea y sus claves. Tommy usa ese equipo hasta que se gradúa, acumulando millones de puntos de información que al ser extraídos pueden diagnosticar sus problemas de aprendizaje, dirigirlo hacia ciertos cursos o carreras, o generar perfiles de consumo que puedan venderse.



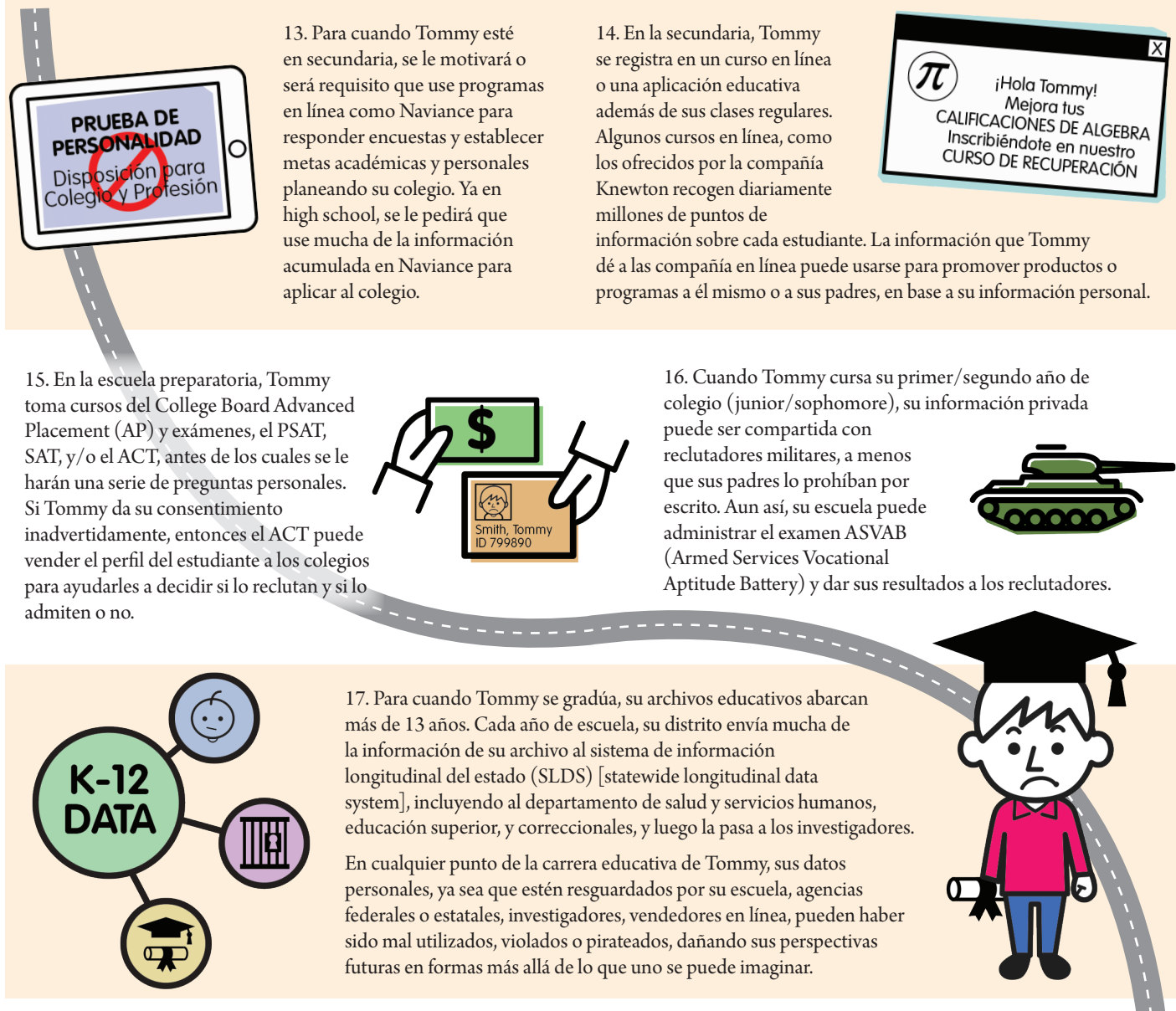
GOBIERNO DE EE. UU.

12. Sin conocimiento o consentimiento de sus padres, el distrito escolar de Tommy puede compartir nombre, calificaciones, registro de asistencia, de disciplina, y resultados de pruebas estandarizadas y discapacidades con investigadores privados, incluso con el Depto. de Educación de EE.UU. Los resultados de los estudios nunca se darán a Tommy o a su familia.

¿CUÁL ES LA REALIDAD DE LOS PRODUCTOS DE “APRENDIZAJE PERSONALIZADO”? Según Data and Society Research Institute, 2016: “la mayoría de los productos de los sitios de Internet describen que la participación de maestros o científicos del aprendizaje dentro del desarrollo de los mismos es mínima y después del hecho (Guernsey y Levine, 2015). Estos no se prueban en campo antes de adoptarse en las escuelas y mas allá de testimonios y anécdotas solo ofrecen investigación limitada o nula sobre la eficacia de los sistemas de aprendizaje personalizado”.¹

¿CÓMO SE SIENTEN LOS PADRES SOBRE LA PRIVACIDAD DEL ESTUDIANTE? Un estudio de Future of Privacy Forum en 2015 encontró que el 87% de los padres encuestados “están preocupados por la posibilidad de que los datos estudiantiles sean pirateados o robados”. Y que el 68% de los padres encuestados están preocupados por “que un archivo electrónico pueda usarse en el futuro contra su hijo, por parte de un colegio o empleador”.²

¿QUÉ SUCEDE CON LOS DATOS CAPTURADOS EN LÍNEA? Cuando los estudiantes navegan en Internet –en casa o escuela– las compañías recogen su información, la empaquetan como perfiles del consumidor, y luego se vende en el mercado sombrío de datos. Como esta información tiene el potencial de predecir conductas, motivaciones y sentimientos, puede ser comprada por colegios, empleadores, prestamistas y aseguradoras para evaluar la adecuación de sus servicios y productos al individuo.



¿LA INFORMACIÓN DEL ESTUDIANTE ALMACENADA EN SISTEMAS ESTATALES O EN EL SLDS HA SIDO MAL UTILIZADA? En marzo del 2016, un juez ordenó que los archivos de 10 millones de estudiantes de California, que incluían "nombres, direcciones, archivos disciplinarios, calificaciones, resultados de pruebas, y hasta detalles tales como embarazos, adicciones e historia criminal", estuvieran disponibles para una organización privada, la cual demandó al Estado para poder tener acceso a la base de datos de los estudiantes.³

¿LA INFORMACIÓN DEL ESTUDIANTE HA SIDO VIOLADA POR LAS ESCUELAS? En febrero del 2016 las Escuelas Públicas de Washington D.C., difundieron públicamente en línea la información privada de aproximadamente 12,000 estudiantes de escuelas públicas, que contenía información sobre necesidades especiales, incluyendo "cada número de identificación del estudiante, raza, edad, escuela, discapacidades y cualquier servicio que él o ella recibía".⁴

¿LAS COMPAÑÍAS QUE OFRECEN PRODUCTOS DE "APRENDIZAJE" EN LÍNEA PUEDEN SER PIRATEADAS? A finales del 2015, VTech, una "compañía de juguetes educativos electrónicos ganadora de reconocimientos", tuvo 4.9 millones de cuentas de padres y 6.4 millones de perfiles de niños violados por un hacker. La información de los padres incluía "nombre, dirección postal, dirección electrónica, dirección IP, historia de descargas y credenciales de las cuentas". Los perfiles de los niños incluían nombre, género y fecha de nacimiento".⁵

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. https://datasociety.net/pubs/ecl/PersonalizedLearning_primer_2016.pdf
2. https://fpf.org/wp-content/uploads/2015/11/Beyond-the-Fear-Factor_Sept2015.pdf
3. http://www.mercurynews.com/bay-area-news/ci_29590794/judge-pulls-back-from-calif-student-records-release
4. https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-%20ea152f0b9561_story.html
5. <https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/>

SECCIÓN II.

Los derechos que tienen los padres para proteger la privacidad de sus hijos ante la ley federal

Puede ser un reto conocer sus derechos bajo el complicado mosaico de leyes federales, estatutos estatales y políticas públicas locales que gobiernan el uso y la revelación de la información personal del estudiante. En esta sección se describen brevemente las leyes federales conocidas como **FERPA** (Ley de Privacidad y Derechos Educativos Familiares) [Family Educational Rights and Privacy Act], **NSLA** (Ley Nacional de Almuerzo Escolar) [National School Lunch Act], **IDEA** (Ley sobre Individuos con Discapacidades Educativas) [Individuals with Disabilities Education Act], **PPRA** (Enmienda de Protección de los Derechos del Alumno) [Protection of Pupil Rights Amendment] y **COPPA** (Ley de Protección de la Privacidad en Línea de los Niños) [Children's Online Privacy Protection Act].

Actualmente, las Leyes Federales proporcionan una línea de referencia para la protección de la privacidad del estudiante. En años recientes, los miembros del Congreso han presentado muchas propuestas de ley en un intento por fortalecer las medidas de protección de privacidad del estudiante, pero hasta enero 2017 ninguna ha sido aprobada.

Recientemente varios estados han aprobado leyes que mejoran la privacidad del estudiante. Usted debe familiarizarse con las leyes de su estado en relación a la privacidad del estudiante y monitorearlas muy de cerca por los cambios que puedan ocurrir. Para conocer las novedades sobre estas propuestas de ley, federales y las nuevas leyes estatales de privacidad del estudiante, visite www.parentcoalitionforstudentprivacy.org y suscríbese a nuestro boletín informativo.

Los distritos escolares locales y los departamentos estatales de educación pueden y deben hacer su parte, desarrollando políticas de privacidad del estudiante y procedimientos que puedan alcanzar más allá de las protecciones ofrecidas en la ley federal o estatal. Le ofrecemos sugerencias al respecto en la Sección IV.



Ley de Privacidad y Derechos y Educativos Familiares [FERPA (Family Education Rights and Privacy Act)]

La **Ley Acta de Privacidad y Derechos Educativos Familiares** (Family Educational Rights and Privacy Act-FERPA- [20 U.S.C. § 1232g; 34 CFR Part 99]) aprobada en 1974, es administrada por el Departamento de Educación de EE. UU. y se aplica a las escuelas y universidades financiadas federalmente. Esta ley prohíbe la divulgación de información personal identificable (PII) en los archivos educativos del estudiante -como calificaciones, resultados de pruebas, registros de disciplina, contacto e información familiar y horarios de clases- a terceras personas sin el consentimiento paterno, pero con algunas excepciones que se describen más abajo. La ley se escribió antes de que surgieran los sistemas de datos computarizados y los programas de aprendizaje que recopilan información y ha sido debilitada considerablemente en los últimos diez años a través de cambios regulatorios. Ambos factores permiten que la PII del estudiante sea compartida fácilmente con otras personas fuera de la escuela.

FERPA contiene múltiples “excepciones” o ciertas circunstancias bajo las cuales la PII del estudiante puede ser divulgada sin el consentimiento de los padres, a personas o grupos externos a

La definición de “Información personal identificable (PII)” del Departamento de Educación de EE.UU. incluye, pero no se limita a: nombre del estudiante; nombre de familiares o padres del estudiante; dirección física; datos de identificación personal como núm. de seguro social o núm. de identificación del estudiante, o archivos biométricos; otros identificadores indirectos como fecha y lugar de nacimiento, apellido de la madre; u otra información, que por sí misma o en combinación con otra, pueda enlazarse o vincularse a un estudiante, permitiendo que terceras personas le identifiquen.

la escuela o distrito. La que se usa más ampliamente es la excepción “oficial escolar” (school official) que permite que la PII del estudiante sea compartida con vendedores, consultores, contratistas y voluntarios que tengan “intereses educativos legítimos” y que están realizando “servicios o funciones institucionales” para la escuela. Los ejemplos más comunes incluyen los proveedores de instrucción y evaluación en línea, compañías de servicios de cafetería o de transporte, vendedores que proporcionan sistemas de información del estudiante y padres u otros voluntarios del salón de clases. La excepción “auditoría y evaluación” también permite la divulgación sin el consentimiento de los padres a “representantes autorizados” de “autoridades educativas locales, federales y estatales conduciendo una auditoría, evaluación o aplicación de programas educativos”. Esta excepción permite el desarrollo de sistemas de datos longitudinales a lo largo del estado (SLDS) donde los datos del estudiante pueden ser compartidos entre varias agencias estatales, incluyendo servicios humanos y de salud, correccionales, seguridad pública y mano de obra y trabajo. Una tercera excepción que es amplia en sí, permite la divulgación no consensual de la PII del estudiante a organizaciones o individuos para propósitos o “estudios”. Estos estudios deben estar limitados a tener el objetivo de “desarrollar, validar o administrar pruebas predictivas; administración de programas de ayuda para el estudiante; de investigación o mejoramiento de la instrucción”. Para más información sobre FERPA visite <https://ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

¿Qué derechos tienen los padres ante FERPA?

1. LOS PADRES TIENEN EL DERECHO de acceso a la información de los archivos educativos de su hijo que tiene el departamento educativo del estado, del distrito local y/o la escuela. El estado, distrito y la escuela no pueden cobrar cuotas a los padres por buscar o por recuperar los archivos educativos, pero sí pueden aplicar una cuota razonable por proporcionar copias de dichos archivos, y deberán proporcionarlos en un formato legible, dentro de los siguientes 45 días en que se reciba la solicitud de los padres. Note que algunos de estos estados tienen leyes que requieren la producción de documentos dentro de un período de tiempo más corto. Los padres necesitan llenar una forma específica para acceder a los archivos educativos, y la pueden encontrar en el sitio de Internet del estado, distrito o escuela o quizás necesiten llamar a la oficina administrativa de la escuela, el distrito o el estado para más información. Si dicha forma no se les proporciona, vea el Anexo A que incluye un ejemplo.

2. LOS PADRES PUEDEN SOLICITAR que se corrija la información en los archivos de su hijo, si piensan que es “inexacta, incorrecta o que está violando los derechos de privacidad del estudiante”.¹⁷ Si la escuela, el distrito o el estado se rehúsan a corregir el archivo, los padres tienen derecho a una audiencia formal. Si después de la audiencia, la escuela, el distrito o el estado se rehúsan aún a corregir el archivo, los padres tienen el derecho de corregir o modificar el archivo colocando en él un comunicado exponiendo su punto de vista en relación a la información impugnada.

3. LOS PADRES TIENEN EL DERECHO a ser informados sobre el criterio que tiene la escuela o distrito para determinar quien constituye un “oficial escolar”, u otra tercera persona con un “interés educativo legítimo”, a quien la escuela o el distrito escolar pueda revelar la PII sin el consentimiento o notificación de los padres.

4. LOS PADRES TIENEN EL DERECHO de optar porque la información de su hijo no esté dentro de la “información de directorio”, donde el distrito o la escuela ofrece dicha información a terceras personas. La información de directorio generalmente incluye un

Las escuelas a menudo designan a compañías que albergan aplicaciones de salón de clase o programas en línea como “oficiales escolares”.

De acuerdo al Departamento de Educación de EE.UU. los “archivos educativos” son aquellos registros que se relacionan directamente a un estudiante y que son mantenidos por la escuela o una persona actuando por parte de la escuela.

Los archivos educativos “incluyen, pero no se limitan a calificaciones, expedientes, listas de clases, horarios de cursos, registros de salud (desde nivel K-12), información financiera (a nivel post-secundario), y registros de disciplina del estudiante. La información puede ser registrada de cualquier forma, incluyendo, pero no se limita a, letra manuscrita, impresión, medios computacionales, videos, audios, fotografías, microfilmes, microfichas y correo electrónico”.

Los archivos educativos también incluyen un registro de cualquier información personal del estudiante solicitada por o divulgada a:

- 1. Organizaciones que realizan “estudios” para o a nombre de la escuela;*
- 2. Autoridades educativas locales, estatales o federales; y*
- 3. Terceras personas sin autorización, incluyendo cualquier instancia de pirateo o violación de seguridad.*

conjunto más limitado de información personal, que no es considerada altamente sensible o delicada. Note que optar por no estar dentro de la "información de directorio" no impide a las escuelas o distritos que proporcionen datos estudiantiles personales, a menudo de una naturaleza aún más sensible, a "oficiales escolares", "representantes autorizados" u "organizaciones" bajo las excepciones mencionadas anteriormente. Para más información sobre como optar por no ser parte de la información de directorio vea el Anexo B.

5. LOS PADRES TIENEN EL DERECHO de optar porque la información de su hijo contenida en la "información de contacto" no se proporcione a los reclutadores militares. Para ello, los padres deben someter a la escuela una solicitud por escrito. Un modelo de un formulario se encuentra en el Anexo C.

6. LOS DISTRITOS ESCOLARES DEBEN INFORMAR A LOS PADRES anualmente sobre sus derechos bajo FERPA. La forma real de notificación se deja a discreción de cada escuela (ej.: correo electrónico, carta, boletín de PTA, cuadernos del estudiante o sitio de Internet).

7. LA INFORMACIÓN PERSONAL DEL ESTUDIANTE NO PUEDE SER COMPARTIDA INDISCRIMINADAMENTE aún dentro de la misma escuela. En su lugar, la divulgación se debe limitar a aquellos maestros y otros empleados escolares que son directamente responsables de la educación o servicios del estudiante, los cuales "necesitan conocer" la información de los estudiantes para poder cumplir con sus responsabilidades profesionales.

NOTA: Los derechos de los padres bajo FERPA se transfieren al estudiante que cumple 18 años de edad o que asiste a una institución escolar post secundaria (ej.: Universidad o colegio), o que se convierte en un menor emancipado ante la ley.

Si usted piensa que los derechos de su hijo bajo FERPA han sido violados, usted debe notificar a su escuela, Superintendente de distrito, y/o al consejo escolar. Si ellos se rehúsan a tomar una acción apropiada, usted puede contactar al capítulo local de la ACLU (American Civil Liberties Union) para buscar ayuda o para someter una denuncia al U.S. Department of Education's Family Policy Compliance Office. Las denuncias que se someten a FERPA deben hacerse por escrito y contener los detalles específicos dando una causa razonable por la que se cree que ha ocurrido la violación de la privacidad; deberá ser sometida por el padre/madre del estudiante de una escuela primaria o secundaria, menor de 18 años o de un estudiante elegible y deberá ser sometida dentro de los 180 días posteriores a la fecha en que ocurrió la violación que se alega o dentro de los 180 días posteriores a que el denunciante supo o debió haber sabido sobre la violación. Para mayor información o para saber más sobre cómo someter una queja o denuncia, visite <https://studentprivacy.ed.gov/file-a-complaint>.

La "Información de Directorio" incluye, pero no se limita al nombre del estudiante, dirección, teléfono, correo electrónico, fotografía, fecha y lugar de nacimiento, principal área de estudio, nivel de escolaridad, estado de inscripción, fecha de graduación, participación en actividades y deportes, peso y talla, grados, honores y premios recibidos, y la escuela a la que asiste más recientemente.

La Información de Directorio no incluye el núm. de seguro social, o el núm. de identificación del estudiante, si ese núm. por sí mismo es suficiente para identificarle.



IDEA (Ley sobre Individuos con Discapacidades Educativas) [Individuals with Disabilities Education Act]

La Ley sobre Individuos con Discapacidades Educativas (IDEA) [The Individuals with Disabilities Education Act] (Ley Pública No. 94-142) está diseñada para proteger los derechos de los niños con discapacidades, incluyendo estudiantes con Programas de Educación Individualizada (IEPs) [Individualized Education Programs], para que se les proporcione educación gratuita y apropiada. La ley es administrada por el Departamento

Para aprender más sobre algunos de los derechos de privacidad adicionales de los niños con discapacidades, vea http://bit.ly/SPTK_IDEA_FERPA.

de Educación de EE.UU. Los niños con discapacidades tienen derechos de privacidad adicionales ante IDEA. Por ejemplo:

1. SE REQUIERE EL CONSENTIMIENTO DE LOS PADRES antes de que la PII de un niño con discapacidad se pueda proporcionar a oficiales de agencias que participan en la proporción o en el pago de servicios de transición secundarios, los cuales están designados para facilitar la transición del estudiante de la escuela a las actividades post-escolares.

2. SE DEBE OBTENER EL CONSENTIMIENTO DE LOS PADRES antes de que la PII del niño se proporcione al distrito en el que se localiza la escuela privada, en un distrito diferente del que viven los padres, donde se inscriba un niño con discapacidades de una escuela pública.

3. LOS PADRES DEBERÁN OTORGAR EL CONSENTIMIENTO POR ESCRITO cada año, antes de que el distrito revele los archivos de servicios de educación especial del niño a la agencia estatal de Medicaid, para que sea reclamado el reembolso del gobierno federal. Los padres podrán retirar su consentimiento en cualquier momento y el distrito deberá proporcionar al niño los servicios obligatorios, sin importar que el consentimiento sea o no otorgado.

NOTA: Para mayor información, contacte al distrito escolar, al director de educación especial local o al director de educación especial del estado o visite el sitio de Internet de IDEA en http://bit.ly/SPTK_IDEA.

Si usted cree que los derechos de privacidad de usted o de su hijo bajo IDEA han sido violados, debe notificar a su escuela, Superintendente de distrito, y/o al consejo escolar. Si ellos se rehúsan a tomar una acción apropiada, usted puede contactar al departamento de educación del estado. Usted también puede contactar al capítulo local de la ACLU (American Civil Liberties Union) para pedir ayuda o someter una denuncia ante el U.S. Department of Education's Family Policy Compliance Office. Para mayor información o para saber más sobre cómo someter una denuncia o queja, visite <https://studentprivacy.ed.gov/file-a-complaint>.



NSLA (Ley Nacional de Almuerzo Escolar) [National School Lunch Act]

La Ley Nacional de Almuerzo Escolar de 1964 [The National School Lunch Act (NSLA) of 1946 (79 P.L. 396, 60 Stat. 230)] es administrada por el Departamento de Agricultura de los EE. UU. [U.S. Department of Agriculture (USDA)] y aplica para todas las escuelas que reciben fondos educativos federales y protege la información de elegibilidad confidencial que es recogida por las escuelas para determinar si el niño puede o no recibir almuerzo gratuito o a un precio reducido [reduced-priced lunch (FRL)] o leche gratuita bajo el Programa Nacional de Almuerzo Escolar (National School Lunch Program). Para mayor información sobre NSLA, visite <https://www.fns.usda.gov/nslp/national-school-lunch-program-nslp>.

La "información de elegibilidad" incluye generalmente, pero no se limita a la información personal sobre el número de personas en la casa, el ingreso familiar; versus "estatus de elegibilidad" el cual designa si el niño es elegible o no para FRL.

¿Qué derechos tienen los padres bajo NSLA?

1. LOS PADRES DEBEN PROPORCIONAR consentimiento previo, antes de que se proporcione la información de elegibilidad de FRL a: 1) programas de educación y de salud

locales; y 2) programas de salud federales y estatales que no sean Medicaid o el Programa Estatal de Seguro de Salud de los Niños [State Children's Health Insurance Program (SCHIP)]. Se deberá proporcionar a los padres una notificación previa y la opción de rechazar que se proporcione la información de elegibilidad al Medicaid o SCHIP.

2. LA INFORMACIÓN DE ELEGIBILIDAD DEL ESTUDIANTE no podrá estar disponible para todos los empleados de la escuela, en su lugar, la disponibilidad de la información deberá limitarse a los maestros, tutores u otros oficiales escolares, directamente responsables de la educación y cuidado del niño. Además, el sistema escolar de información del estudiante (SIS) y/o las pantallas de las computadoras o listas que se usan en las cafeterías, deberán enmascarar u ocultar de alguna manera el estatus de elegibilidad del estudiante para evitar que otros puedan verlos o tener acceso a ellos, -especialmente otros estudiantes.

Si una organización local sin fines de lucro o programa recreativo quisiera ofrecer libros de texto gratuitos o clases de atletismo durante el verano, basándose en el estatus de FRL del niño, los padres primero deberán dar el consentimiento para permitir a la escuela que proporcione la información de elegibilidad del niño.

3. LA "IDENTIFICACIÓN ABIERTA" de estudiantes FRL está prohibida por la NSLA, incluyendo:

- publicidad o anuncio de los nombres de niños o familias elegibles;
- tener áreas para comer, líneas para servir y horarios de servicio separados; o
- el uso de tarjetas, boletos, fichas de comida u otros métodos para obtener alimentos reembolsables (ej.: uso de color o de códigos) de manera que se pueda identificar abiertamente a los niños que son elegibles de FRL.

4. LAS ESCUELAS PUEDEN REVELAR información agregada que no identifique a los individuos (ej.: un reporte sobre el número de niños elegibles para FRL en un distrito escolar) sin el consentimiento por escrito de los padres de los estudiantes.

NOTA: La información confidencial de elegibilidad que se recoge de las familias y los niños que aplican a otros Programas de Nutrición del Niño de USDA también está protegida para que no sea revelada sin autorización, incluyendo el Programa de Desayuno Escolar [School Breakfast Program (SBP)],³ El Programa Especial de la Leche [Special Milk Program (SMP)],⁴ El Programa de Verano de Servicio de Comida [Summer Food Service Program],⁵ y el Programa de Cuidado de Alimentos del Niño y el Adulto [Child and Adult Care Food Program].⁶

Una escuela del distrito de Kansas permitió repetidamente que empleados sin autorización vieran ilegalmente el estatus de elegibilidad de los estudiantes a través del sistema de información del estudiante del distrito. Después los maestros mostraron públicamente esta información en la "información publicada en muros" violando aparentemente las leyes de NSLA y FERPA.²

Si usted cree que los derechos de su hijo bajo NSLA han sido violados, deberá notificar a su escuela, Superintendente de distrito, y/o a el consejo escolar. Si ellos se rehúsan a tomar una acción apropiada, usted puede contactar al capítulo local de la ACLU (American Civil Liberties Union) para pedir ayuda o someter una denuncia con el USDA. Para mayor información y para obtener un formulario, visite http://www.ascr.usda.gov/complaint_filing_cust.html.



PPRA (Enmienda de Protección de los Derechos del Alumno) [Protection of Pupil Rights Amendment]

La Enmienda de Protección de los Derechos del Alumno (PPRA) [The Protection of Pupil Rights Amendment] (20 U.S.C. § 1232h; 34 CFR Part 98) también es administrada por el Departamento de Educación de los EE. UU. y se estableció en 1978. La PPRA aplica

para la administración de encuestas, análisis o evaluaciones de los estudiantes relacionadas con cuestiones muy sensibles o delicadas. Y también se refiere a las encuestas de mercadeo, acceso parental a los materiales educativos y ciertos exámenes físicos que aplican las escuelas a los estudiantes. Para más información sobre PPRA visite http://bit.ly/SPTK_PPRA

¿Cuáles son los derechos que tienen los padres ante la PPRA?

1. SE REQUIERE EL CONSENTIMIENTO DE LOS PADRES antes de que los niños participen en cualquier encuesta, análisis o evaluación financiada por el Departamento de Educación de los EE.UU. que se refiera a las siguientes áreas consideradas sensibles o delicadas:

- creencias o afiliaciones políticas del estudiante o de los padres del estudiante;
- problemas mentales y psicológicos del estudiante o de la familia del estudiante;
- creencias y afiliaciones religiosas;
- conducta y actitudes sexuales;
- conducta ilegal, antisocial, auto-incriminatoria y degradante;
- valoraciones críticas de familiares cercanos;
- relaciones privilegiadas reconocidas legalmente, como de abogados, médicos y ministros; o
- ingreso (más allá del requerido por la ley para determinar la elegibilidad para un programa).

2. NO SE REQUIERE EL CONSENTIMIENTO PARENTAL POR ESCRITO, si una encuesta, análisis o evaluación es administrada a los estudiantes y trata con las cuestiones mencionadas anteriormente y no está financiada federalmente – pero los padres deben ser notificados con anticipación y deben tener la opción de negarse a que sus hijos participen.

3. BAJO SOLICITUD, los padres pueden inspeccionar “cualquier material educativo que se use como parte del currículo educativo del estudiante”.^{4,5} Algunas escuelas usan currículo con “carácter de enriquecimiento”, el cual puede violar la privacidad del estudiante y la familia. Bajo PPRA, los padres tienen derechos específicos para revisar dichos materiales.

4. LA PPRA REQUIERE que las escuelas notifiquen directamente a los padres, por lo menos una vez al año, al principio del año escolar, cuando puedan ocurrir las siguientes actividades y otorga a los padres el derecho de optar por que sus hijos no participen en:

- la administración de cualquier encuesta que contenga uno o más de los temas mencionados anteriormente;
- cualquier revisión o examen físico invasivo, que no sea de emergencia, administrado por la escuela innecesariamente, para proteger la salud y seguridad inmediata de un estudiante, con excepción de las revisiones de escoliosis, de audición y visión; y
- actividades que involucren la recopilación, revelación o el uso de información personal obtenida de los estudiantes con propósitos de mercadeo o para vender o distribuir de cualquier forma, la información a terceras partes.

NOTA: Los derechos de los padres bajo PPRA se transfieren a los estudiantes que alcancen los 18 años de edad o que se conviertan en menores emancipados bajo la ley Estatal.

Si usted cree que los derechos de usted o de su hijo bajo PPRA han sido violados, notifique a su escuela, Superintendente de distrito, y/o el consejo escolar. Si ellos se rehúsan a tomar una

PPRA permite a los padres inspeccionar: “todos los materiales educativos, incluyendo manuales de los maestros, películas, tapes u otros materiales complementarios que vayan a ser usados en conexión con cualquier encuesta, análisis o evaluación, como parte de cualquier programa aplicable”.

Los materiales educativos incluyen: “contenidos educativos que se proporcionen a un estudiante, sin importar su formato, incluyendo materiales impresos o representativos, materiales audio visuales, y materiales en formato digital o electrónico (como los materiales accesibles a través del Internet). El término no incluye las evaluaciones o pruebas académicas”.

Su estado puede permitir o requerir que su escuela realice un examen o revisión física sin el consentimiento o notificación de los padres. Para familiarizarse con la ley que aplica en su estado, asegúrese de preguntar a su consejero o director escolar.

acción apropiada, puede contactar al capítulo local de la ACLU (American Civil Liberties Union) para pedir ayuda o someter una denuncia similar a FERPA con el U.S. Department of Education's Family Policy Compliance Office en:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520
Teléfono: 1-800-USA-LEARN (1-800-872-5327)
Email: FERPA.customer@ed.gov
Fax: 202-260-9001



COPPA (Ley de Protección de la Privacidad en Línea de los Niños) [Children's Online Privacy Protection Act]

El Congreso promulgó la **Ley de Protección de la Privacidad en Línea de los Niños (COPPA)** [Children's Online Privacy Protection Act] (15 U.S.C. 6501-6505) en 1998. Y es aplicada por la Comisión de Comercio Federal (FTC) [Federal Trade Commission].

La meta principal de COPPA es permitir a los padres controlar qué información personal se obtiene en línea, de sus hijos menores de 13 años. La ley se aplica a cualquier comerciante u operador de sitios de Internet dirigidos a menores de edad, incluyendo las pruebas, programas o aplicaciones ("apps") que se realizan en Internet y que recogen, usan o revelan información personal de los niños, ya sea en la escuela o en el hogar. La información personal puede incluir el nombre del menor, correo electrónico, número de teléfono, nombre en la pantalla, localización geográfica, foto, grabación de voz u otro identificador único persistente. Pero es importante saber que COPPA solamente se aplica a la información personal obtenida en línea directamente de los niños; y no cubre la información referente a sus hijos obtenida de los adultos. Para más información sobre COPPA visite <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.¹²

¿Qué derechos tienen los padres ante COPPA?

Si un menor de 13 años usa un sitio de Internet o aplicación como la descrita anteriormente, el vendedor u operador deberá obtener el consentimiento de los padres y deberá proporcionar una notificación clara y visible de sus prácticas de uso y revelación de información en su sitio de Internet, incluyendo lo siguiente:

1. **EL NOMBRE**, dirección, número de teléfono y correo electrónico de todos los operadores y vendedores que recogen o mantienen la información personal dentro de todo el sitio de Internet o durante el servicio que éste proporcione;
2. **UNA DESCRIPCIÓN** de cual información personal está recogiendo el vendedor u operador, incluyendo si el sitio de Internet o programa permite o no a los niños que hagan pública su información personal, cómo usa el vendedor u operador esta información y las prácticas de revelación de información del operador para tal información; y

De acuerdo a FTC, COPPA "se aplica también a los servicios en línea o sitios de Internet que tienen el conocimiento real de que están recopilando información personal directamente de usuarios de OTRO servicio en línea o sitio de Internet dirigido a niños".

De acuerdo a la FTC, el que un servicio de Internet o un sitio de Internet esté o no "dirigido a niños" se determina por "el tema del sitio o servicio, su contenido visual, el uso de caracteres animados o de actividades e incentivos orientados al niño, la música u otro contenido, la edad de los modelos, la presencia de celebridades infantiles o celebridades atractivas para niños, el lenguaje u otras características del servicio en línea o sitio de Internet, o ya sea que la publicidad que se promueva o que aparece en el mismo, esté dirigido a niños".

3. **UN AVISO** de que, a solicitud expresa, los padres pueden revisar y/o borrar la información personal del menor, rehusarse a permitir que se continúe usando o recogiendo información y una descripción de los procedimientos para hacerlo.

¿Qué derechos tienen los padres ante COPPA en las escuelas?

1. **LAS ESCUELAS PUEDEN CONSENTIR** a nombre de los padres, que los estudiantes creen cuentas e ingresen información personal dentro de programas en línea, que los estudiantes puedan usar cuando están en su escuela o casa –ya sea para instrucción, pruebas u otros propósitos- pero sólo donde el vendedor u operador del programa en línea recoge información personal para el uso y único beneficio de la escuela, y no para otros propósitos comerciales. Si la información personal del estudiante se usa para publicidad dirigida, por ejemplo, o para crear perfiles de usuarios con propósitos comerciales, la escuela **NO PUEDE** consentir a nombre de los padres.

2. **CUANDO LA ESCUELA DA SU CONSENTIMIENTO** a nombre de los padres, COPPA transfiere los derechos parentales a la escuela. En ese caso, 1) un vendedor u operador debe proporcionar a la escuela -no a los padres- un aviso claro y visible de sus prácticas de uso y revelación de información en su sitio de Internet o en cualquier otra aplicación, como se describió antes; y 2) las escuelas -no los padres- tienen el derecho de solicitar que el vendedor u operador borre la información personal de los estudiantes y deje de obtener y usar más información.

Si usted cree que el vendedor u operador está violando los derechos bajo COPPA, notifique primero a su escuela o Superintendente de distrito. También puede contactar al capítulo local de la ACLU (American Civil Liberties Union) para pedir ayuda; o contactar al FTC para hacer preguntas o someter una denuncia o queja al <https://www.ftccomplaintassistant.gov>, email CoppaHotLine@ftc.gov o llamar a la línea gratuita (877) FTC-HELP.

Limitación de responsabilidad: Aunque la meta de la Coalición de Padres por la Privacidad del Estudiante y la Campaña por una Infancia Sin Comerciales (Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood) es proporcionar recursos valiosos para ayudarle a proteger la privacidad del estudiante, nuestras sugerencias y recomendaciones no deben reemplazar los consejos legales de un abogado. Si tiene preguntas sobre cómo las leyes y políticas locales, estatales y federales pueden aplicarse a su situación particular, puede buscar el apoyo de un abogado con licencia, contactando al servicio de referencia de su asociación local de abogados.

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

El aviso debe localizarse en la "página principal o página inicial o en la pantalla de su sitio de Internet o servicio en línea y en cada área del servicio en línea o sitio de Internet donde se recopile información personal de niños".

La escuela puede negar el consentimiento a nombre de los padres, si un sitio de Internet o programa en línea dirigido al niño busca usar o revelar cualquier información personal, proporcionada por estudiantes menores de 13 años, para sus propios intereses o para propósitos comerciales.

Antes de que una escuela pueda consentir a sus estudiantes que usen programas en línea que recopilen información personal, el vendedor del sitio de Internet debe proporcionar a la escuela una notificación completa de cómo recopila, usa y divulga la información del estudiante.

REFERENCIAS

1. <https://nces.ed.gov/programs/slds/>
2. <http://cjonline.com/news-education-local-state/2014-08-19/usd-501-admits-student-privacy-violations-says-breach>
3. <https://www.fns.usda.gov/sbp/school-breakfast-program-sbp>
4. <https://www.fns.usda.gov/smp/special-milk-program>
5. <https://www.fns.usda.gov/sfsp/summer-food-service-program>
6. <https://www.fns.usda.gov/cacfp/child-and-adult-care-food-program>

SECCIÓN III.

Consejos para padres que quieren proteger la privacidad de su estudiante

En la escuela como en el hogar los niños y sus padres están muy presionados para que se involucren con la tecnología. Ya sea que los niños usen voluntariamente medios sociales personales o que los maestros asignen el uso de aplicaciones (apps) y programas en línea, ellos están compartiendo en línea cada vez más y más detalles de sus vidas. Usted puede sentirse abrumado, como si el genio se hubiera escapado de la botella, pero no es muy tarde para proteger la privacidad de sus hijos, tomando medidas simples. ¡Intente lo siguientes!



Consejos para el hogar

■ **RESISTA SU URGENCIA** de compartir todo con todos los demás. Antes de publicar fotos íntimas o detalles sobre la vida de sus hijos en los medios sociales, considere las implicaciones a largo plazo que tiene revelar esa información de manera tan amplia. Un estudio encontró que los niños resienten que sus padres publiquen sus fotografías en los medios sociales sin su consentimiento.¹ Otro estudio encontró que el padre de familia promedio en el Reino Unido comparte aproximadamente 1500 fotos de sus hijos antes de que estos cumplan 5 años.² Hablar con sus hijos sobre lo que es apropiado publicar para usted, también es una muy buena forma de iniciar conversaciones con ellos, sobre su conducta en los medios sociales.

■ **ESTABLEZCA LÍMITES** con sus hijos. Hable con ellos sobre la información que es apropiada para compartir en línea y aquella que no lo es. Anímeles a que pidan el permiso de sus amigos antes de publicar o compartir con los demás una fotografía de ellos.

■ **INSTALE BLOQUEADORES O FILTROS DE PUBLICIDAD** en los teléfonos, dispositivos y computadoras portátiles que sus hijos usan en la casa. Por ejemplo Privacy Badger,⁵ o una combinación de AdBlock⁶ y Ghostery,⁷ permite que los sitios de Internet se carguen más rápido y bloquea la publicidad que pudiera contener programas dañinos y otros virus. Estos programas también pueden evitar que las compañías monitoreen y obtengan un perfil de sus hijos.⁸

■ **ADHIERA UNA NOTA** o un pedazo de cinta adhesiva (ej.: un curita) sobre el lente de la cámara en los dispositivos electrónicos que sus hijos y usted utilicen, para evitar que los hackers las activen. ¡El fundador de Facebook Mark Zuckerberg y el ex-Director del FBI James Comey lo hacen!⁹

■ **ANTES DE DESCARGAR APLICACIONES GRATUITAS**, considere si está claro que el servicio o producto en línea se ofrece “gratuitamente”, a menudo, el precio real que usted paga es la información de sus hijos, que se explota con propósitos de publicidad y mercadeo. Motive a sus hijos para que le pidan permiso antes de suscribirse a cualquier aplicación. Esto es un requerimiento legal bajo COPPA (Ley de Protección de la Privacidad en Línea de los Niños) [Children’s Online Privacy Protection Act], si ellos son menores

Un estudio reciente reveló que “los mismos circuitos cerebrales que se activan por comer chocolate y ganar dinero, se activan cuando los adolescentes ven números elevados de “me gusta” (likes) en sus propias fotos y que son influenciados definitivamente por sus “amigos” en línea, aún cuando casi no les conozcan”.⁴

Otórquese una capa adicional de protección usando “HTTPS Everywhere” de Electronic Frontier Foundation. Aprenda más al respecto en <https://www.eff.org/https-everywhere>.

de 13 años y están proporcionando información personal. Para más información sobre COPPA vea la Sección II.

■ CONSIDERE LA CREACIÓN DE UNA CUENTA NUEVA DE CORREO ELECTRÓNICO

—que no contenga un nombre real u otra información que le identifique— para que inscriba a sus hijos en aplicaciones o cuentas en línea.

■ **ENSEÑE A SUS HIJOS** a crear nombres de usuarios y claves para sus cuentas en línea que no contengan su información de identificación personal como nombre, fecha de nacimiento, número de estudiante, nombre de su mascota o nombre de la escuela.

■ **LOS TÉRMINOS DE SERVICIO** y políticas de privacidad son, con frecuencia, a propósito muy largos, complicados y difíciles de entender. Use la sección que se presenta enseguida, “QUÉ BUSCAR EN LOS TÉRMINOS DE SERVICIO Y POLÍTICAS DE PRIVACIDAD”, para revisar rápidamente los términos y políticas de cualquier aplicación o programa en línea que sus hijos utilicen. No permita que su hijo los use si ve cualquier señal de alarma de las que se mencionan en esta lista.



Consejos para la escuela

■ **PREGUNTE A LOS MAESTROS DE SUS HIJOS** cuáles aplicaciones o programas en línea se usarán a lo largo del año escolar, y qué información personal recoge cada aplicación. Pregunte si esos programas han sido aprobados por el distrito o el estado en términos de protección de privacidad y seguridad y si cumplen con las leyes estatales y federales. En la Sección V y Anexo D encontrará una lista de preguntas para hacerle al maestro.

■ **ANIME A LOS MAESTROS DE SUS HIJOS** y a la escuela a que se resistan a usar aplicaciones y programas en línea que no sean imprescindibles, siempre que les sea posible. Considere optar porque su hijo no use aplicaciones y programas en línea excesivos o inseguros.

■ **PREGUNTE A LOS MAESTROS DE SUS HIJOS** si ellos pueden crear cuentas sin usar los nombres reales de los estudiantes, y/o si pueden evitar la revelación de cualquier información del estudiante que no se necesite para el uso de la aplicación o programa en línea.

■ **NO ASUMA** que las políticas de privacidad de las aplicaciones o programas en línea asignados a sus hijos —especialmente las gratuitas— han sido lo suficientemente examinadas por sus maestros. Las aplicaciones educativas o del salón de clases pueden no respetar la privacidad del estudiante más allá que cualquier otra aplicación.

■ **REVISE LOS TÉRMINOS DE SERVICIO** y políticas de privacidad de cualquier aplicación o programa en línea para usar en el salón de clases, que se asigne a su hijo. Si usted ve cualquiera de las señales de alarma que se describen en la siguiente sección, acérquese al maestro o director de la escuela y hablele de sus preocupaciones.

■ **PREGUNTE AL DIRECTOR** si la escuela mantiene la información personal del estudiante en la “Nube”, y si es así, si existe un contrato que impida que el vendedor u

¡Ayude a su hijo a crear claves seguras! Trate de usar un acrónimo de algo que su hijo pueda recordar con facilidad, de preferencia una oración completa. Use combinaciones de letras mayúsculas y minúsculas, números y símbolos. Por ejemplo, la oración “Yo amo el videojuego de la Copa Mundial de la FIFA” puede expresarse como “I<3tFIFAWCvg.”

¿Por qué algunas aplicaciones del salón de clases son gratuitas y qué significa esto para la privacidad del niño? La tecnología puede ser una herramienta para aumentar el conocimiento del estudiante, pero también puede ser cara, razón por la que las aplicaciones y los programas del salón de clases gratuitos son muy atractivos para los maestros y las escuelas. Pero como dice un viejo refrán, “nada en la vida es gratis.” Si la escuela o el distrito no están pagando por la aplicación o programa en línea, lo más probable es que la compañía se está beneficiando de la información de su hijo, de alguna u otra forma.

operador venda la información, la vuelva a revelar a otros, o la use con propósitos no-educativos. Pregunte si la información está siendo codificada adecuadamente durante su almacenamiento y transmisión.

■ **HABLE CON SUS HIJOS QUE ESTÁN EN LA ESCUELA PREPARATORIA** (high school) sobre los reclutadores militares que puedan visitar la escuela. Si sus hijos no están considerando inscribirse en el servicio militar, asegúrese que no acepten regalos de parte de los reclutadores y que no compartan información personal con ellos.

■ **SOMETA UNA PETICIÓN POR ESCRITO** al director de la escuela para optar por no proporcionar la información personal de la escuela preparatoria de su hijo, a los reclutadores militares. Vea un ejemplo de un formulario en el Anexo C.

■ **PREGUNTE AL DIRECTOR** de la escuela como optar por no estar en la “información de directorio” y prohibir a la escuela que comparta información personal con terceros, ejerciendo su derecho bajo FERPA (Ley de Privacidad y Derechos Educativos Familiares) [Federal Education Rights and Privacy Act]. Su escuela le debe proporcionar esas formas sin que usted las solicite, pero muchas escuelas no lo hacen. A menudo, también las escuelas tienen una fecha límite para optar por no incluirse dentro de la información de directorio, regularmente es dentro de los primeros 10 a 30 días del ciclo escolar. Para mayor información al respecto, vea la Sección II y el Anexo B donde presentamos un ejemplo de un formulario para optar por no incluirse en la información de directorio.

■ **EJERZA SUS DERECHOS** ante FERPA para acceder y revisar anualmente los archivos educativos de sus hijos en la escuela y a nivel del distrito, así como los archivos contenidos en el SLDS (Sistema Estatal de Datos Longitudinales) [Statewide Longitudinal Data System]. Solicite que corrijan cualquier error que usted vea en esos archivos. Para más información sobre el SLDS, vea las Secciones II y VII. Para solicitar acceso y revisar los archivos de su hijo, use el ejemplo de formulario de solicitud que se encuentra en el Anexo A.

■ **CUANDO REGISTRE A SUS HIJOS** para los exámenes de College Board/SAT o ACT, no marque la casilla para optar por compartir información personal con colegios u otras organizaciones ajenas, y no proporcione a esas compañías ninguna información innecesaria. Puede ser que, le pidan a sus hijos que proporcionen información personal de nuevo el día del examen; aconséjeles que no marquen ninguna otra casilla o que no proporcionen ninguna otra información, más allá que su nombre, grado escolar, escuela y otros detalles requeridos para poder presentar el examen. Cuando los estudiantes marcan esa casilla sobre información adicional, a menudo, las compañías que hacen los exámenes venden la información a colegios, universidades o terceros, para usarla con propósitos de publicidad o reclutamiento o para ayudar a los colegios a decidir si los aceptan o los rechazan.



¿Qué buscar en los términos de servicio y políticas de privacidad?

Si los términos de servicio y/o las políticas de privacidad de los programas en línea que sus hijos usan en la casa o en la escuela incluyen cualquiera de las señales de alarma que

Un estudio realizado por la Escuela de Leyes de Fordham (Fordham Law School) en el 2010 encontró que el “95% de los distritos se apoyan en los vendedores para un rango muy diverso de funciones, incluyendo la recopilación y la extracción de datos relacionada con la ejecución del estudiante, el apoyo para las actividades del salón de clases, la guía del estudiante, el almacenamiento de la información, así como servicios especiales como los pagos de cafetería y la planeación del transporte.”¹¹

Antes de una prueba, el maestro de su hijo puede leer en voz alta las instrucciones preparadas por el College Board/ACT y a los estudiantes les puede parecer que deben responder a preguntas personales. Asegúrese de informar a su hijo antes de la prueba, que es estrictamente voluntario proporcionar respuestas a cualquier pregunta relacionada con los temas que mencionamos enseguida.

Las preguntas pueden relacionarse con los siguientes temas personales:

- información para contactarle;
- área de estudio;
- género;
- estado de necesidades especiales;
- calificaciones y rango;
- antecedentes étnicos;
- religión;
- ingreso de los padres y ayuda financiera;
- deportes;
- preferencias para vivir en el colegio;
- ciudadanía;
- características del colegio deseado;
- cursos y actividades de la escuela preparatoria (high school); y
- honores.

Para ejemplos adicionales refiérase a nuestra Sección de Recursos donde encontrará enlaces al Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. (U.S. Department of Education's Privacy Technical Assistance Center).

se mencionan a continuación, considere no usarlos. El lenguaje debe ser revisado por un oficial de la escuela o un abogado, para asegurar que no están violando las leyes estatales o federales o las políticas del distrito.

EJEMPLO: “La Compañía se reserva el derecho, a su absoluta discreción, de modificar o reemplazar cualquier parte de esta Política de Privacidad”.

MOTIVO DE PREOCUPACIÓN: No se debe permitir a las compañías cambiar sus políticas antes de notificar y obtener el consentimiento de los usuarios. En el caso de las aplicaciones usadas en las escuelas, los cambios unilaterales hechos por una compañía pueden resultar en el uso o divulgación inapropiada o hasta ilegal de la información del estudiante.

EJEMPLO: “Al usar este Servicio, usted está autorizando a la Compañía a usar, recoger, analizar y retener cualquier información relacionada con la porción del Servicio”.

MOTIVO DE PREOCUPACIÓN: Las compañías deben ser muy explícitas sobre qué información del usuario van a recoger, y cómo la van a utilizar, compartir y borrar. Cuando las aplicaciones se usan en las escuelas, generalmente se les permite usar la información del estudiante únicamente con propósitos educativos. Utilizar esa información con cualquier otro propósito –comercial o de otra índole– puede ser una violación a la ley federal incluyendo FERPA y COPPA.

EJEMPLO: “La Compañía comparte su información con terceros socios comerciales con el propósito de proporcionarle el Servicio. También podemos compartir cierta información, tal como el buscador y datos de cookies y otra información relativa al uso de nuestro Servicio con nuestros socios comerciales para proporcionar información sobre productos y servicios que puedan ser de su interés”.

MOTIVO DE PREOCUPACIÓN: Las compañías deben identificar por su nombre, dirección, número de teléfono y correo electrónico a cualquier otro socio tercero que recoja o mantenga la información personal de sus hijos, obtenida a través de la aplicación. Si no es así, ellos pueden estar violando COPPA (si su hijo es menor de 13 años y el sitio de Internet está dirigido a niños) o FERPA. Además, las compañías no deben usar la información recogida sobre los niños para desarrollar perfiles comerciales o de publicidad o para hacer anuncios dirigidos a los niños o a sus padres.

EJEMPLO: “La Compañía y sus socios y licenciarios pueden recoger, usar, transmitir, procesar y mantener los datos de localización, incluyendo, pero no limitándose a la localización geográfica de su dispositivo (por ejemplo latitud y/o longitud) de la información relacionada con su cuenta”.

MOTIVO DE PREOCUPACIÓN: Ya sea que la aplicación se use en casa o en la escuela, las compañías no deben recoger los datos de localización geográfica de los niños.

EJEMPLO: “Ninguna transmisión de datos en el Internet es 100% segura. La Compañía se esforzará en proteger su información de identificación personal, pero no puede garantizar la seguridad de cualquier información que usted nos transmita y usted lo hace bajo su propio riesgo”.

MOTIVO DE PREOCUPACIÓN: Las compañías deben siempre cifrar los datos personales de sus usuarios, emplear las mejores prácticas para asegurar los datos y no deben intentar eximirse de responsabilidades si ocurren violaciones.

CommonSense Media aconseja a los padres que “busquen la ‘https’ en la URL” y ofrece otros consejos para mejorar la seguridad y privacidad de los datos del estudiante en <https://www.commonsense.org/education/privacy>.¹²

EJEMPLO: “La compañía puede compartir información que recopile en conexión con una transacción corporativa, tal como la venta de nuestros servicios, una fusión, consolidación o venta de bienes o en caso de bancarrota”.

MOTIVO DE PREOCUPACIÓN: Mientras que algunas leyes estatales de privacidad prohíben la venta de datos estudiantiles personales, las compañías pueden reclamar excepciones que permitan la venta de los datos en caso de una fusión, bancarrota o venta de “bienes”. Otros pueden reclamar que mientras que no vendan los datos, ellos pueden dar “licencia” a otras compañías u organizaciones, a cambio de una cuota. Los padres deben estar alertas sobre ese tipo de enunciados en los Términos de Servicio o Políticas de Privacidad de una corporación.

Limitación de responsabilidad: Aunque la meta de la Coalición de Padres por la Privacidad del Estudiante y la Campaña por una Infancia sin Comerciales (Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood) es proporcionar recursos valiosos para ayudarle a proteger la privacidad del estudiante, nuestras sugerencias y recomendaciones no deben reemplazar los consejos legales de un abogado. Si tiene preguntas de cómo las leyes y políticas locales, estatales y federales pueden aplicar a su situación particular, puede buscar el apoyo de un abogado con licencia, contactando al servicio de referencia de su asociación local de abogados.

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. http://well.blogs.nytimes.com/2016/03/08/dont-post-about-me-on-social-media-children-say/?_r=0
2. <http://www.nominet.uk/wp-content/uploads/2016/09/Nominet-Share-with-Care-2016-Infographic.pdf>
3. <http://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/>
4. <https://www.sciencedaily.com/releases/2016/05/160531104423.htm>
5. <https://www.eff.org/privacybadger>
6. <https://getadblock.com/>
7. <https://www.ghostery.com/>
8. <http://www.computerworld.com/article/2692560/six-browser-plug-ins-that-protect-your-privacy.html>
9. http://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html?_r=0
10. <http://www.siiia.net/Press/SIIA-Estimates-838-Billion-Dollars-US-Market-for-PreK-12-Educational-Software-and-Digital-Content>
11. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip>
12. <https://www.commonsense.org/education/privacy/survey/encryption>

SECCIÓN IV.

Buenas prácticas de protección de la privacidad de los estudiantes para maestros, escuelas, distritos y estados

En un mundo ideal, la información delicada o sensible del estudiante se debería mantener resguardada bajo llave y solamente con el permiso de los padres, podría ser compartida con maestros, consejeros, tutores y otro personal escolar confiable. Aunque esto no es posible en el mundo actual de las escuelas controladas por la tecnología y los datos, es importante implementar las mejores prácticas, bien pensadas, para salvaguardar la información del estudiante a nivel de la escuela, del distrito y del estado.

Muchas de estas recomendaciones provienen de nuestra coalición integrada por Cinco Principios para Proteger la Privacidad del Estudiante (Five Principals to Protect Student Privacy),² el PTAC (Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU.) [U.S. Department of Education's Privacy Technical Assistance Center]³, y otras organizaciones expertas que se ocupan en este tema. Aunque nuestras mejores prácticas pueden ir más allá de lo requerido por nuestras actuales leyes estatales y federales, los estados, los distritos, las escuelas y sus maestros deben implementar esas políticas, si quieren mejorar las protecciones de seguridad y privacidad del estudiante y limitar su propia responsabilidad. ¡Comparta hoy mismo estas prácticas con su escuela!

LA IMPORTANCIA DE LOS ACUERDOS POR ESCRITO

Uno de los mejores métodos para ayudar a proteger la información del estudiante es solicitar por escrito acuerdos, contratos, memorándums de entendimiento (MOUs) entre estados/escuelas/distritos y cualquier otro tercero interesado en tener acceso o recibir información personal del estudiante, incluyendo compañías que ofrezcan programas educativos en línea o aplicaciones (apps) de salón de clases gratuitos. Los acuerdos por escrito pueden limitar como se recoge, usa y comparte con otros la información del estudiante; los acuerdos también requieren que la compañía adopte requisitos fuertes de notificación de seguridad y violaciones cibernéticas, incluyendo sanciones aplicables por incumplimiento y que especifiquen los procedimientos a los que pueden recurrir los padres.

Para obtener una lista completa de lo que se debe incluir en los acuerdos por escrito, vea el documento del Consorcio de Redes de Escuelas (CoSN) [Consortium of School Network's] titulado “Términos de Contrato Sugeridos”, (http://www.cosn.org/sites/default/files/pdf/Suggested_Contract_Terms_09_2014.pdf) y un ejemplo de contrato preparado por la Alianza para la Privacidad del Estudiante de Massachusetts (https://secure2.cpsd.us/mspa/MSPA_Student_%20Data_Privacy_Agreement_V4.pdf).

Nota: Si los estados, escuelas y/o distritos comparten la información del estudiante con organizaciones y agencias sin el consentimiento de los padres, como se estipula bajo las excepciones de “estudios” o “auditorías o evaluaciones” de FERPA (Ley Federal de Privacidad y Derechos Educativos) [Federal Education Rights and Privacy Act], como se describe en la Sección II, se requiere un acuerdo por escrito. Para más información vea la “Lista de Acuerdos por Escrito” (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Written_Agreement_Checklist_0.pdf) proporcionado por el Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. (U.S. Department of Education Privacy Technical Assistance Center).



Las mejores prácticas para los departamentos de educación estatales

- **SOLICITAR** por escrito los acuerdos, contratos o memorándums de entendimiento (MOUs) entre el estado y cualquier tercero en cuestión, que reciba información personal del estudiante, y publicar dichos documentos de forma prominente en el sitio de Internet del estado.
- **NOMBRAR** a un Oficial de Privacidad en Jefe, que sea un experto en la ley y en las prácticas de seguridad y privacidad, para que sea el responsable de establecer un programa de gobernanza de datos integral y se comuniquen con los padres que tengan preguntas o preocupaciones.
- **CREAR** un consejo asesor de las partes interesadas en los datos que incluya padres, maestros y expertos en privacidad, para que aporten al respecto y supervisen la recolección, gobernanza y divulgación de los datos del estudiante. Este es un punto crítico para asegurar que la privacidad y la seguridad tengan prioridad y que el público pueda aportar en las decisiones que se refieran al uso de la información personal del estudiante.
- **EVALUAR** los programas educativos en línea y las aplicaciones gratuitas que se usan en el salón de clases en términos de su propósito y contenido educativo, prácticas de uso de los datos, y estándares de privacidad y seguridad, y aprobarles o rechazarles de acuerdo a ello. Ninguna aplicación o programa en línea debe considerar usarse si proviene de cualquier vendedor u operador que no haya firmado un contrato con el estado y que no haya firmado el Compromiso de Privacidad del Estudiante (Student Privacy Pledge), el cual prohíbe la venta de información personal del estudiante excepto en los casos de fusiones, adquisiciones y bancarrotas.



Las mejores prácticas para las escuelas y los distritos escolares

- **REQUERIR** por escrito los acuerdos, contratos o memorándums de entendimiento (MOUs) entre el distrito/escuela y cualquier otro tercero que reciba o tenga acceso a la información personal del estudiante. Publicarlos de manera prominente en la escuela o sitio de Internet del distrito y enviar a los padres al hogar y/o por correo electrónico la información sobre donde pueden leerlos.
- **ADOPTAR** y apegarse a la lista de aplicaciones y programas en línea aprobados por el departamento de educación del estado, y publicar la lista actual en el sitio de Internet de la escuela o del distrito. También los distritos pueden decidir crear un procedimiento aún más riguroso para prohibir aplicaciones y programas en línea.
- **DESIGNAR** un Oficial de Privacidad en Jefe, o algún miembro del personal para que se haga responsable de asegurar que se realicen las mejores prácticas y para comunicarse con los padres.

El Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. recomienda que los programas de gobernanza de los datos deben abordar:

- *protección de datos sensibles;*
- *evaluación de la vulnerabilidad y manejo del riesgo;*
- *aplicación de requisitos legales, regulatorios, contractuales y de arquitectura;*
- *identificación de las partes interesadas, como padres y administradores, así como de sus roles y responsabilidades;*
- *acceso a la administración".*

El Consorcio de Redes Escolares (CoSN) recomienda que los contratos deben: "Incluir una restricción específica sobre el uso de la información del estudiante por parte del proveedor para propósitos de publicidad o mercadeo, o sobre la divulgación de la información del estudiante por parte de los proveedores".⁴

La Escuela de Leyes de Fordham recomienda que "los acuerdos de servicios de la nube" deben: "Incluir una cláusula explícita que se refiera a nube" deben: "Incluir una cláusula explícita sobre la venta y mercadeo de la información transferida o el uso de esa información por el mismo vendedor, con propósitos de venta y mercadeo, cuando no se da el consentimiento parental".⁵

■ **TRABAJAR CON** los padres, maestros y promotores de la privacidad para adoptar políticas transparentes en relación a la recolección, uso y protección de los datos del estudiante, incluyendo:

- identificar y luego minimizar la recopilación de la información personal del estudiante;
- justificar el objetivo de cada tipo de recopilación, incluyendo una explicación de su propósito educativo;
- describir cómo se recopila, almacena y se protege la información de posibles violaciones cibernéticas y cómo los padres pueden acceder a la información y corregirla si es necesario;
- identificar a quién se revelará la información, incluyendo individuos, organizaciones o vendedores u operadores fuera de la escuela o distrito, y con qué propósitos se revelará; y
- definir el proceso para notificar a los padres antes de que la información sea revelada.

■ **PROHIBIR** a las escuelas que proporcionen toda información personal del estudiante, incluyendo la “información de directorio”, a cualquier tercero en cuestión que tenga la intención de usar o vender la información del estudiante con propósitos comerciales.

■ **ADOPTAR** una política pública que permita a los padres especificar cual “información de directorio” puede ser compartida y con quien. Vea la Sección II para mayor información sobre este tema.

■ **PEDIR** el permiso o consentimiento de los padres antes de compartir datos altamente sensibles, como discapacidad, salud e información disciplinaria, con terceras personas, incluyendo vendedores, operadores u organizaciones.

■ **PROPORCIONAR** regularmente capacitación sobre seguridad de la información, incluyendo buenas prácticas, a maestros, a administradores y a cualquier otra persona que maneje información personal del estudiante.

■ **PROHIBIR** a los maestros que asignen o promuevan que los estudiantes usen en el salón de clases cualquier aplicación o programa en línea que no esté en la lista aprobada por el distrito o el estado.

■ **PROHIBIR** la publicación en cualquier área semi-pública, incluyendo salones de clase o pasillos, de “datos para publicar en muros” (data walls) que revelen información personal del estudiante, incluyendo nombres u otra información de identificación.



Las mejores prácticas para los maestros

■ **ANTES DE ASIGNAR** a los estudiantes una aplicación o un programa en línea, considere si su uso es o no necesario – se pueden evitar muchos problemas de privacidad simplemente no adoptando cada una de las nuevas herramientas en línea que se ofrecen a las escuelas.

■ **NO USE** o pida a los estudiantes que no usen cualquier aplicación o programa en línea, a menos que haya sido primero examinada y aprobada por el departamento de educación del estado o distrito.

Nosotros recomendamos que la notificación a los padres debe incluir:

- una lista de aplicaciones y programas en línea, que solicitan usar.
- el propósito/valor educativo de cada aplicación o programa en línea.
- la información del estudiante que se extraerá en cada aplicación o programa.
- los términos principales de cada política de privacidad de cada aplicación o programa en línea.
- si los padres pueden o no optar por prohibir que sus hijos usen la aplicación o programa en línea, y si es así, las alternativas disponibles.
- si la aplicación o programa en línea recoge y analiza datos o no, para crear un perfil de aprendizaje que dirija las lecciones o vías educativas del estudiante. Si lo hace, se debe explicar la tecnología a los padres para poder probar su utilidad y exactitud.

El Distrito Escolar Independiente de Houston desarrolló un sistema para evaluar la privacidad, la seguridad y la protección de aplicaciones del Internet que se usan comúnmente. Usted puede revisar los criterios utilizados en: <http://www.houstonisd.org/Page/126147>.

■ **PREPÁRESE** para ofrecer una alternativa apropiada (ej.: un libro de texto o una versión de lápiz y papel) a los estudiantes cuyos padres opten por no usar un programa en línea que accede a su información personal.

■ **NUNCA SE SUSCRIBA** a programas en línea o aplicaciones para salones de clase que incluyan “aceptar el acuerdo con un click” (“click-wrap” agreements) –donde el usuario marca una casilla para aceptar los términos y condiciones antes de usar un producto o servicio– a menos que los términos de servicio hayan sido revisados rigurosamente por alguien que tenga experiencia técnica y/o legal. Recuerde que aún con la revisión, los términos de servicio pueden cambiar con el tiempo, poniendo en riesgo la privacidad del estudiante. Para aprender más sobre “aceptar el acuerdo con un click, vea la guía de PTAC en http://bit.ly/SPTK_C”

Inscríbese hoy en los entrenamientos sobre privacidad que ofrece el Departamento de Educación de los EE.UU. en <https://studentprivacy.ed.gov/training/student-privacy-101>

■ **APRENDA POR SÍ MISMO** sobre los principios de la buena ciudadanía digital e incorpore prácticas responsables de tecnología en su salón de clases. Incorpore el currículo “Privacidad para Educadores de Salones de Clases” (“Privacy Educators Classroom”) de la Escuela de Leyes de Fordham dentro de sus lecciones. Lo puede encontrar en https://www.fordham.edu/info/24071/privacy_education.

■ **CUANDO GENERE** “datos para publicar en muros” en áreas públicas como los salones o pasillos donde se muestren grados o calificaciones de exámenes estudiantiles, nunca incluya información alguna que pueda usarse para identificar a los estudiantes.

Limitación de responsabilidad: Aunque la meta de la Coalición de Padres por la Privacidad del Estudiante y la Campaña por una Infancia Sin Comerciales (Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood) es proporcionar recursos valiosos para ayudarle a proteger la privacidad del estudiante, nuestras sugerencias y recomendaciones no deben reemplazar los consejos legales de un abogado. Si tiene preguntas sobre cómo las leyes y políticas locales, estatales y federales pueden aplicarse a su situación particular, puede buscar el apoyo de un abogado con licencia, contactando al servicio de referencia de su asociación local de abogados.

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. <http://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/>
2. <https://studentprivacy.ed.gov/training/student-privacy-101>
3. <https://studentprivacypledge.org/>
4. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip>
5. <http://cosn.org/sites/default/files/CoSN-Privacy-Toolkit.pdf>

SECCIÓN V.

Hablando con los maestros, las escuelas y los distritos sobre la privacidad del estudiante

Usted no tiene que ser un experto en la ley de privacidad o en las políticas del distrito escolar para expresar sus preocupaciones sobre la privacidad del estudiante. Simplemente, organice una reunión con el maestro de su hijo o el director de la escuela y haga algunas preguntas que le ayuden a establecer líneas de comunicación. A continuación le sugerimos algunas preguntas, pero recuerde que no tiene que hacerlas todas. También puede darle seguimiento a sus preocupaciones con algunas de las preguntas adicionales que se presentan en el Anexo D.

■ **¿CUÁNTAS HORAS AL DÍA APROXIMADAMENTE**, se espera que mi hijo use un dispositivo electrónico, incluyendo computadoras, computadoras portátiles, tabletas, y/o teléfonos inteligentes?

■ **¿CUÁLES PROGRAMAS EN LÍNEA** y aplicaciones (apps) del salón de clases se asignarán a mi hijo en este año escolar?

■ **¿ESTOS PROGRAMAS Y APLICACIONES SE HAN ANALIZADO** en cuanto a seguridad, privacidad y cumplimiento con las leyes de privacidad, estatales y federales?

■ **¿QUÉ DATOS SOBRE MI HIJO ESTÁ RECOGIENDO** la escuela, sus contratistas y cualquier otro vendedor u operador de programas en línea y aplicaciones que se usan en el salón de clases?

■ **¿CUÁLES DE ESOS DATOS ESTÁN ENVIÁNDOSE** al departamento de educación del estado?

■ **LOS VENDEDORES** que proporcionan esos programas, ¿están siendo vetados para que no puedan usar los datos con propósitos comerciales y compartirlos con terceros, y/o enviar anuncios a mi hijo?

■ **¿CÓMO PUEDO YO ACCEDER** a los datos de mi hijo que han sido extraídos y almacenados por el vendedor u operador, la escuela, el distrito o el estado? (Vea la Sección II para obtener más información sobre los derechos que usted tiene bajo la ley federal, para acceder a esa información).

■ **¿QUIÉNES DEL PERSONAL DE LA ESCUELA** o entre los contratistas, vendedores u operadores, tienen acceso a los datos de mi hijo?

■ **¿CUÁL ES LA POLÍTICA QUE GOBIERNA**, si existe, quien puede tener acceso a los datos de mi hijo(a) y bajo que circunstancias?

■ **¿CÓMO ES QUE LOS DATOS DE MI HIJO** están protegidos contra violaciones cibernéticas de la seguridad?

■ **¿POR CUÁNTO TIEMPO** los datos de mi hijo son retenidos por la escuela, contratistas o vendedores de programas en línea y aplicaciones del salón de clases?

■ **¿A QUÉ DATOS** tiene acceso la escuela o el proveedor del dispositivo electrónico (ej.: Microsoft, Apple, Google, etc.) cuando mi hijo está usando un dispositivo que le proporciona la escuela? Por ejemplo, ¿puede la escuela tener acceso a la información que se menciona abajo?

- información de ubicación;
- dirección de IP;
- cámara y micrófono;
- historia de sitios visitados en Internet;
- contenido almacenado localmente;
- contactos; o
- cualquier otra información que mi hijo no haya proporcionado explícitamente a la escuela.

■ **¿OFRECE LA ESCUELA** a las familias alguna forma de que opten por no proporcionar o minimizar la cantidad de información que recoge la escuela o cualquier otro programa/aplicación en línea usados en el salón de clases?

■ **¿A QUIÉN MÁS** puedo preguntar, si usted no puede responder a mis preguntas?

Para más consejos vea la Fundación WICKR en www.wickr.org/expiration-date-for-kids-data/

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

SECCIÓN VI.

Abogando por la privacidad del estudiante en las escuelas, los distritos y más allá

Si usted no está satisfecho con la respuesta de la escuela a sus preocupaciones y preguntas mencionadas en la Sección V, quizás sea tiempo de abogar por mejores prácticas y políticas públicas de privacidad. ¡Usted lo puede hacer! Algo que ayuda bastante es conectarse con otros padres de su comunidad escolar que tienen preocupaciones similares. Posiblemente usted encuentre aliados y expertos en otras organizaciones que le puedan dar información y apoyo muy valioso.



Pasos iniciales importantes

- **HABLE CON OTROS PADRES** de compañeros de clases de su hijo y/o con miembros de la organización de padres-maestros para compartir sus preocupaciones.
- **PREPARE PUNTOS CLAVES** y preséntelos ante el consejo de la escuela; pida a un amigo que grabe video de su presentación y considere publicarla en línea.
- **JUNTO CON OTROS PADRES**, publique una petición en línea o recopile firmas para presentar una petición fuera de la escuela; asegúrese de obtener los correos electrónicos y otra información de contacto. En el Anexo E encontrará un modelo de petición a un consejo escolar solicitando que realice audiencias públicas donde se aborden los problemas de privacidad del estudiante.
- **SI USA MEDIOS SOCIALES ELECTRÓNICOS**, publique sus preocupaciones en su cuenta personal, o en una cuenta importante de la comunidad local. También puede crear su propia cuenta de medios sociales electrónicos específicamente para ese tema de interés. ¡Los medios sociales electrónicos pueden ser una herramienta muy poderosa!
- **DÉ SEGUIMIENTO** con los administradores del distrito o con los miembros del consejo escolar, y/o los oficiales locales electos que le representan, y propicie una reunión que incluya a otros padres que compartan sus preocupaciones.

Intente usar estas tres formas de iniciar una conversación:

1. "Pareciera que a mi hijo le están enseñando cada vez más y más por medio de programas de computadora en lugar de que sea el maestro quien lo haga. ¿Ha notado usted eso?"
2. "Es difícil estar al corriente con todas las cuentas y nombres y claves de ingreso que mi hija tiene que recordar para poder terminar su tarea. ¿También su familia se siente así?"
3. "Recuerdo los viejos tiempos cuando hablábamos con los maestros de nuestros hijos en persona, en lugar de hacerlo a través de notificaciones por teléfono. ¿No cree usted también que esta comunicación es impersonal?"



Organice, involucre y empodere

- **UNA VEZ QUE YA IDENTIFICÓ** a un grupo pequeño de padres activos con las mismas preocupaciones que usted, realice una reunión en un centro comunitario, biblioteca, iglesia u otro lugar de reunión.
- **INVITE A EXPERTOS** que compartan y conozcan sobre la causa, como los miembros de su Unión Estadounidense por las Libertades Civiles (ACLU) [American Civil Liberties Union], oficiales electos locales o especialistas en Tecnología de la Información (IT), para

Cuando prepare los puntos claves, una buena forma de iniciar es usar o modificar las sugerencias que le presentamos en la Sección IV.

que hablen sobre el tema de la privacidad de los estudiantes y respondan preguntas. Los padres pueden describir cómo las prácticas laxas de privacidad del estudiante pudieron haber afectado a sus propios hijos y puesto en riesgo su privacidad.

■ **INVITE A LOS MIEMBROS** de la comunidad escolar a través de los medios sociales electrónicos, correos electrónicos y volantes. Asegúrese de invitar a los padres que firmaron su petición.

■ **DECIDA** si quiere pedir a los medios de comunicación locales a que den publicidad a la reunión, y /o invitar a los reporteros a que asistan y puedan ayudar a diseminar la noticia. Enseguida se presenta más información al respecto.

■ **PRESENTE LA INFORMACIÓN** de nuestra caja de recursos, incluyendo la Sección IV.

■ **DESPUÉS DE UN PERÍODO DE PREGUNTAS Y RESPUESTAS**, discuta colectivamente o en grupos pequeños cuáles serán los siguientes pasos. Asegúrese de entregar la información sobre su petición junto con la información para contactarle.



Expanda su alcance

■ **ORGANICE** una reunión de seguimiento con los administradores del distrito, miembros del consejo escolar u oficiales locales electos, para discutir sus preocupaciones y presentar su petición.

■ **PIDA A LOS ADMINISTRADORES** que consideren la adopción de prácticas efectivas para asegurar y proteger la información del estudiante. Usted puede usar las recomendaciones que le presentamos en la Sección IV como punto de inicio.

■ **EXHORTE A LOS MIEMBROS DEL CONSEJO ESCOLAR** a que patrocinen una resolución que adopte dichas sugerencias.

■ **PIDA A LOS OFICIALES LOCALES ELECTOS** que escriban una carta de apoyo.

Si usted tiene una reunión o una presentación, puede copiar e incluir cualquier sección o material de apoyo de esta caja de recursos – use lo que sea más relevante para aquello que está tratando de lograr.

Acérquese a grupos que le pueden ayudar¹ y que se preocupen por la privacidad del estudiante como:

*Parent Coalition for Student Privacy
Campaign for a Commercial-Free
Childhood
Electronic Frontier Foundation
Network for Public Education
Electronic Privacy Information Center
Parents Across America
American Civil Liberties Union*

¡NO OLVIDE!

Asegúrese de dar seguimiento a cualquier reunión que realice, haciendo una carta dirigida a los oficiales agradeciéndoles por su tiempo y responsabilizándoles por las promesas que hayan realizado. Si ellos no están preparados para apoyar mejoras tendientes a proteger la privacidad de los estudiantes, pídeles que justifiquen por qué no lo están. Comparta cualquier respuesta que obtenga, ya sea positiva o negativa, con los padres preocupados y con los reporteros.



Llame la atención de los medios de comunicación

Busque la atención de los medios de comunicación si está organizando una reunión pública en la ciudad, movilización, manifestación o protesta, o simplemente si está abogando por una causa. Obtener la atención de los medios de comunicación es extremadamente útil para lograr su meta.

■ **SI USTED VA A REALIZAR** un evento, envíe a los reporteros una breve nota de prensa en el cuerpo de un correo electrónico una semana antes y un recordatorio el día anterior al evento, no más tarde de las 2 p.m. En el asunto, incluya la fecha del evento diciendo dónde, cuándo y qué. Asegúrese de agregar información como correo electrónico y número de teléfono de la persona que debe contactar para obtener más información. En el Anexo F encontrará un modelo con consejos útiles que puede usar para escribir su propia nota de prensa. Envíe por correo electrónico la nota de prensa (sin anexos) a la Prensa Asociada (Associated Press) a info@ap.org, y contacte a la recepción regional para que le indiquen a donde enviar el fax o correo electrónico: <http://www.ap.org/contact-us/bureaus>

Escoja notas textuales y titulares que sean claros, simples, atractivos, fuertes, emocionales y que agreguen valor a la historia.

■ **DURANTE EL EVENTO**, pida a un amigo que tome fotos y/o grabe un video, y publíquelos en línea en sus cuentas de medios sociales electrónicos y en YouTube, Facebook, Twitter, Flickr, etc. Con anterioridad, aclare a los participantes que usted está grabando y que es posible que comparta la grabación del evento más ampliamente con miembros del público; y permita a los presentadores que opten por no ser grabados, si así lo prefieren.

■ **DISTRIBUYA UN BOLETÍN DE PRENSA** a los reporteros después del evento. El boletín debe ser un documento de una o dos páginas que describa brevemente el evento, a los participantes y la cuestión que se está discutiendo. Si puede, incluya citas textuales y titulares. Vea el Anexo F donde encontrará un modelo con consejos útiles que puede usar para escribir su propio boletín.

■ **ENVÍE EL BOLETÍN DE PRENSA** después del evento a los reporteros, padres, oficiales y a aquellos que no pudieron asistir.

■ **EN GENERAL**, es importante conocer a sus reporteros locales, para que pueda aprovechar cualquier noticia de última hora que se relacione con la privacidad del estudiante. Aprovechar una noticia que se está dando en el momento, es la mejor oportunidad para atraer más atención a su cuestión y punto de vista. Prepare con anticipación un buen titular que resuma su perspectiva en unas cuantas palabras o frases. Una vez que un reportero sabe que usted está interesado en el tema, puede contactarle buscando información relevante en la siguiente ocasión que el tema salga a relucir en las noticias.

No exagere en el uso de la lista de correos electrónicos de la prensa, o los reporteros empezarán tratar su mensajes como correo "no deseado" (spam).

■ **ESCRIBA CARTAS** al editor; y no olvide escribir a los periódicos comunitarios.

CONSEJOS PARA ESCRIBIR UNA CARTA AL EDITOR:

1. Las cartas al editor que más se publican son aquellas que responden a un tema que ha sido cubierto recientemente en la publicación, así que manténgase vigilante de las historias o noticias que aparezcan con relación a la privacidad del estudiante, incluyendo las violaciones cibernéticas.
2. Cuando encuentre una historia o noticia relevante, investigue las reglas para enviar cartas específicamente a esa publicación. Algunas limitan el número de palabras a 200-250 para mantener la brevedad de la carta.
3. Preséntese a sí mismo y explique por qué le preocupa el tema. Presente un argumento convincente o persuasivo que incluya hechos o detalles. Las cartas al editor con relevancia local tienen más oportunidad de ser publicadas.
4. Dé a conocer su punto incluyendo información importante para los lectores de la publicación y termine con un llamado a la acción (ej.: firmar mi petición).
5. No olvide firmar la carta con su nombre y apellido, y proporcionar su correo electrónico y número de teléfono.

Para más consejos, vea la caja de recursos para promover una causa de la Sociedad Internacional para la Tecnología en la Educación (International Society for Technology in Education advocacy toolkit) en http://bit.ly/SPTK_OpEds ² y asegúrese de contactar a la Coalición de Padres para la Privacidad del Estudiante (Parent Coalition for Student Privacy) en info@studentprivacymatters.org. ¡Quizás le podamos ayudar!

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. <http://www.studentprivacymatters.org/>
<http://www.commercialfreechildhood.org/>
<https://www.eff.org/>
<http://networkforpubliceducation.org/>
<https://epic.org/>
<http://parentsacrossamerica.org/>
<https://www.aclu.org/>
2. <http://www.iste.org/docs/pdfs/iste-advocacy-toolkit---letter-to-the-editor.pdf>

SECCIÓN VII.

Preguntas frecuentes sobre la privacidad del estudiante

Enseguida presentamos algunas respuestas a las preguntas más frecuentes sobre la privacidad del estudiante. Exhortamos a los padres de familia a que consulten la caja de recursos completa para obtener más información. Si no puede encontrar lo que está buscando, envíe un correo electrónico a info@studentprivacymatters.org. ¡Haremos nuestro mejor esfuerzo para responder a sus preguntas!

P: ¿Qué es FERPA y qué archivos protege?

R: La Ley de Privacidad y Derechos Educativos Familiares (FERPA) [Family Educational Rights and Privacy Act], fue aprobada en 1974 para proteger la privacidad de los “archivos educativos” de los estudiante en las escuelas y universidades que reciben fondos federales. Los archivos educativos se definen como aquellos que “(1) se relacionan directamente con un estudiante; y (2) son retenidos por una agencia o institución educativa o por un tercero actuando a nombre de la agencia o institución”. Para más información vea la Sección II.

P: ¿Bajo qué circunstancias pueden compartirse los contenidos de los archivos educativos de mi hijo sin el consentimiento de los padres?

R: En los últimos años FERPA se ha suavizado a través de la regulación, permitiendo a las escuelas revelar a terceros información personal contenida en los archivos educativos de su hijo, bajo una variedad de circunstancias. Para una explicación de estas circunstancias vea la Sección II.

P: ¿Se puede compartir la información personal de mi hijo con cada uno de los empleados dentro de la escuela?

R: No. La información personal del estudiante puede ser compartida únicamente con aquellos miembros del personal de la escuela que son directamente responsables de la educación o servicios de su hijo, y solo se debe compartir la información estrictamente necesaria para que ellos cumplan con sus deberes profesionales.

P: ¿Puede mi escuela o distrito compartir la información de mi hijo con el departamento de educación del estado sin el consentimiento de los padres?

R: Sí. La mayoría de las escuelas y/o distritos reportan regularmente un cierto nivel de información del estudiante al departamento de educación del estado; algunos de estos datos pueden requerir que cumplan con las provisiones de rendición de cuentas delineadas en la ley estatal o federal. Otra obtención de datos puede ser meramente discrecional por parte del estado. La información del estudiante enviada por las escuelas al estado, típicamente es almacenada en el Sistema Estatal de Datos Longitudinales (SLDS-Statewide Longitudinal Data System) y éste puede estar enlazado con datos de otras agencias estatales, incluyendo servicios de salud y servicios humanos, educación superior, trabajo, correccionales y seguridad pública. La información contenida en el SDLD puede entonces estar disponible para los investigadores y hacedores de políticas públicas, si el estado así lo decide. Casi cada estado en la nación tiene un SLDS; la meta del programa SLDS es seguir y monitorear a los estudiantes desde pre-escolar hasta la escuela preparatoria, colegio y más allá.

¿QUÉ DATOS DEL ESTUDIANTE ESTÁN EN EL SLDS DEL ESTADO?

Cada estado en la nación, con excepción de Wyoming, Nuevo México y Alabama, recibe subvenciones federales de financiamiento, del Departamento de Educación de los EE.UU., para desarrollar o sostener un SDLS. Los estados que reciben fondos deben adoptar en sus sistemas de datos los siguientes requisitos mínimos:

1. Un identificador único para cada estudiante, que permita que el estudiante no sea identificado individualmente (excepto como lo permite la ley estatal y federal);
2. La historia de inscripciones de la escuela, características demográficas y archivos de participación en programas de cada estudiante;
3. Información sobre cuándo se inscribe un estudiante, se transfiere, se da de baja o se gradúa de una escuela;
4. Los resultados de los estudiantes en las pruebas estatales conforme lo requiere La Ley de Educación Primaria y Secundaria (Elementary and Secondary Education Act);
5. Información por grado escolar y tema del curso, sobre los estudiantes que no realizan pruebas;
6. Resultados de las pruebas que midan si el estudiante está o no listo para ingresar al colegio;
7. Una forma de identificar a los maestros y enlazarlos con sus estudiantes;
8. Información de los expedientes educativos, específicamente los cursos tomados y los grados obtenidos;
9. Datos sobre el éxito de los estudiantes en el colegio, incluyendo si se inscribieron en cursos de recuperación;
10. Datos que revelen si los estudiantes de pre-escolar hasta el grado 12 están preparados para tener éxito en el colegio;
11. Un sistema para auditar los datos en términos de calidad, validez y confiabilidad; y
12. La habilidad para compartir datos entre los sistemas de información desde pre-escolar hasta la educación post-secundaria.

NOTA: Muchos SLDS estatales contienen información específicamente para identificar a los estudiantes incluyendo nombres, direcciones, diagnósticos de discapacidades y hasta detalles de suspensión.

Entérese qué tanto financiamiento de subvenciones federales recibió su estado para desarrollar o mantener un Sistema Estatal de Datos Longitudinales (SDLS) en http://bit.ly/SPTK_SLDS¹ y aprenda detalles sobre el SLDS de su estado en <http://www.workforcedqc.org/state-solutions>

P: ¿Puedo tener acceso a la información contenida en el archivo educativo de mi hijo? ¿Qué debo hacer si la información es incorrecta?

R: Sí. FERPA garantiza que los padres tengan la oportunidad de inspeccionar los archivos educativos de su hijo dentro de los siguientes 45 días después de sometida la solicitud, ya sea que dichos archivos estén en posesión de la escuela, el distrito o el estado. La escuela o agencia educativa no le puede aplicar una cuota de pago por buscar o sacar dichos archivos, pero sí le puede aplicar una cuota mínima por hacerle copias de los documentos. FERPA también le da el derecho de corregir la información contenida en los archivos de su hijo, si usted cree que es “incorrecta, engañosa o está violando los derechos de privacidad del estudiante”. Vea la Sección II para mayor información sobre sus derechos para tener acceso y corregir o comprobar la información en un archivo educativo.

P: ¿La información médica de mi hijo está incluida en su archivo educativo? ¿Esta información está protegida por HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico- Health Insurance Portability and Accountability Act)?

R: En la mayoría de los casos, la información médica que usted y su hijo proporcionan a la escuela, así como los registros hechos por la enfermera escolar, consejero o clínica de salud operada por la escuela, pasan a ser parte del archivo educativo y están cubiertos por FERPA y no por HIPAA. Los servicios de apoyo y discapacidad que recibe un estudiante de educación especial son también

parte de su archivo educativo y puede ser revelado sin el consentimiento de los padres bajo las condiciones o excepciones que se mencionaron en la Sección II.

En términos generales, las escuelas no necesitan cumplir con HIPAA (también conocida como “Regla de Privacidad”) porque no son consideradas “entidades cubiertas” bajo la ley, como sí lo son los planes de salud, las redes de servicios de salud y los proveedores de servicios de salud. A pesar de eso, usted debe preguntar a su escuela quien tiene acceso a los registros médicos, de discapacidad y de consejería y promover que esta información esté resguardada dentro de la escuela y que su revelación fuera de la escuela se limite lo más posible. Para aprender más sobre HIPAA en la escuela, visite http://bit.ly/SPTK_HIPAA ²

P: Si yo envío un correo electrónico sobre un asunto confidencial, al maestro de mi hijo ¿esta información se incluirá en el archivo educativo de mi hijo?

R: Es posible. Si usted tiene un asunto sensible que quiere discutir con el maestro de su hijo, le sugerimos que programe una reunión cara a cara para discutir sus preocupaciones. Cualquier cosa por escrito que usted comparta -notas escritas a mano o comunicación por correo electrónico- pueden formar parte del archivo educativo de su hijo.

P: ¿Está protegida por FERPA la información digital de mi hijo obtenida a través de las aplicaciones (apps) de salón de clases o programas en línea?

R: Depende de muchos factores incluyendo, pero no limitándose a, qué información del estudiante, la aplicación de salón de clase o programa en línea recoge y/o mantiene, y cómo usa y comparte dicha información. FERPA se volvió una ley en 1974, mucho tiempo antes de que la tecnología fuera tan utilizada en nuestros salones de clases. Aunque el Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. (PTAC-U.S. Department of Education's Privacy Technical Assistance Center) ha intentado proporcionar algunas directrices sobre este tema, se les aconseja a las escuelas y los distritos que evalúen “cada caso en particular” para saber si FERPA se puede aplicar. Hasta que la ley federal no sea actualizada y fortalecida para proteger la información estudiantil –digital o no– nosotros ofrecemos en la Sección IV recomendaciones importantes que usted puede compartir con su escuela, distrito y/o estado.

P: El maestro de mi hijo o director de la escuela me dijo que la aplicación del salón de clases y el programa en línea que se usan en mi escuela cumplen con FERPA. ¿Qué quiere decir eso?

R: Esa aseveración no debe reafirmarle que la información de su hijo está bien protegida o se mantiene privada. FERPA permite una revelación amplia de información personal contenida en los archivos estudiantiles, sin el consentimiento de los padres, como se describió en la Sección II y la ley no requiere estándares mínimos para protección de seguridad de los datos. Además, FERPA regula las prácticas de las escuelas que reciben fondos federales; y no regula directamente las acciones de los operadores en línea o vendedores privados. Si un vendedor u operador utiliza la información estudiantil para un propósito que no está autorizado, los padres deben responsabilizar a los oficiales educativos locales para que mantengan una supervisión estricta y detengan dicha práctica. Para más información sobre buenas prácticas, refiérase a la Sección IV.

P: ¿Cómo se castiga una violación de FERPA?

R: Si se encontrara que una escuela está violando FERPA, puede ser que el financiamiento federal se retenga. Sin embargo, el gobierno federal nunca ha hecho esto en los 43 años de historia de FERPA. Además, el Departamento de Educación de los EE.UU. puede prohibir a los terceros en cuestión, que reciban información personal estudiantil hasta por cinco años, si encuentra que vuelven a divulgar información del estudiante, violando de nuevo FERPA. Si una organización no destruye la información del estudiante después de que ya no es necesaria, con propósitos de un “estudio”, es posible que también se le prohíba recibir información estudiantil, hasta por cinco años.

P: ¿Es permitido por la ley que el maestro inscriba a mi hijo, sin mi consentimiento, en aplicaciones de salón de clases o programas en línea?

R: Bajo la excepción “oficial escolar” FERPA permite que su maestro use la información personal del archivo educativo de su hijo para crear una cuenta en línea, sin su consentimiento. También esto se puede hacer con un conjunto más limitado de información del estudiante, usando la excepción de “información de directorio.” Sin embargo, si su hijo es menor de 13 años y él mismo está ingresando información personal dentro de un programa en línea dirigido a niños, ya sea en la escuela o en la casa, podría aplicar la ley federal COPPA (Ley de Protección de la Privacidad en Línea de los Niños-Children’s Online Privacy Protection Act). El maestro puede consentir que su hijo use una herramienta educativa en línea, si cualquier información personal recogida por el operador o vendedor en línea, no es usada con propósitos comerciales. Es responsabilidad de la escuela, distrito o estado asegurar que el vendedor u operador use la información del estudiante solo para los propósitos especificados y que la asegure suficientemente. Como se mencionó en la Sección IV, recomendamos que ningún maestro inscriba a los estudiantes en programas en línea sin un examen cuidadoso del programa a nivel escolar, distrital o estatal.

MÁS INFORMACIÓN SOBRE COPPA EN LAS ESCUELAS

Para que un maestro/escuela proporcione el consentimiento a nombre de un padre de familia, el operador de la aplicación del salón de clases o programa en línea debe proporcionar a la escuela todas las notificaciones que requiere COPPA.

Además, una vez que la escuela lo solicite, el operador debe proporcionar a la escuela:

1. Una descripción de los tipos de información personal de los estudiantes que se recopilará;
2. La oportunidad de revisar la información personal del estudiante y/o hacer que se borre la información; y
3. La oportunidad de evitar la recopilación en línea o un uso más allá del necesario de la información personal del niño.

Para más información sobre los derechos de los padres ante COPPA, vea la Sección II.

P: ¿Pueden las escuelas o las compañías a las que se les permite recopilar información vender la información personal del estudiante?

R: Varias leyes estatales, incluyendo la histórica ley de California del 2014 llamada SOPIPA (Ley de Protección de Información Personal del Estudiante en Línea- Student Online Personal Information Protection Act), prohíbe a las compañías que recopilan datos a través de sus servicios educativos en línea, que vendan dicha información del estudiante – excepto cuando la compañía del vendedor u operador es adquirida por otra compañía, en cuyo caso el nuevo vendedor u operador debe cumplir con las previsiones de privacidad establecidas por la ley. SOPIPA y algunas otras leyes estatales prohíben también el uso de información personal del estudiante para publicidad dirigida.³

FERPA prohíbe a las compañías designadas como “oficiales escolares” que usen la información de los estudiantes por cualquier razón que no sea aquella para la que originalmente fue autorizada, a menos que el padre o el estudiante elegible haya dado su consentimiento para un propósito adicional. Esto significa que la compañía no puede hacerlo, a menos que la escuela haya autorizado a la compañía para que use los datos de los estudiantes para anuncios dirigidos, supuestamente con propósitos educativos, o con el consentimiento del padre o el estudiante elegible. Sin embargo, FERPA no permite la divulgación de la “información de directorio” sin limitaciones, incluyendo el mercadeo hacia los estudiantes y la venta de información a otros. Vea la Sección II, para conocer más sobre la información de directorio y cómo optar por no proporcionar dicha información.

COPPA evita que los vendedores u operadores de aplicaciones o sitios de Internet dirigidos a niños, usen la información personal que se recopila directamente de un estudiante menor de 13 años, con propósitos comerciales, como el mercadeo o compartir la información con otras compañías con dicho propósito, a menos que uno de los padres dé su consentimiento.

La Enmienda de Protección de los Derechos del Alumno (PPRA) [The Protection of Pupil Rights Amendment] requiere que las escuelas notifiquen a los padres y les permitan la opción de negarse, cuando los estudiantes están “programados para participar en actividades que involucren la recopilación, divulgación o uso de información personal obtenida de los estudiantes con propósito de mercadeo, o para vender o proporcionar de otra manera información a otros, también con propósitos de mercadeo”. Sin embargo, PPRA permite a las compañías, vendedores y operadores que usen la información personal de los estudiantes para el “propósito exclusivo de desarrollar, evaluar o proporcionar productos o servicios educativos para los estudiantes o las escuelas”.

P: ¿Las compañías que ofrecen exámenes de admisión para el colegio, por ejemplo el College Board (PSAT/SAT) y ACT, venden la información que mi hijo les proporciona voluntariamente?

R: Sí. Quizás usted haya notado una casilla para marcar que es parte de la forma de registro en línea para el PSAT, SAT o ACT, donde le preguntan si usted o su hijo optan por compartir su información con los colegios y programas de becas. Durante el día del examen, se le puede animar a su hijo para que marque esa casilla y proporcione más información. Si usted o su hijo marcan esa casilla aceptando, el perfil personal de su hijo puede que sea vendido con propósitos de mercadeo o decisiones de admisión a los colegios u otras organizaciones elegibles. Para proteger la privacidad de su hijo, le recomendamos que usted o su hijo no proporcionen información personal ajena al ACT o Consejo de Colegios (College Board).

NOTA: Si usted ya optó por compartir la información de su hijo a través del Servicio de Búsqueda del Estudiante del Consejo de Colegios (SAT) [College Board -SAT- Student Search Service], es posible que si cambia de opinión, revoque su permiso visitando el siguiente enlace: <https://student.collegeboard.org/student-search-service/opt-out>

P: Mi hijo me dijo que hizo una encuesta en la escuela en la que le hacían varias preguntas personales. ¿Está eso permitido?

R: Ante PPRA, se debe obtener el consentimiento de los padres por escrito antes de que se le pueda pedir a un niño que conteste una encuesta, análisis o evaluación financiada federalmente, que haga preguntas relacionadas con afiliaciones políticas, creencias religiosas, conducta sexual y actitudes y otros temas delicados. Si la encuesta hace preguntas sobre ese tipo de cuestiones personales, pero no está financiada federalmente, los padres deben ser notificados con anterioridad y se les debe dar la opción de negarse a que sus hijos realicen la encuesta. Para más información sobre PPRA y el tipo de preguntas que regula, vea la Sección II.

P: ¿La escuela tiene la obligación de informar a los padres cuando hay una violación de los datos de los estudiantes?

R: Ninguna de las leyes de privacidad federales (FERPA, COPPA, PPRA) requieren que las escuelas informen a los padres cuando la información de los estudiantes ha sido interceptada. Sin embargo, algunas leyes estatales requieren dicha notificación. Además, FERPA requiere que las escuelas mantengan en el archivo educativo del estudiante un archivo adicional que contenga cualquier divulgación sin autorización, tales como las violaciones de datos y deben poner esta información a disposición de los padres que lo soliciten. Vea la Sección II para más información. Conforme aumentan los incidentes de violación de los datos en la educación, urgimos a los padres para que promuevan y aboguen por reglas más estrictas de divulgación de violaciones, a nivel de la escuela, del distrito y del estado.

P: ¿Es cierto que los reclutadores del ejército pueden obtener la información personal de mi hijo directamente de la escuela preparatoria? ¿Puedo negarme a autorizar que la escuela proporcione dicha información?

R: Sí. Bajo la Sección 9528 de Que Ningún Niño Se quede Atrás (NCLB) [No Child Left Behind] y bajo la Sección 8025 de la Ley Cada Estudiante Trieunfa (ESSA) [Every Student Succeeds Act], los reclutadores militares pueden solicitar acceso a la información de contacto de los estudiantes. Los padres pueden optar por negarse a esta divulgación, enviando a la escuela o distrito un formulario de negación por escrito; vea el Anexo C que contiene un modelo de carta.

P: ¿Qué son los “datos para publicar en muros” y bajo que circunstancias se prohíben?

R: Los datos para publicar o exponer en muros son tablas que los maestros usan para publicar los resultados de las pruebas de los estudiantes y/o su progreso en un tema o habilidad. FERPA generalmente prohíbe la revelación, sin el consentimiento de los padres, de esa información personal del estudiante a los oficiales no escolares. Si la información incluida en los datos expuestos en muros incluye el nombre del estudiante y otra información de identificación, como la identificación del estudiante (ID), junto con las calificaciones o los resultados de las pruebas y es visible a cualquier empleado no escolar en una área semi-pública, como un salón de clases o un pasillo y se publica sin el consentimiento de los padres, entonces está violando FERPA.

¿PUEDEN LOS DATOS CONTRIBUIR A LOS ESTEREOTIPOS?

Antes de que inicie la escuela, los maestros pueden ver los detalles del archivo académico del estudiante, incluyendo sus calificaciones, asistencia, resultados de exámenes y registros disciplinarios a través de “datos expuestos en muros” o a través de una interfaz en línea llamada “tablero de datos.” Los estudiantes con historias positivas pueden beneficiarse de un fenómeno denominado “Efecto Pigmalión”, donde los maestros tendrán expectativas más altas de tales estudiantes, y les conducirán a una ejecución mejor. Los estudiantes con historias pobres pueden sufrir del llamado “Efecto Golem” donde los maestros tendrán expectativas más bajas para ellos, conduciéndoles a una ejecución más pobre.⁴

P: ¿Qué puedo hacer si creo que los derechos de mi hijo han sido violados?

R: Si usted cree que los derechos de su hijo han sido violados ante cualquier ley federal, incluyendo FERPA, PPRA o COPPA, debe notificar a su escuela, al Superintendente del distrito, y/o al consejo escolar, tan pronto como le sea posible. Si ellos se rehúsan a tomar las acciones apropiadas, usted puede contactar al capítulo local de la Unión Estadounidense por las Libertades Civiles (ACLU) [American Civil Liberties Union] para solicitar ayuda o someter una denuncia. Vea la Sección II para obtener detalles de cómo realizarlo.

¿Necesita ayuda? ¡Contacte a la Coalición de Padres por la Privacidad del Estudiante (Parent Coalition for Student Privacy) en info@studentprivacymatters.org y le conectaremos con otros grupos de apoyo y/o recursos!

Limitación de responsabilidad: Aunque la meta de la Coalición de Padres por la Privacidad del Estudiante y la Campaña por una Infancia Sin Comerciales (Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood) es proporcionar recursos valiosos para ayudarle a proteger la privacidad del estudiante, nuestras sugerencias y recomendaciones no deben reemplazar los consejos legales de un abogado. Si tiene preguntas de cómo se pueden aplicar a su situación particular las leyes y políticas locales, estatales y federales, puede buscar el apoyo de un abogado con licencia contactando al servicio de referencia de la asociación local de abogados.

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. <https://nces.ed.gov/programs/slds/stateinfo.asp>
2. <https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html>
3. https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf
4. <http://www.oxfordbibliographies.com/view/document/obo-9780199846740/obo-9780199846740-0014.xml>

ANEXO A.

Solicitud para inspeccionar los archivos educativos que están en posesión de la escuela, el distrito o el estado

Yo entiendo que la Ley Federal de Privacidad y Derechos Educativos Familiares (Federal Education Rights and Privacy Act –FERPA–), es una ley federal que otorga a los padres el derecho de inspeccionar la información contenida en los archivos educativos de sus hijos, que es recopilada y que está en posesión de la escuela, el distrito o el estado. De acuerdo al Departamento de Educación de los EE.UU., los archivos educativos “incluyen, pero no se limitan a calificaciones, expedientes académicos, lista de clases, horarios de cursos del estudiante, archivos de salud (en el nivel pre-escolar hasta el grado 12), información financiera (en el nivel de post- secundaria), y archivos de disciplina del estudiante. Esta información pudo haberse recopilado en cualquier formato, incluyendo, pero sin limitarse a: escritos a mano, información impresa, medios computacionales, videos, audios, películas, microfilmes, microfichas, y correo electrónico”. **Fuente:** 34 CFR § 99.3 “Archivos Educativos” y “Archivos” (34 CFR § 99.3 “Educación Records” and “Record”).

Además comprendo que la escuela o el distrito pueden no cobrar una cuota por la búsqueda u obtención de los archivos escolares, pero que si puede aplicar una cuota razonable por la entrega de copias de los archivos educativos. Dichas copias deben entregarse en un formato legible dentro de los siguientes 45 días de recibida la solicitud.

Por lo anterior, favor de aceptar esta solicitud para acceder a toda la información personal identificable en los archivos educativos de mi hijo, incluyendo los archivos que se le requiere a usted que almacene y proporcione ante las solicitudes de información personal de mi hijo, realizadas por parte de organizaciones que hacen estudios para o en nombre de la escuela y de las autoridades educativas locales, estatales o federales. Los archivos solicitados también deben incluir toda la información de mi hijo, que fue otorgada sin autorización, incluyendo aquellos casos de violaciones cibernéticas o pirateo de seguridad. **Fuente:** 34 CFR § 99.32 Requisitos para el Almacenamiento de Archivos (34 CFR § 99.32 Recordkeeping Requirements).

Por favor, infórmeme primero si estima que las cuotas por las copias de estos archivos serán más de [\$ _____].

NOMBRE DEL PADRE O TUTOR*: _____

NOMBRE DEL ESTUDIANTE: _____

GRADO ESCOLAR DEL ESTUDIANTE: _____ NÚMERO DE IDENTIFICACIÓN DEL ESTUDIANTE: _____

NOMBRE DE LA ESCUELA: _____

FECHA: _____

FIRMA DEL PADRE/TUTOR (SI EL ESTUDIANTE ES MENOR DE 18 AÑOS): _____

CORREO ELECTRÓNICO DEL PADRE O TUTOR: _____

DIRECCIÓN DE LA CASA DEL PADRE O TUTOR: _____

TELÉFONO DEL PADRE O TUTOR: _____

FIRMA DEL ESTUDIANTE (SI ES MAYOR DE 18 AÑOS): _____

* también llamado "Guardián legal"

ANEXO B.

Modelo de carta para optar por negarse a revelar datos de la “información de directorio”

Yo entiendo que FERPA (Ley de Privacidad y Derechos Educativos Familiares) [Family Educational Rights and Privacy Act], una ley federal, permite a mi escuela o distrito escolar que revele la “información de directorio” designada, a terceras personas sin mi consentimiento por escrito, excepto que yo informe lo contrario a mi escuela/distrito y de acuerdo a cualquier política y/o procedimiento existente.

Yo estoy sometiendo esta forma porque: [escoja una opción]

- ☐ La escuela o distrito escolar de mi hijo no tiene una política sobre la “información de directorio”.
- ☐ La política de la “información de directorio” existente de la escuela o distrito escolar de mi hijo no es suficiente para proteger la privacidad de mi hijo.

NOMBRE DEL PADRE O TUTOR*: _____

NOMBRE DEL ESTUDIANTE: _____

GRADO DEL ESTUDIANTE: _____

NÚMERO DE IDENTIFICACIÓN DEL ESTUDIANTE: _____

NOMBRE DE LA ESCUELA: _____

FECHA: _____

FIRMA DEL PADRE/TUTOR (SI EL ESTUDIANTE ES MENOR DE 18 AÑOS): _____

CORREO ELECTRÓNICO DEL PADRE O TUTOR: _____

FIRMA DEL ESTUDIANTE (SI ES MAYOR DE 18 AÑOS): _____

* también llamado "Guardián legal"

Información de directorio que YO PERMITO a la escuela o distrito que comparta:

(Nota: Marque sólo la información que USTED PERMITE a su escuela o distrito compartir)

- | | |
|--|---|
| ☐ Nombre del estudiante | ☐ Imágenes o videos electrónicos |
| ☐ Números de teléfono (ej.: casa, celular, etc.) | ☐ Fecha de nacimiento |
| ☐ Información personal de los padres (ej.: nombre, dirección, teléfono, correo electrónico, etc.) | ☐ Lugar de nacimiento |
| ☐ Fotografía | ☐ Dirección de casa o dirección permanente |
| | ☐ Dirección de correo electrónico |
| | ☐ Fechas de asistencia |
| | ☐ Peso/altura |

Caja de Recursos para Padres de Familia sobre la Privacidad del Estudiante

- | | |
|--|--|
| ☐ Estado de inscripción | ☐ Honores y reconocimientos recibidos |
| ☐ Grado escolar | ☐ Clubes/Afiliaciones |
| ☐ La escuela o institución educativa más reciente a la que asistió | ☐ Número de identificación (ID) emitida por la escuela o el distrito* |
| ☐ Participación en deportes y actividades reconocidas oficialmente. | |

***NOTA:** El número de identificación (ID) del estudiante puede o no, ser considerado como información del directorio, dependiendo de cómo lo use la escuela/distrito. Para más información, vea el sitio de Internet de Preguntas Más Frecuentes del Departamento de Educación de los EE.UU. en familypolicy.ed.gov/faq-page¹

YO PERMITO que los siguientes elementos de la información de directorio de mi hijo, y que están marcados arriba, sean compartidos, exclusivamente con las siguientes entidades:

- ☐ En publicaciones escolares o del distrito, incluyendo el libro anual, programa de graduación, programa de teatro, lista de la banda o del equipo de atletismo, boletín escolar y otras publicaciones como éstas.
- ☐ Con el Servicio Militar de EE.UU.
- ☐ Con colegios y otras instituciones educativas.
- ☐ Con posibles empleadores.
- ☐ Con oficiales políticos.
- ☐ Con el Centro Nacional de Información Estudiantil (National Student Clearinghouse).
- ☐ Con medios de comunicación.
- ☐ Con la PTA (Asociación de Padres y Estudiantes) [Parent Teacher Association] o la organización de padres del distrito.
- ☐ Con otros grupos o entidades fuera del distrito escolar, incluyendo organizaciones comunitarias, de abogacía y/o de padres de familia.
- ☐ Con compañías que venden servicios o productos.
- ☐ Con escuelas “charter” (charter school) o centros de correspondencia utilizados por escuelas “charter” para enviar a las familias materiales de reclutamiento.
- ☐ En sitios de Internet o cuentas de medios sociales oficiales relacionados con la escuela.
- ☐ En sitios de Internet o cuentas de medios sociales personales de los empleados de la escuela.
- ☐ Para inscribir a mi hijo en aplicaciones (apps) de salón de clases o herramientas educativas en línea.*

***NOTA:** FERPA permite a la escuela o distrito escolar que comparta sin el conocimiento o consentimiento de los padres o sin la opción de negarse a compartirlos, un gran rango de información personal del estudiante –más allá de la información de directorio– con individuos o compañías que ofrecen servicios operacionales, aplicaciones (apps) del salón de clases o herramientas educativas en línea, así como para propósitos de evaluación o investigación.²

REFERENCIAS

1. U. S. Department of Education, Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information. See <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html>

2. U.S. Department of Education, Privacy Technical Assistance Center, FERPA Exceptions - Summary. See https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf

ANEXO C.

Modelo de carta para optar por no ser reclutado por el ejército

NOTA: Esta forma es para ser usada exclusivamente por padres de estudiantes de preparatoria (high school).

Yo entiendo que la Sección 8025 de la Ley Cada Estudiante Triunfa (ESSA- Every Student Succeeds Act), que es una ley federal, me permite someter una solicitud por escrito a la escuela y/o al distrito escolar, para prohibir que se divulgue o se revele, sin mi consentimiento previo por escrito, cualquier información de mi hijo, incluyendo su nombre, dirección y número de teléfono, a cualquier reclutador del ejército de los EE.UU. ^{1,2} Note por favor que este documento constituye una solicitud formal por escrito, para prohibir la divulgación de la información antes mencionada.

NOMBRE DEL PADRE O TUTOR*: _____

NOMBRE DEL ESTUDIANTE: _____

NOMBRE DE LA ESCUELA: _____

NÚMERO DE IDENTIFICACIÓN DEL ESTUDIANTE: _____

NOMBRE DE LA ESCUELA: _____

FECHA: _____

FIRMA DEL PADRE/TUTOR (SI EL ESTUDIANTE ES MENOR DE 18 AÑOS): _____

CORREO ELECTRÓNICO DEL PADRE O TUTOR: _____

DIRECCIÓN DE LA CASA DEL PADRE O TUTOR: _____

TELÉFONO DEL PADRE O TUTOR: _____

FIRMA DEL ESTUDIANTE (SI ES MAYOR DE 18 AÑOS): _____

* también llamado "Guardián legal"

REFERENCIAS

1. Ver [[Página129 STAT. 2115]] <https://www.congress.gov/bill/114th-congress/senate-bill/1177/text#toc-H7549C9B976024930B024320484A07993>.
2. La Sección 8025 de la Ley Cada Estudiante Triunfa (ESSA) [Section 8025 of Every Student Succeeds Act], requiere que las escuelas y/o distritos escolares notifiquen a los padres de la escuela secundaria.

ANEXO D.

Preguntas adicionales para hacer al maestro o al director

Revise la Sección V donde encontrará una lista de preguntas iniciales que puede hacerle al maestro de su hijo. A continuación se presentan preguntas adicionales que puede realizar.

Preguntas que puede hacer sobre la información del estudiante que la escuela o el distrito recogen, usan y comparten

■ **¿QUÉ TIPO DE INFORMACIÓN RECOGE LA ESCUELA O EL DISTRITO** sobre los estudiantes y por qué? ¿Con quién se comparte? ¿Se notificará a los padres sobre qué información personal se recoge y comparte y si eso es considerado una buena práctica?¹

CONSEJO ÚTIL:

El Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. (U.S. Department of Education Privacy Technical Assistance Center) recomienda que las escuelas y/o los distritos deben:

- Desarrollar y publicar un inventario de datos, enlistando la información específica que se recoge de/sobre los estudiantes.
- Explicar por qué se recoge cada pieza de información del estudiante (ej.: para reportes federales o estatales, para proporcionar servicios educativos, para mejorar la instrucción, para administrar los servicios de cafetería, etc.).

■ **SI LOS DATOS SE ALMACENAN EN UN SISTEMA DE INFORMACIÓN ESTUDIANTIL (SIS)**, como InfiniteCampus o PowerSchool, ¿quién tiene acceso a los datos de mi hijo?, y ¿qué es lo que se les permite hacer con ellos? ¿solo sus maestros, consejeros y directores pueden ver la información o tienen acceso a ella otros maestros y oficiales de distrito? ¿y los individuos y organizaciones fuera de la escuela o del distrito?

■ **SI YO QUISIERA TENER ACCESO Y REVISAR** la información de mi hijo que está almacenada en sus archivos educativos, así como la información en el SIS, como parte de mi derecho ante la ley federal, ¿cómo puedo hacerlo?

■ **¿LA ESCUELA INFORMARÁ A LOS PADRES** cuando hay alguna violación de los datos de sus hijos, por parte de la escuela o el distrito? ¿cuáles métodos se usarán para informar a los padres, y qué tan rápido sucederá esto?

■ **¿CUÁNDO LA ESCUELA O EL DISTRITO BORRARÁN** la información personal de mi hijo? ¿una vez que se gradúe de la escuela preparatoria o si nos cambiamos de casa? ¿y se borrará toda la información o solo alguna de ella?

Preguntas sobre la información del estudiante que el distrito comparte con el departamento de educación del estado, el gobierno federal o investigadores

■ **¿EXACTAMENTE QUÉ INFORMACIÓN DEL ESTUDIANTE** se requiere que el distrito o la escuela compartan con el departamento de educación del estado?

■ **SI YO QUISIERA TENER ACCESO Y REVISAR** la información de mi hijo, conforme a mi derecho bajo la ley federal, ¿cómo puedo hacerlo?

■ **SI LA ESCUELA O EL DISTRITO PARTICIPA EN UN ESTUDIO** realizado por investigadores independientes o el Departamento de Educación de EE.UU., ¿ellos notificarán a los padres antes de compartir información personal del estudiante y explicarán por qué la información agregada o de-identificada no es suficiente para el estudio?

■ **SI USTED NO SABE** las respuestas a las preguntas anteriores, ¿a quién le puedo preguntar?

Preguntas sobre el uso que su hijo hace de programas en línea y aplicaciones de salón de clases (apps)

■ **¿CUÁLES APLICACIONES DE SALÓN DE CLASES** y programas en línea van a ser asignadas a mi hijo y cuáles son sus políticas de privacidad?

CONSEJO ÚTIL:

El Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU. recomienda que las escuelas y/o los distritos: "Proporcionen a los padres una lista de las aplicaciones o servicios educativos en línea que están aprobados para ser usados en el salón de clases".

■ **¿SABE USTED QUÉ INFORMACIÓN RECOGEN LOS VENDEDORES** sobre mi hijo?, ¿cómo se está usando y con qué otros contratistas o terceros pueden los vendedores estar compartiendo los datos?

■ **¿SE LE PERMITE AL VENDEDOR O CONTRATISTA** usar la información de mi hijo para propósitos de mercadeo? ¿mi hijo verá anuncios o publicidad como parte del programa? o ¿se enviará publicidad a mi hijo o a mí? Si es así, ¿cómo podemos negarnos a recibirlos?

CONSEJO ÚTIL:

Si su hijo es menor de 13 años, la ley federal conocida como COPPA requiere que su escuela conozca como usará la compañía la información privada de su hijo antes de que se le permita, en su nombre, suscribir a su hijo para usar la aplicación o programa en línea. Si la compañía usara la información privada de su hijo para cualquier propósito fuera del contexto educativo, la escuela (o el maestro) no puede inscribir a su hijo sin su permiso en esa aplicación del salón de clases.

■ **¿ESTOS PROGRAMAS HAN SIDO REVISADOS** por la escuela, el distrito o el estado en cuanto a su privacidad y seguridad? Si es así ¿cuáles son los criterios para su aprobación?

■ **SI NO ES ASÍ, ¿QUÉ ACCIONES HAN TOMADO PARA ASEGURAR** que la información de mi hijo esté a salvo de cualquier abuso o violación? y ¿para asegurar que esas aplicaciones cumplen con las leyes estatales y federales?

■ **¿CÓMO PUEDO YO TENER ACCESO, REVISAR Y/O SOLICITAR** que sea borrada la información privada de mi hijo que tienen esas compañías? y/o solicitar que sea borrada?

CONSEJO ÚTIL:

Las escuelas o distritos que designan a compañías como "oficiales escolares" y luego les revelan información personal identificable de los records estudiantiles, deben considerar sus obligaciones bajo la ley federal conocida como FERPA. De acuerdo al Centro de Asistencia Técnica para la Privacidad del Departamento de Educación de los EE.UU.: "Siempre que un proveedor mantenga archivos educativos estudiantiles, la escuela y el distrito deben poder proporcionar al padre solicitante (o el estudiante elegible) el acceso a esos archivos. Las escuelas y distritos deben asegurar que sus acuerdos con los proveedores incluyen cláusulas que permitan el acceso parental directo o indirecto".

■ **SI YO ME REHUSO A PERMITIR QUE MI HIJO USE** una o más de las aplicaciones de salón de clases o programas en línea, ¿qué formas educativas de instrucción y evaluación estarán disponibles para mi hijo?

■ **¿LA ESCUELA INFORMARÁ A LOS PADRES** cuando haya una violación de los datos del estudiante por parte de un proveedor de servicio o terceros? Si nos damos cuenta de que ocurrió alguna violación, ¿qué se hará para minimizar los impactos? ¿el vendedor tiene alguna responsabilidad para proporcionar monitoreo de crédito o congelamiento de crédito para aquellas familias afectadas?

CONSEJO ÚTIL:

También conocida como congelamiento de seguridad (securityfreeze), esta herramienta restringe el acceso a su reporte de crédito, lo que hace que sea más difícil para los ladrones de identidades que puedan abrir cuentas nuevas en su nombre. Esto es porque la mayoría de quienes proporcionan créditos, necesitan ver el reporte de su crédito antes de que puedan aprobar una cuenta nueva. Si ellos no pueden ver su reporte, puede ser que no extiendan su crédito.

Preguntas sobre programas de computación uno-a-uno (1:1) y de traer su propio dispositivo (BYOD)

■ **¿CUANDO SE USA UN DISPOSITIVO OTORGADO POR LA ESCUELA**, la escuela/distrito o la compañía que proporciona el dispositivo tiene acceso a los correos electrónicos de mi hijo, sus conversaciones de video, fotografías, documentos y otros contenidos? ¿la información de mi hijo se monitoreará, se recogerá o se grabará?

■ **¿PUEDE MI HIJO USAR SU PROPIO DISPOSITIVO?** Si es así, ¿qué información se recogerá o monitoreará por parte de la escuela?

■ **SI HAY CONFIGURACIONES PREDETERMINADAS** en los dispositivos proporcionados por la escuela para que obtengan datos de los estudiantes, ¿cómo podemos la escuela o yo cambiar dichas configuraciones?

CONSEJO ÚTIL:

Las escuelas y los distritos usan a menudo Chromebooks, pre cargados con Google's Suite G para Educación (Suite G), para sus programas 1:1. La Fundación Frontera Electrónica recomienda cambiar las configuraciones predeterminadas de Chromebooks y Suite G para mejorar la privacidad del estudiante. Las instrucciones paso a paso sobre como hacerlo se pueden encontrar en: <https://www.eff.org/issues/student-privacy/device-settings>

■ **¿LOS DATOS DE MI HIJO QUE SON** recopilados de los dispositivos proporcionados por la escuela se pueden de-identificar?

■ **¿LA ESCUELA/DISTRITO O TERCERO** que proporcione los dispositivos otorgados por la escuela, tienen acceso al dispositivo? Si es así, ¿quién tiene acceso al dispositivo de mi hijo –el administrador del sistema escolar, la gente que trabaja para los programas de la compañía, los administradores, los maestros o alguien más?

■ **¿PUEDE EL PROVEEDOR O LA ESCUELA** encender la cámara o audio del dispositivo proporcionado por la escuela? ¿Pueden ellos acceder remotamente los archivos y documentos o ver la pantalla del dispositivo?

CONSEJO ÚTIL:

Un distrito escolar de Pensilvania reconoció haber accedido remotamente las cámaras de las computadoras portátiles otorgadas por la escuela y que secretamente tomó fotografías de estudiantes en sus casas. El incidente de espionaje terminó en que el distrito pagó \$61,000 dólares para concluir varias demandas.²

■ **¿TIENE LA ESCUELA** acceso físico o remoto a las claves de mi hijo en el dispositivo?

■ **SI YO NO QUIERO** que mi hijo sea monitoreado o seguido, ¿Se respetarán mis deseos? Y aún así, ¿puede mi hijo participar en programas uno-a-uno o BYOD?

■ **LA ESCUELA USA** programas de monitoreo de ubicación, para monitorear la ubicación de los dispositivos proporcionados por ellos? Si es así, ¿quién puede acceder a la ubicación del dispositivo de mi hijo y bajo que circunstancias?

■ **¿HAY REGLAS ESPECIALES QUE APLICAN** si otros miembros de nuestra familia usan el dispositivo otorgado por la escuela?

■ **¿QUIÉN ES RESPONSABLE** si el dispositivo otorgado por la escuela se pierde o se daña?

Preguntas sobre el aprendizaje en línea en general

Estas preguntas han sido adaptadas de materiales desarrollados por Padres A Través de América (Parents Across America). Para aprender más al respecto, visite <http://parentsacrossamerica.org>

■ **¿CUÁNTO TIEMPO AL DÍA** mi hijo estará usando un dispositivo electrónico mientras está en la escuela?

■ **¿CUÁNTO TIEMPO ADICIONAL**, fuera del horario escolar, se le pedirá a mi hijo que use en un dispositivo electrónico?

■ **¿QUÉ TANTO LE CUESTA ESTE PROGRAMA** a la escuela o distrito?

■ **¿ESTÁ EL VENDEDOR PLANEANDO BENEFICIARSE** usando la información de mi hijo, ya sea por mercadeo u otros propósitos comerciales?

■ **POR CADA PROGRAMA ESPECÍFICO** agregado al dispositivo electrónico que mi hijo está usando, por favor, explique el propósito del mismo, la razón de su inclusión en el currículo y la evidencia de su efectividad.

Si usted no recibe respuestas suficientes a sus preguntas, considere abogar contra el uso excesivo de programas en línea, usando las estrategias delineadas en la Sección VI o considere negarse a que su hijo participe en uno o más de esos programas.

¿Preguntas? Visite www.studentprivacymatters.org/toolkit para más información, incluyendo seminarios en línea (webinars) gratuitos sobre cómo usar las herramientas contenidas en esta caja de recursos.

REFERENCIAS

1. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA%20Transparency%20Best%20Practices%20final_0.pdf

2. http://articles.philly.com/2010-10-12/news/24981536_1_laptop-students-district-several-million-dollars

ANEXO E.

Modelo de petición

Las peticiones son una herramienta muy poderosa para sus esfuerzos de abogacía o promoción de una causa. Pida a los padres de familia que firmen peticiones en papel o en línea para llamar la atención de la comunidad escolar, la prensa y de los tomadores de decisiones. Conserve los correos electrónicos de aquellos que firmen para que les mantenga informados y les involucre en esfuerzos que se están realizando para promover una causa. Asegúrese de resguardar la versión original de la petición y mandar copias a los tomadores de decisiones.

Modelo de petición

Para: Paul Harris, Superintendente de las Escuelas Unificadas de Smithville

Con copia para: Consejo Directivo de la Escuela Unificada de Smithville

Reginald Hayes, Alcalde de Smithville

Demandamos mejores protecciones de privacidad para los estudiantes de SUSD

A raíz de la violación que sufrió el programa educativo llamado Edufile, estamos demandando que el Distrito Escolar Unificado de Smithville (SUSD) deje de utilizar dicho programa y que inmediatamente siga los pasos necesarios para proteger la información personal del estudiante. Nos hemos dado cuenta que las políticas de seguridad y privacidad de SUSD no están actualizadas, y que no protegen adecuadamente dicha información contra violaciones, además de que no prohíben a los vendedores que usen la información personal del estudiante con propósitos comerciales, de publicidad o mercadeo.

La tecnología puede jugar un papel muy importante en la educación, pero no debe darse a expensas de la privacidad o la seguridad, y no debe usarse para anunciar aquello que distrae o disminuye la habilidad de aprendizaje. Urgimos al distrito para que adopte los Cinco Principios para la Privacidad del Estudiante como los articula la Coalición de Padres por la Privacidad del Estudiante (Parent Coalition for Student Privacy):

TRANSPARENCIA: Los padres deben ser notificados con anticipación, de cualquier divulgación de la información personal del estudiante a cualquier persona, compañía u organización fuera de la escuela o del distrito, así como de los contratos publicados o disponibles bajo demanda.

NO USOS COMERCIALES: Los datos personales del estudiante no deben ser usados con propósitos de negocios, de publicidad o mercadeo.

PROTECCIONES DE SEGURIDAD: Por lo menos, debe hacerse el cifrado de datos personales, el entrenamiento a todos los individuos que tengan acceso a los datos, y auditorías de seguridad realizadas por un auditor independiente.

DERECHOS DE LOS ESTUDIANTES/PADRES: Sin la notificación y el consentimiento de los padres, no debe permitirse la re-divulgación de información por parte de terceros, ya sean individuos, sub-contratistas u organizaciones.

MECANISMOS FUERTES DE APLICACIÓN: Se deben requerir multas y se debe permitir que los padres demanden legalmente en caso de que los vendedores violen los términos del contrato o de la ley.

Nombre	Escuela/Organización	Teléfono	Correo electrónico

ANEXO F.

Consejos para llegar a los medios de comunicación y ejemplos de materiales dirigidos a la prensa

Cuando se lleve a cabo una reunión pública u otro tipo de reunión para educar y abogar sobre cuestiones relacionadas con la privacidad del estudiante, no olvide invitar a la prensa, enviando una “nota de prensa”. ¡Use los consejos y ejemplos que se presentan a continuación para empezar a escribir su propia nota ahora mismo!

Cómo escribir una nota de prensa para los medios de comunicación

PASO 1: Empiece con la fecha del día actual.

PASO 2: Seleccione a la persona que será el contacto y quien responderá a las preguntas de los reporteros, incluya su nombre, número de teléfono y correo electrónico. Los otros miembros de su grupo pueden y deben hablar con la prensa, pero es mejor tener una persona encargada.

PASO 3: Escoja un título concreto y atractivo.

PASO 4: Escriba una descripción breve de su evento.

PASO 5: Agregue las “cinco preguntas” (ver ejemplo abajo).

PASO 6: Termine la nota con un recordatorio para los medios de comunicación interesados en conectarse con su contacto y proporcione detalles.

PASO 7: Coloque tres símbolos como éste # (###) al final de la nota.

PASO 8: Envíe la nota a los periódicos, televisoras y estaciones de radio locales, una semana antes del evento.

PASO 9: Dé seguimiento con llamadas telefónicas para asegurar que la nota fue recibida y preguntarles si enviarán a alguien a cubrir el evento.

PASO 10: Envíe la nota de nuevo, un día antes del evento, no más tarde de las 2 p.m.

NOTA: Usted puede enviar una nota de prensa en el cuerpo de un correo electrónico. Incluya la fecha del evento en “asunto”, diciendo qué y dónde.

Ejemplo de nota de prensa

Fecha: 20 de Octubre del 2017 Contacto: Lynn Jones, (555 -555-1212; lynn.jones1982@gmail.com)

Los padres de Smithville realizarán un Foro sobre la Privacidad del Estudiante

El Distrito Escolar Unificado de Smithville (SUSD) ordena cada vez más que sus estudiantes usen aplicaciones y programas en línea para realizar las tareas dentro de la escuela así como en la casa. Sin embargo, el Distrito no tiene un procedimiento para analizar las políticas de privacidad de esas aplicaciones. Aún más, el año pasado una de las aplicaciones usadas por los estudiantes de la escuela secundaria (middle school) de SUSD sufrió una violación cibernética (hacking). Los padres de Smithville pidieron a los oficiales de SUSD que organizaran un foro público para tratar las preocupaciones sobre privacidad,

pero se han negado a hacerlo. Es por eso que los *Padres de familia de Smithville por la Privacidad del Estudiante* organizarán su propio foro para discutir que es lo que SUSd puede hacer mejor para proteger la información personal del estudiante.

QUÉ: Foro sobre la Privacidad del Estudiante de Smithville.

QUIÉN: Hablarán Jill Brown, padre de familia; John Doe, Asesor de SUSd; Frank Allen, maestro de 4º año; y la Dra. Rhonda Little, una experta en privacidad del estudiante y Profesora de Ciencias Computacionales de la Universidad de Smithville.

DÓNDE: 100 Main Street, Smithville.

CUÁNDO: Martes, 12 de Abril, 2017 a las 7:00 p.m.

POR QUÉ: Las políticas actuales de SUSd no protegen de manera adecuada la información personal del estudiante.

Para más información o para organizaciones nuevas interesadas en asistir o cubrir este evento, contacte a Lynn Jones en 555-555-1212 o lynn.jones1982@gmail.com

###

Mientras que las notas de prensa son un adelanto para atraer a los medios y que cubran el evento, los boletines de prensa hablan sobre la historia completa y no necesariamente tienen que estar enlazados a un evento.

Ya que en ocasiones, los periódicos locales, citan directamente lo que el boletín de prensa dice, sin hacer ningún cambio, su boletín debe incluir todo lo necesario para contar su historia. También el boletín debe estar escrito de tal forma que capte la atención de los reporteros quienes querrán darle seguimiento y escribir sus propias historias.

Como escribir un Boletín de Prensa

PASO 1: Empiece con la fecha del día.

PASO 2: Seleccione a la persona que será el contacto y quien responderá a las preguntas de los reporteros, incluya su nombre, número de teléfono y correo electrónico.

PASO 3: Agregue la frase "Para ser publicado inmediatamente".

PASO 4: Escoja un título concreto y atractivo.

PASO 5: Mantenga el comunicado en un máximo de una página y media. Si está realizando un evento, describa brevemente los detalles del mismo y de los participantes y el tema a discutir. Incluya declaraciones textuales, escritas en tiempo pasado y algunos titulares. Si hay un evento de interés periodístico con el que usted pueda enlazar sus esfuerzos, como una violación de datos o la publicación de una investigación nueva sobre privacidad, puede eso hacer que su comunicado sea más llamativo. Incluya detalles importantes sobre cualquier contacto con expertos o con la escuela. El objetivo no es avergonzar a los oficiales de las escuelas o defraudar su confianza, sino demostrar a la prensa que usted ya ha comunicado a los oficiales sus preocupaciones. Incluya cualquier recomendación o demanda, tales como mejorar la política de privacidad o programar reuniones públicas.

PASO 6: Concluya con una frase fuerte.

PASO 7: Coloque tres símbolos como éste # (###) al final de su comunicado.

PASO 8: Envíe su comunicado de prensa después del evento a los periódicos, televisoras y estaciones de radio, así como a los padres, oficiales y otras personas que no pudieron asistir.

Ejemplo de Boletín de Prensa

Fecha: 20 de Octubre, 2017

Contacto: Lynn Jones, (555-555-1212; lynn.jones1982@gmail.com)

Para ser publicado inmediatamente

La Coalición demanda mejores protecciones de privacidad para los estudiantes de SUSD

SMITHVILLE, NC — A raíz de una reciente violación cibernética de los programas educativos (hacking) que dejó desprotegida la información personal de millones de estudiantes, una coalición de padres y maestros preocupados al respecto, están demandando que el Distrito Escolar Unificado de Smithville (SUSD) implemente inmediatamente los pasos necesarios para proteger la información personal del estudiante. La coalición afirma que las políticas de privacidad de SUSD no están actualizadas y no reflejan el creciente uso de aplicaciones y servicios utilizados por el distrito que se basan en la Nube.

“La tecnología puede jugar un papel muy importante en la educación, pero no debe darse a expensas de la privacidad”, dijo Phillip Grant, un padre de familia de Smithville High School. “En la actual era digital, los datos de nuestros estudiantes son un bien muy valioso y no me queda claro que SUSD esté tomando las precauciones necesarias para protegerlos contra la violaciones cibernéticas o el mal uso comercial”.

La coalición contactó primero a los oficiales escolares después de que los piratas cibernéticos se infiltraran en Edufile, un sistema basado en la Nube, que permite el acceso a los datos del estudiante a aquellos vendedores aprobados por el distrito. En febrero 18, un grupo de padres preocupados se reunieron con el Superintendente Paul Harris. Durante la reunión, se hizo aparente que las políticas de privacidad de SUSD eran deficientes y que ni siquiera prohíben el uso de aplicaciones que recogen información personal de los estudiantes, con propósitos comerciales.

“Me sorprendió descubrir que el programa en línea asignado a mi hija para hacer su tarea, estuviera recopilando un expediente de sus gustos e intereses” dijo Jill Brown, la madre de un estudiante de Smithville Middle School. “Yo entiendo que las aplicaciones gratuitas pueden ser atractivas para un maestro, pero no quiero que mi hija pague por su educación con su privacidad”.

La coalición está urgiendo al distrito para que adopte políticas que incorporen los principios de la Coalición de Padres por la Privacidad del Estudiante (Parent Coalition for Student Privacy), para proteger la privacidad de los estudiantes. Dichos principios están disponibles en <http://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/> e incluyen:

- **Transparencia:** Los padres deben ser notificados por la escuela o el distrito escolar de sus hijos con anticipación, de cualquier divulgación de la información personal del estudiante a cualquier persona, compañía u organización fuera de la escuela o el distrito. Toda revelación de información a terceros debe requerir también de políticas de privacidad y contratos disponibles públicamente, que especifiquen que tipo de información se va a revelar y con qué propósitos y proporcionar una fecha exacta en que dicha información se destruirá.
- **No usos comerciales:** La venta de datos personales del estudiante y/o el uso de ellos con propósitos de mercadeo debe ser prohibido. NO se debe permitir publicidad en los programas o sitios de Internet educativos que sean asignados a los estudiantes por parte de su escuela, ya que los anuncios son una distracción para el aprendizaje y no sirven para ningún propósito educativo.
- **Protecciones de seguridad:** Por lo menos, debe hacerse el cifrado de datos personales durante la actividad y la inactividad, debe darse entrenamiento a todos los individuos que tengan acceso a los datos personales del

estudiante, a los archivos de auditoría y a auditorías de seguridad realizadas por un auditor independiente. Las claves de seguridad deben estar protegidas de la misma forma que cualquier otra información personal del estudiante.

- **Derechos de los estudiantes/padres:** NO se debe permitir la re-divulgación de información por parte de terceros, a individuos adicionales, sub-contratistas u organizaciones, sin la notificación de los padres y el consentimiento de los padres o estudiantes (si tienen 18 años o más).

El Sr. Grant agregó: “Como padre de familia, yo debo tener el derecho de controlar quién tiene acceso a la información personal de mi hijo”.

#

RECURSOS ADICIONALES

Recursos sobre Leyes Federales que Protegen la Privacidad del Estudiante

LEY DE PRIVACIDAD Y DERECHOS EDUCATIVOS FAMILIARES (FERPA) [FAMILY EDUCATION RIGHTS AND PRIVACY ACT]: vea el sitio de Internet de la Oficina para el Cumplimiento de las Políticas Familiares del Departamento de Educación de los EE.UU. (U.S. Department of Education's Family Policy Compliance Office) en <https://studentprivacy.ed.gov/content/what-do-we-suggest>

ENMIENDA DE PROTECCIÓN DE LOS DERECHOS DEL ALUMNO (PPRA) [PROTECTION OF PUPIL RIGHTS AMENDMENT]: vea el sitio de Internet de la Oficina para el Cumplimiento de las Políticas Familiares del Departamento de Educación de los EE.UU. (U.S. Department of Education's Family Policy Compliance Office) en <https://studentprivacy.ed.gov/topic/protection-pupil-rights-amendment-ppra>

LEY SOBRE INDIVIDUOS CON DISCAPACIDADES EDUCATIVAS (IDEA) [INDIVIDUALS WITH DISABILITIES ACT]: vea el sitio de Internet de la Oficina de Educación Especial y Servicios Rehabilitativos del Departamento de Educación de los EE.UU. (U.S. Department of Education's Office of Special Education and Rehabilitative Services) en www2.ed.gov/about/offices/list/osep/osep-idea.html

LEY NACIONAL DE ALMUERZO ESCOLAR (NSLA) [NATIONAL SCHOOL LUNCH ACT]: vea el sitio de Internet del Servicio de Alimentos y Nutrición del Departamento de Agricultura de los EE.UU. (U.S. Department of Agriculture's Food and Nutrition Service) en www.fns.usda.gov/nslp/history__5

LEY DE PROTECCIÓN DE LA PRIVACIDAD EN LÍNEA DE LOS NIÑOS (COPPA) [CHILDREN'S ONLINE PRIVACY PROTECTION ACT]: vea el sitio de Internet de la Comisión Federal de Comercio (Federal Trade Commission) en www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Recursos para Padres y Promotores de la Causa

Para guías generales y recursos, vea el sitio de Internet del **CENTRO DE ASISTENCIA TÉCNICA PARA LA PRIVACIDAD DEL DEPARTAMENTO DE EDUCACIÓN DE LOS EE.UU. (PTAC-U.S. DEPARTMENT OF EDUCATION'S PRIVACY TECHNICAL ASSISTANCE CENTER)** en <https://studentprivacy.ed.gov/training/student-privacy-101>

Para más información sobre el **CENTRO DE INFORMACIÓN SOBRE LA PRIVACIDAD ELECTRÓNICA (EPIC) PROYECTO DE PRIVACIDAD DEL ESTUDIANTE (ELECTRONIC PRIVACY INFORMATION CENTER'S (EPIC) STUDENT PRIVACY PROJECT)**, visite epic.org/privacy/student

Para aprender más sobre la iniciativa **ESPIANDO A LOS ESTUDIANTES: DISPOSITIVOS ENTREGADOS POR LA ESCUELA Y LA PRIVACIDAD DEL ESTUDIANTE DE LA FUNDACIÓN FRONTERA ELECTRÓNICA (ELECTRONIC FRONTIER FOUNDATION'S (EFF) SPYING ON STUDENTS: SCHOOL-ISSUED DEVICES AND STUDENT PRIVACY)** y el reporte que lo acompaña, vea www.eff.org/issues/student-privacy

Para acceder a los recursos de **PADRES A TRAVÉS DE AMÉRICA (PARENTS ACROSS AMÉRICA)** sobre el “aprendizaje personalizado” y limitando el tiempo de los niños frente a una pantalla, visite parentsacrossamerica.org

UNIÓN ESTADOUNIDENSE POR LAS LIBERTADES CIVILES (ACLU) [THE AMERICAN CIVIL LIBERTIES UNION] promueve derechos de privacidad más fuertes para los estudiantes y otros; vea www.aclu.org/map/takectrl-nationwide-privacy-push

Recursos para compartir con escuelas y distritos escolares

EL CENTRO DE LEYES E INFORMACIÓN SOBRE POLÍTICAS PÚBLICAS DE LA ESCUELA DE LEYES DE FORDHAM (FORDHAM LAW SCHOOL'S CENTER ON LAW AND INFORMATION POLICY) ofrece un currículo para el salón de clases sobre la privacidad del estudiante en www.fordham.edu/info/24071/privacy_education

EL CONSORCIO DE REDES ESCOLARES (COSN) [CONSORTIUM OF SCHOOL NETWORKS], una asociación profesional para líderes escolares en tecnología, ofrece una caja de recursos para la seguridad y privacidad de los datos del estudiante en cosn.org/sites/default/files/CoSN-Privacy-Toolkit.pdf

EL CONSORCIO PARA LA PRIVACIDAD DE LOS DATOS DEL ESTUDIANTE (SDPC) [THE STUDENT DATA PRIVACY CONSORTIUM] es una colaboración de escuelas, distritos, agencias regionales y estatales que buscan soluciones a las preocupaciones de la privacidad de los datos del estudiante. Más información en: <https://secure2.cpsd.us/a4l>

Para evaluación de programas de computación educativos específicos y programas educativos visite COMMON SENSE MEDIA en www.commonsense.org/education/privacy

*Y no olvide nuestro sitio de Internet, Campaña por una Infancia Sin Comerciales
(Campaign for a Commercial-Free Childhood) en www.commercialfreechildhood*