



## STUDENT TECHNOLOGY ACCEPTABLE USE POLICY AND RELEASE OF DISTRICT FROM LIABILITY

Lake Tahoe Unified School District offers its educational community offer a wide range of technologies to support teaching and learning. The district aims to promote a learning environment that is respectful, secure, and responsible. This Technology Acceptable Use Policy provides students guidelines as to how this can be carried out in a digital context.

Use of district technology resources shall comply with federal and state laws and in accordance with the policies and procedures of LTUSD. This Student Technology Acceptable Use Policy also applies per California Education Code 48900 which describes a school's jurisdiction over student activity and discipline to include:

1. *While on school grounds.*
2. *While going to or coming from school.*
3. *During the lunch period whether on or off the campus.*
4. *During, or while going to or coming from, a school-sponsored activity.*

The advent of online learning spaces, particularly those managed by the school district (including Google's G-Suite) expands the concept of class time beyond the school campus. In fact, students may consider their use of district provided online accounts a school-sponsored activity so that their actions and behaviors while online using school accounts and interacting with their classmates do fall under the purview of this Acceptable Use Policy.

District technology includes, but is not limited to, District owned and/or district managed computing devices and peripherals (e.g., computers, laptops, tablets, removable storage devices, wearable technology, interactive classroom projection systems, etc.) District network and communication devices/services (telephones, wired and wireless networks including WiFi access points, emergency radios, email systems, file servers, etc.), and District managed online services (such as G-Suite, Aeries, etc.); access to online information sources; and future technological innovations.

Failure to adhere to this policy may result in discipline including loss of access, confiscation of a device, or up to and including expulsion in accordance with the student behavior and discipline policies. Students are expected to practice ethical behavior when using District and personal technology tools in all areas while refraining from harassment, academic dishonesty, and plagiarism. At the discretion of the school site, District administration, or in accordance with law, students may be disciplined for engaging in conduct deemed detrimental to the school and its mission, or harmful to other students. All aspects of this acceptable use policy apply whether District technology is accessed on or off campus and whether through District-owned or personally-owned devices. By using District managed technology tools and services, students and parents agree to the following stipulations:

1. By using District technology tools and services whether from personal or District-owned devices, students and parents grant specific consent, as defined by the California Electronic Communications Privacy Act (also known as Senate Bill 178), to the District to review and monitor all electronic communication information and electronic device information created with, stored on, or transmitted via District technology services.

2. Students and Parents acknowledge that the district may therefore monitor or access any and all student use of District technology without further specific advanced notice and that they have no expectation of any right to privacy while using district devices or network services, which includes, but is not limited to, any and all files and communications traveling over or stored on its network, or while using District provisioned accounts and online resources including email and online collaboration tools at any time.
3. Students agree to abide by the school's policies at all times, especially when using District technology tools and services. Students and Parents agree that any inappropriate use of technology while on campus or through district managed accounts off campus may result in school discipline.
4. Students understand that electronic devices are only permitted for educational uses while on campus. Students who play games, text message, or attempt to access social networking websites or applications during class time without the direction and supervision of a teacher may have the privilege to use District technology suspended or revoked. Repeated violations may result in more severe consequences
5. Parents agree that the district may act as an authorized agent for the creation of student online accounts solely for educational purposes in accordance to state and federal student information privacy laws (COPPA, FERPA, SOPIPIA, etc.). District managed student accounts may include, but are not limited to, online accounts created to access Google G-Suite (Google Apps for Education) and access to other apps, programs, or online services and digital curriculum resources.
6. The District holds the safety of its students in highest regard. However, the ability to share information and teach responsible digital citizenship is also vital to the educational process. This includes the use of e-mail, school learning management systems, online collaboration tools, classroom photo sharing services, and other social media avenues when applicable.
7. Parents and students understand that cellular phones and personal electronic devices outside of the district's managed 1-to-1 computer program may be brought to campus and used only under specific circumstances. Students who bring personal electronic devices to campus do so at their own risk and release the District from liability due to loss, damage, or theft of device, or loss of use of the device if confiscated. During class time, these devices may only be used under the direct supervision and instruction of a teacher or administrator. These devices may be used outside of class time in any manner not prohibited below.

The following activities or uses of technology are strictly prohibited to ensure a respectful digital learning environment:

- Using technology to threaten, bully, or harass others. This may include, but is not limited to, sending, accessing, uploading, downloading, or distributing text, images, or other materials that are offensive, threatening, profane, obscene, or sexually suggestive.
- Recording video or audio of other students or staff without their permission.
- Searching for, accessing, or possessing lewd, sexually suggestive, graphically violent, or derogatory/demeaning images and/or media files.

- Using District issued devices or network to search for and/or access repositories of illegal content, content that may cause harm to the District's network, or content that promotes, encourages, or teaches students how to commit an illegal act (i.e. bomb making, pirating electronic media, intentionally causing harm, etc.).
- Bypassing (or attempting to bypass) the District's internet content filter through a web proxy, anonymizers, or other means from a District or personal computing device.
- Circumventing network security measures or attempting to access confidential, private, or restricted information on the District's network or district managed online services.
- Sharing one's passwords or access to online accounts with anyone other than the student's parent or trusted adult.
- Logging into a device or service with the account of another student or a staff member or otherwise gaining access to their files and accounts without their permission.
- Sharing, publishing, or otherwise distributing confidential personal identification information, such as the name, home address, telephone number, Social Security number, financial details, or login credentials and passwords, of another student, staff member, or other person, with the intent to threaten, intimidate, harass, or harm that person.
- Destroying, damaging, defacing, or rendering unusable any property (both physical property like a computer, or virtual, such as a webpage) belonging to the District or another student or adult.
- Altering a district device's settings in a manner to cause confusion, frustration, or loss of use to other users (changing backgrounds, homepages, dock, network configurations, account logins, etc.).
- Using or installing viruses, malware, keyloggers, spyware, or other software/hardware that can be used to damage the District's network, harvest other users' login information, or propagate unwanted messages or files.
- Illegally downloading, storing, installing, or transmitting copyrighted materials without the proper license or permissions. The district explicitly forbids student use of torrenting software or services on the District network.
- Stealing others' intellectual property including text, music, movies, and software, or using them without the appropriate citation or expressed permission in accordance with Copyright Laws and Fair Use guidelines.
- Visiting social networking sites that are not directly used for educational purposes (including Facebook, Instagram, Twitter, Vine, etc.) during class time.
- Use of instant messaging or chat rooms not directly related to instruction (including texting, picture messaging, audio and video messaging) during class time.

## **Permanent Digital Footprint**

Students are reminded that anything they put online creates a permanent digital footprint that remains out of their control. Be mindful that the digital trail one creates for themselves and others is more like a tattoo which is almost impossible to completely erase. Apps, websites and software that claim to delete information may still leave a permanent record accessible to others. Students should not assume their online presence will remain private and should conduct themselves online expecting that any and all data they furnish could be accessible to a wider audience such as admissions officers and potential employers in the future.

## **Student Online Accounts and Opting Out**

As the District works to fulfill its mission of preparing students for the work force they will soon be entering, it will increasingly utilize tools and resources that are housed online and accessed through the internet. Online accounts are necessary to access web based file storage and collaboration tools such as Google Drive, Google Classroom, Google Docs, and District administered Google email as well as other educational web resources. These web and cloud based services permit online distribution and hand-in of student assignments, online based class discussions and collaboration activities, web based curriculum or learning resources, and in some grade levels, student email.

All District provisioned student accounts will be in compliance with state and federal student privacy requirements. In California, the Student Online Personal Information Protection Act SOPIPA (AB1584, SB1777, and AB1442) creates privacy standards for all online services catering to K-12 education in California and prevents them from advertising to students, building digital profiles about them, and/or selling harvested student information to other parties. The District believes these restrictions provide a safe environment for students to utilize accounts that are created by the District for accessing online educational resources and services.

The federal Child Online Privacy and Protection Act (COPPA) allows Local Education Authorities (LEA's) such as districts and schools to provide consent on the parent's behalf to create online accounts which may collect student information limited to the educational context and for no other commercial purpose. LTUSD operates under COPPA guidelines to create and manage student online accounts. By law, parents may choose to have their child opt out of this implied parental consent. This may be done in LTUSD by obtaining the Student Online Account Opt-Out Form from the school office, scheduling a conference with the school principal, and completing and signing the Opt-Out form in the presence of the principal who will counter sign receipt of the form after a discussion about the reasons for and the consequences of opting out.

Opting out of District managed online accounts for students would significantly impact a child's ability to participate in many class lessons and activities and would prevent students from learning state mandated digital citizenship principles and practicing responsible digital behaviors being taught in class. It might make it difficult for them to receive assignments, participate in online collaborative class projects, submit work back to their teacher, or access online lessons, digital textbooks, and online tutorials. Because the district's progressive use of technology to enhance learning is part of its core values, virtually all parents recognize the importance of allowing the district to carry out its mission to promote responsible digital citizenship and safe online practices and behaviors for all students through creating and maintaining student online accounts.

As part of the student's graduated digital citizenship training strategy students in grades K-8 will have limited email functionality which only allows them to send and receive emails with their teacher and other students within the District, but not the "outside world". Students in higher grades (9-12) may be granted more access to

send and receive emails with individuals and organizations outside of the District as needed, but all email communications may be monitored by the District.

**Student**

**Name:** \_\_\_\_\_

**School:** \_\_\_\_\_ **Grade:** \_\_\_\_\_ **Student ID:** \_\_\_\_\_

**Student Acknowledgment**

I have received, read, understand, and agree to abide by this Acceptable Use Agreement and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name: \_\_\_\_\_ Grade: \_\_\_\_\_  
(Please print)

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Parent or Legal Guardian Acknowledgment**

If the student is under 18 years of age, a parent/guardian must also read and sign the agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the Acceptable Use Agreement. By signing this Agreement, I give permission for my child to use district technology and/or to access the school's computer network and the Internet. I understand that, despite the district's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, district, and district personnel against all claims, damages, and costs that may result from my child's use of district technology or the failure of any technology protection measures used by the district. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting. If the device is damaged, due to abuse or neglect, or if the device and/or AC power adaptor is lost, the student must pay a loss/damage fee of up to \$200.00.

Name: \_\_\_\_\_ Date: \_\_\_\_\_  
(Please print)

Signature: \_\_\_\_\_

Exhibit LAKE TAHOE UNIFIED SCHOOL DISTRICT  
version: May 1, 2010 South Lake Tahoe, California  
revised: August 5, 2010  
revised: October 13, 2015  
revised: July 24, 2018



## POLITICA DE ACEPTACION DEL USO DE LA TECNOLOGIA DE LOS ESTUDIANTES Y FORMA DE LIBERACION DE RESPONSABILIDAD DEL DISTRITO.

El Distrito Unificado Escolar de Lake Tahoe ofrece a su comunidad educativa una amplia gama de tecnologías para apoyar la enseñanza y el aprendizaje. El Distrito pretende promover un ambiente de aprendizaje que sea respetuoso, seguro y responsable. Esta Política de Uso Aceptable de Tecnología provee a los estudiantes reglas de como esto puede ser llevado a cabo en un contexto digital.

El uso de los recursos tecnológicos del distrito debe acatar las leyes federales y estatales de acuerdo a las políticas y procedimientos de LTUSD. Esta Política de Uso de Aceptable de Tecnología Estudiantil también se aplica por el Código Educacional de California 48900 en el cual describe la jurisdicción escolar sobre la actividad y la disciplina de los estudiantes para incluir:

1. *Cuando este en áreas escolares*
2. *Cuando vaya o venga de la escuela*
3. *Durante el periodo de almuerzo tanto si está dentro o fuera del campus.*
4. *Durante o mientras vaya o venga de alguna actividad patrocinada por la escuela.*

Con la llegada de los espacios de aprendizaje en línea, particularmente aquellos manejados por el Distrito escolar (incluyendo Google G Suite) se expande el concepto de tiempo de clase más allá de las instalaciones escolares. De hecho, los estudiantes pueden considerar el uso de las cuentas en línea provistas por el Distrito como una actividad patrocinada por la escuela, por lo que sus acciones y comportamientos cuando se estén usando cuentas o hagan interacciones en línea con compañeros de clase cae dentro del alcance de la Política de Uso Aceptable.

La tecnología del Distrito incluye, pero no está limitada a, los dispositivos informativos y periféricos (computadoras, laptops, tabletas, dispositivos de almacenaje extraíbles, tecnología usable, sistemas de proyección interactiva en el aula) que sean propiedad del Distrito y / o manejados por el Distrito, la red del Distrito y dispositivos/servicios de comunicación (Teléfonos, redes conectadas con cable o sin cable incluyendo puntos de acceso de WiFi, radios de emergencia, sistemas de correo electrónico, servidores de almacenamiento, etc.) y servicios en línea manejados por el Distrito (Google G Suite, Aeries, etc.); y futuras innovaciones de tecnología.

La falta del cumplimiento de esta política puede repercutir en la disciplina incluyendo perdida de acceso, confiscación del dispositivo, o hasta puede incluir la expulsión de acuerdo con el comportamiento del estudiante y las políticas de disciplina. Se espera que los estudiantes ejerzan un comportamiento ético cuando estén utilizando herramientas de tecnología del Distrito y personales cuando se hace referencia al acoso, deshonestidad académica y plagio. A discreción de la escuela, la administración del Distrito, o de acuerdo con la ley, los estudiantes deben de ser disciplinados por emplear una conducta considerada como perjudicial para la escuela y su misión, o dañina para otros estudiantes. Todos los aspectos de esta Política de Uso Aceptable aplican tanto se acceso a la tecnología del Distrito dentro o fuera el campus y tanto si el dispositivo es de propiedad del Distrito o personal. Al usar herramientas de tecnologías o servicios manejados por el Distrito, los estudiantes y los padres aceptan las siguientes estipulaciones:

1. Al usar las herramientas y servicios de tecnología del Distrito tanto si los dispositivos son de propiedad personal o del Distrito, los estudiantes y padres dan consentimiento específico, como está definido en el Acto de Privacidad de Comunicación Electrónica de California (también conocido como Senado Bill 178), para

que el Distrito pueda revisar y monitorear toda la información de comunicación electrónica y la información que se produzca, se transmita o se almacene en los dispositivos a través de los servicios de tecnología del Distrito.

2. Por lo tanto, los estudiantes y padres reconocen que el Distrito podría monitorear o acceder a cualquier y todo el uso de tecnología de los estudiantes sin previo aviso, y no se tiene ninguna expectativa de que haya derecho de privacidad cuando se estén usando dispositivos del Distrito o servicios de red, o cuando en cualquier momento se estén usando cuentas y recursos en línea provistas por el Distrito, incluyendo correo electrónico y herramientas de colaboración en línea.
3. Los estudiantes aceptan seguir las políticas escolares en todo momento, especialmente cuando se esté usando las herramientas de tecnología y servicios del Distrito. Los estudiantes y padres aceptan que cualquier uso inapropiado de la tecnología, cuando se esté dentro del campus escolar o fuera del campus a través de cuentas manejadas por el Distrito, puede ser el resultado de una disciplina escolar.
4. Los estudiantes entienden que los dispositivos electrónicos solo por permitidos para uso educacional cuando se esté en el campus. Si los estudiantes están jugando, mandando mensajes o intentan acceder a alguna sitio web o aplicaciones durante el tiempo de clase sin la dirección y supervisión de algún maestro podrían perder el privilegio, suspensión o anulación del uso el dispositivo tecnológico. Si la violación se repite podría dar resultado a consecuencias más severas.
5. Los padres aceptan que el Distrito puede actuar como un agente autorizado para la creación de cuentas en línea para los estudiantes que se únicamente para propósitos educacionales de acuerdo a la ley estatal y federal de privacidad de información de los estudiantes (COPPA, FERPA, SOPIPIA, etc.). Las cuentas de los estudiantes que son manejadas por el Distrito pueden incluir, pero no están limitadas a: cuentas creadas en línea para Google G Suite (Aplicaciones de Google para la Educación) y accesos para otras aplicaciones, o servicios en línea y recursos de currículo digital.
6. El Distrito tiene la seguridad de sus estudiantes en su más alta consideración. Sin embargo, la habilidad de compartir información y de enseñar a los estudiantes una ciudadanía digitalmente responsable es vital para el proceso educacional. Esto incluye el uso de correo electrónico, sistemas de gestión de aprendizaje escolar, herramientas de colaboración en línea, servicios para compartir fotografías en clase y otras vías de redes sociales cuando sea aplicable.
7. Los padres y los estudiantes entienden que los teléfonos celulares y dispositivos personales de programa computacional 1-a-1 que no son manejados por el Distrito, pueden ser traídos al campus solo bajo las circunstancias específicas. Los estudiantes que traigan dispositivos electrónicos personales al campus, lo hacen bajo su propio riesgo y el distrito no se hace responsable de pérdida, daño o robo del dispositivo en caso de ser confiscado. Durante el horario de clases estos dispositivos solo pueden ser utilizados bajo la supervisión e instrucción de un maestro o administrador. Estos dispositivos pueden ser utilizados fuera del tiempo de clase de cualquier manera que no esté prohibida a continuación.

Las siguientes actividades o uso de tecnologías son estrictamente prohibidos para asegurar un ambiente de aprendizaje digital respetuoso:

- El uso de tecnología para amenazar, intimidar o acosar a otros. Esto puede incluir, pero no está limitado a: enviar, acceder, subir, descargar o distribuir mensajes de texto, imágenes u otros materiales ofensivos, amenazadores, profanadores, obscenos o sexualmente sugestivos.
- Grabar video o audios de otros estudiantes o personal escolar sin su autorización.
- Buscar, acceder o poseer imágenes o archivos multimedia que sean lascivos/indecenas, sexualmente sugestivos, violencia gráfica, o despectivas/degradantes.
- Usar los dispositivos o la red provista por el Distrito para buscar y/o acceder a almacenes de contenido ilegal, contenido que pueda causar daño a la red del Distrito o contenido que promueva, aliente o enseñe a los

estudiantes a cometer actos ilegales (por ejemplo: hacer bombas, piratear información electrónica, causar daño intencional, etc.).

- Evitar (o intentar evitar) los filtros de contenido de Internet del Distrito a través de una red proxy, anonimadores u otras formas a través de dispositivos de información del Distrito o personales.
- Eludir/evitar las medidas de seguridad de la red o intentar acceder a información confidencial, privada o restringida en la red del Distrito o servicios del Distrito manejados en línea.
- Compartir las contraseñas o accesos en línea únicamente con los padres o tutores del estudiante o adulto de confianza.
- Iniciar sesión en dispositivos o servicios con la cuenta de otro estudiante o personal escolar o de otra manera obtener acceso a sus archivos y cuentas sin su permiso.
- Compartir, publicar o distribuir información confidencial de identificación personal en línea como: nombre, su número telefónico, la dirección de la casa, detalles financieros, números de seguro social, credenciales para iniciar sesión o contraseñas de otro estudiante, personal escolar o cualquier otra persona, con la intención de amenazar, intimidar, acosar o dañar a esa persona.
- Destruir, dañar, vandalizar, regresar inservible cualquier propiedad (ya sea propiedad física como la computadora o virtual como una página web.) que pertenezca al Distrito, a otro estudiante o adulto.
- Alterar la configuración de los dispositivos del Distrito de manera que pueda causar confusión, frustración o pérdida de acceso a otros usuarios (cambiar el fondo de pantalla, páginas principales, dock, configuración de redes, cuentas de inicio de sesión, etc.).
- El uso o instalación de virus, malware, keyloggers, spyware, u otros softwares/hardwares que puedan ser utilizados para el daño de las redes del Distrito, extraer información de acceso de otros usuarios o propagar mensajes o archivos no deseados.
- Descarga ilegal, almacenamiento, instalación o transmisión de material con derechos de autor sin la licencia o los permisos adecuados. El Distrito prohíbe explícitamente la descarga de programas o servicios en las redes del Distrito.
- El robo de la propiedad intelectual incluyendo mensajes, música, películas y software, o el uso de ellos sin la apropiada referencia o el permiso expresado de acuerdo con las leyes de Copyright y las normas de Uso Justo.
- La visita de páginas de redes sociales que no están destinadas directamente con la educación (incluyendo Facebook, Instagram, Twitter, Vine, etc.). durante la clase.
- El uso de mensajería instantánea o salas de chat en línea que no estén directamente relacionados con la instrucción (incluyendo enviar mensajes, mandar fotografías por mensaje, mensajes de audio o video) durante las clases.

### **Marca Digital Permanente**

Se les recuerda a los estudiantes, que cualquier cosa que se ponga en línea crea una marca permanente que quedará fuera de su control. Tengan en mente que el rastro que se crea para ustedes o para otros, es como un tatuaje casi imposible de borrar por completo. Aplicaciones, sitios web y softwares que reclaman para borrar información pueden dejar un rastro permanente y accesible para otros. Los estudiantes no deben asumir que su presencia en línea permanecerá en privado y deberán de manejar su actividad en línea esperando que cualquier o toda la información que suministren pueda ser accesada a una audiencia más amplia, tanto como a oficiales de admisión y posibles futuros empleadores.

### **Cuentas en línea de los estudiantes y opción de exclusión.**

Mientras el Distrito trabaja para cumplir la misión de preparar a los estudiantes para el ambiente laboral al que pronto entrarán, aumentará la utilización de herramientas y recursos que son almacenados en línea y que tengan acceso a



través de internet. Las cuentas en línea son necesarias para acceder a archivos que son almacenados en la web y herramientas de colaboración como Google G Suite, Google Classroom, Google Docs y el correo electrónico administrado por Google, así como otros recursos educativos en línea. Estos servicios con base en la nube y en la web permiten una distribución en línea y la entrega de asignación de los estudiantes, discusiones en línea y actividades de colaboración, currículo con base en la web o recursos de aprendizaje y en algunos niveles académicos el correo electrónico de los estudiantes.

Todas las cuentas provistas a los estudiantes a través del Distrito, se alinearán con los requerimientos de la privacidad de estudiantes federal y estatal. En California, El Acto de Protección de Información Personal en Línea, por sus siglas en inglés SOPIPA, (AB1584, SB1777 y AB1442) crea una privacidad estándar para todos los servicios en línea encargados de la educación en California de los grados K-12 y los previene de promoverse con estudiantes, construir perfiles digitales acerca de ellos y/o vender información obtenida a otros usuarios. El Distrito cree que estas restricciones proveen un ambiente de seguridad para sus estudiantes y utilizan cuentas que son creadas por el Distrito para acceder a los recursos y servicios educativos en línea.

El Acto de Protección Federal en Línea para los Niños, por sus siglas en inglés COPPA, permite a las Autoridades de Educación Local (LEA), tanto a los distritos como a las escuelas, proveer consentimiento a nombre de los padres para crear cuentas en línea que podría recolectar información limitada al contexto educacional y no para propósitos comerciales. LTUSD opera bajo las normas de COPPA y crea y maneja cuentas de estudiantes en línea. Por Ley, los padres pueden elegir excluir a sus hijos de este consentimiento implícito de los padres. Esto se puede hacer en LTUSD obteniendo el formulario de “exclusión de cuentas en línea” en la oficina escolar, agendar una conferencia con el director de la escuela y completar y firmar el formulario en presencia del director, que firmará el recibo de la forma después de haber discutido las razones y las consecuencias de exclusión.

Al excluir a los estudiantes de las cuentas del Distrito manejadas en línea, se impactará significativamente la habilidad de los estudiantes a participar en las lecciones y actividades de clase y podría impedir a los estudiantes de aprender los principios de ciudadanía digital requeridos por el estado y practicar comportamientos de responsabilidad digital enseñados en clase. Podría ser difícil que los estudiantes reciban asignaciones, participación en proyectos de colaboración en línea, volver a subir trabajo regresado por los maestros o acceder a las lecciones en línea, textos digitales y tutoriales. Debido al uso progresivo de la tecnología del Distrito, mejorar el aprendizaje es parte de los valores fundamentales, prácticamente todos los padres reconocen la importancia de permitir al distrito llevar a cabo la misión de promover una ciudadanía digital responsable y prácticas y comportamientos seguros en línea para todos los estudiantes y a su vez creando y manteniendo las cuentas en línea de los estudiantes.

Como parte de los entrenamientos estratégicos de graduación de ciudadanía digital, los estudiantes de K-8 tendrán un funcionamiento de correo electrónico limitado que solo les permitirá enviar y recibir correo electrónico de sus maestros o de otros estudiantes dentro del Distrito, pero no de cuentas fuera de él. Los estudiantes de los grados 9-12 podrán tener un mayor acceso para enviar y recibir correos electrónicos con individuos y organizaciones fuera del Distrito si es necesario, pero todas las comunicaciones a través de correo electrónico serán monitoreadas por el Distrito.

**Nombre del  
estudiante** \_\_\_\_\_

**Escuela** \_\_\_\_\_

**Grado:** \_\_\_\_\_

**Número de  
estudiante** \_\_\_\_\_

**Acuse de recibo del Estudiante:**

He recibido, leído, entiendo y acepto seguir este Acuerdo Aceptable de Uso y otras leyes aplicables y políticas del distrito y regulaciones que controlan el uso de la tecnología del distrito. Entiendo que no hay privacidad cuando se utiliza la tecnología del distrito. Además, entiendo que cualquier violación puede dar como resultado la pérdida de privilegios de usuario, acciones disciplinarias y/o acciones legales adecuadas.

Nombre: \_\_\_\_\_ Grado: \_\_\_\_\_  
(Por favor escriba el nombre)

Firma: \_\_\_\_\_ Fecha: \_\_\_\_\_

**Acuse de recibo de Padre/Guardián**

Si el estudiante es menor de 18 años, el padre o guardián también debe de leer y firmar el acuerdo.

Como padre o guardián del estudiante nombrado anteriormente, he leído, entiendo y acepto que mi hijo debe cumplir con los términos del Acuerdo Aceptable de Uso. Al firmar este Acuerdo, doy permiso para que mi hijo utilice la tecnología del distrito y/o que tenga acceso a la red de las computadoras escolares e Internet. Entiendo que, a pesar de los mejores esfuerzos, es imposible para la escuela restringir el acceso a todos los materiales ofensivos y controversiales. Acepto liberar de responsabilidad, indemnización y de exoneración a la escuela, el distrito y el personal del distrito en contra de cualquier reclamación, daño o costo que pueda resultar del uso que mi hijo haga de la tecnología del distrito o falla de cualquier medida de protección usada por el distrito. Además, acepto la completa responsabilidad de supervisar a mi hijo en el uso de su cuenta de acceso si y cuando dicho acceso no se encuentre en el entorno escolar. Si el dispositivo es dañado, debido a abuso o negligencia, o si se el dispositivo y/o adaptador de corriente AC se pierden, el estudiante debe pagar una cuota de \$200.00 por la pérdida/daño.

Nombre: \_\_\_\_\_ Fecha: \_\_\_\_\_  
(Por favor escriba el nombre)

Firma: \_\_\_\_\_