

Póliza del Uso Aceptable de Tecnología del Distrito

Uso aceptable de la Tecnología del Distrito ocurre donde el propósito principal de dicho uso es mejorar el aprendizaje estudiantil y preparar a los estudiantes graduados listos para una carrera.

Mediante el uso de la tecnología y redes de comunicación del Distrito, los aprendices han acordado implícitamente a todos los términos de esta Póliza de Uso Aceptable. Si un aprendiz no está seguro acerca de si un uso en particular es aceptable o apropiado, él o ella deben consultar a un maestro, administrador o personal apropiado del Distrito.

SUMARIO: Esta póliza de Uso Aceptable (“AUP”) fue escrita para informar a los estudiantes, sus familias y el personal del Distrito acerca de las maneras aceptables en las cuales los sistemas de tecnología que pertenecen al Distrito Escolar Unificado de Fresno (“Distrito”) pueden ser utilizados. La información de tecnología y los sistemas del Distrito serán referidos como “Tecnología del Distrito” en el resto de estos documentos.

Uso Responsable de Tecnología del Distrito

Soy un ciudadano responsable de practicar una conducta digital positiva y ética.

- Practicaré una conducta apropiada, y contribuciones en el internet (websites), redes sociales, discusión en sitios de medios compartidos y todas las otras comunicaciones electrónicas, incluyendo nueva tecnología.
- Seré honesto en todas las comunicaciones digitales.
- Comprendo que lo que yo haga y coloque en el internet no debe interrumpir las actividades escolares ni comprometer la seguridad y protección escolar.
- Usaré el lenguaje escolar apropiado en todas las comunicaciones electrónicas, incluyendo correos electrónicos, publicaciones en las redes sociales, grabaciones de audio, videoconferencias y trabajos artísticos.
- No enviaré ni distribuiré comunicaciones digitales de odio, discriminación o comunicación digital de acoso/hostigamiento, ni participaré en mensajes de texto con contenido sensual.
- Comprendo que cualquier manera de acoso, incluyendo cibernético, es inaceptable.
- No buscaré, mostraré, ni distribuiré material que sea discurso de odio, sexualmente explícito o violencia.
- No compartiré información personal acerca de mí mismo o de los demás, no limitada a, nombres, direcciones de casas, números de teléfonos, fechas de nacimiento, o visuales como fotos, videos y dibujos para fines no educativos o negocios no pertenecientes al Distrito.
- No publicaré fotos, trabajo estudiantil u otros artículos que estén en violación de FERPA*.
- Entiendo que el uso de la tecnología del Distrito con fines ilegales, políticos o comerciales está estrictamente prohibido.

Soy responsable por el uso y cuidado de mi computadora.

- Llevaré mi computadora todos los días a la escuela, cargada y lista para el aprendizaje.
- Me aseguraré de que mi computadora esté segura y protegida.
- Discutiré con mis padres o tutores las expectativas con respecto al uso de Internet y el dispositivo.
- No alteraré, desconfiguraré ni eliminaré ninguna etiqueta de distrito en mi computadora.
- Devolveré los dispositivos prestados en las mismas condiciones que me fueron dados.

Soy responsable de mis contraseñas y mis acciones en la tecnología del Distrito.

- No compartiré con nadie ningún nombre de usuario ni contraseñas de la escuela o Distrito.
- No accederé la información de la cuenta de otros.
- Me desconectaré/cerraré las sesiones de equipos y cuentas desatendidas para mantener la privacidad y seguridad.
- Entiendo que los dispositivos emitidos a los estudiantes y el personal son para el aprendizaje o los negocios del Distrito.

Soy responsable de respetar el trabajo de los demás.

- Seguiré todas las normas de derechos de autor (<http://copyright.gov/title17/>).
- No descargaré música obtenida ilegalmente, software, aplicaciones ni otros trabajos.

*La Ley de Derechos de Educación Familiar y Privacidad (FERPA, por sus siglas en Inglés) es una ley federal que requiere confidencialidad de la información de los estudiantes. Publicar públicamente información personal de los estudiantes, registros de estudiantes o trabajo calificado es una violación de FERPA. Para obtener más información sobre FERPA más allá del uso responsable y la publicación en línea, visite <https://studentprivacy.ed.gov/>.

Definiciones: Como se usa en este documento, la palabra “Aprendiz” incluye cualquier persona —empleados, estudiantes, padres e invitados —que usan la Tecnología del Distrito. Solo los aprendices que están de acuerdo con esta Póliza de Uso Aceptable están autorizados para usar la Tecnología del Distrito.

El uso de Tecnología del Distrito se ofrece a los estudiantes principalmente con fines educativos, como un privilegio que debe ser protegido por todos los aprendices. El Distrito está comprometido a mejorar los logros académicos y preparar a todos los estudiantes para ser graduados listos en una carrera y usar la Tecnología del Distrito con este fin. La Tecnología del Distrito se emite al personal apropiado en el curso para realizar sus tareas de trabajo.

La Tecnología del Distrito incluye, pero no es limitada a; teléfonos celulares, programas hardware de la computadora, laptops, tabletas, e-readers, software, hotspots, redes de comunicación con conexión e inalámbrico y acceso a internet. Estos artículos proveen herramientas que se pueden usar para acceso de información y comunicación con personas, ampliar el aprendizaje y le permiten al distrito operar eficientemente. La tecnología y el uso de esta por las personas está cambiando siempre, por lo tanto, es crucial que el Distrito asegure un ambiente de aprendizaje seguro para los estudiantes y el personal; protección a la privacidad de datos electrónicos y proteger los valores de la tecnología del distrito. La Tecnología del Distrito permanece como propiedad del Distrito todo el tiempo.

Póliza del Uso Aceptable de Tecnología del Distrito

Esta póliza de uso aceptable debe satisfacer las pólizas existentes del distrito incluyendo la Póliza de la Junta 0440 y 0440.1 (Póliza Tecnológica y Reglamentos Administrativos de la Junta Directiva), así como también los procedimientos y leyes de derecho de autor establecidas. Si alguna parte de estas pólizas no es de acuerdo con las leyes federales, estatales o locales, estas leyes toman precedencia, dejando el resto de las pólizas en esta AUP en pleno vigor.

Este AUP de tecnología está destinado a:

- Prevenir o desanimar el acceso sin autorización y otras actividades ilegales en-línea;
- Prevenir o desanimar el acceso de o dar a conocer sin autorización información sensible;
- Cumplir con la Ley de Protección de Internet de los Niños de 1997 ("CIPA");
- Definir las pólizas para administrar documentos electrónicos que son propiedad del Distrito.
- Ampliar la enseñanza y el aprendizaje;
- Incrementar la seguridad para los estudiantes y el personal;
- Mejorar la eficacia de los sistemas de tecnología del distrito;
- Asegurar el alineamiento con las Creencias y Compromisos Centrales del Distrito;
- Asegurar el cumplimiento con las pólizas aplicables del distrito, leyes estatales y federales; y
- Educar a los estudiantes, personal y otros a que usan la tecnología del Distrito.

Filtrar. El Distrito usará una variedad de medidas de protección tecnológicas para bloquear o filtrar, hasta la extensión posible, el acceso de descripciones visuales que son obscenos, pornográficos y dañinos para los menores, u otro contenido que no es académicamente relevante. El Distrito reserva el derecho de supervisar/monitorear las actividades de los aprendices en-línea y acceso o guardar cualquier comunicación electrónica o contenido y darlos a conocer a otros según lo considere necesario el Distrito. Los aprendices no deben tener ninguna expectativa de privacidad en relación con su uso de la propiedad del Distrito, acceso a la red de comunicación y/o Internet o archivos, incluyendo correos electrónicos u otras formas de comunicación usando la Tecnología del Distrito. Si bien nuestra intención es poner el acceso a la computadora a disposición de los estudiantes para apoyar su crecimiento educativo, los estudiantes pueden encontrar maneras de acceder a material inapropiado también. En última instancia, los padres y tutores son responsables de establecer y transmitir los estándares que sus estudiantes deben seguir al usar la tecnología. Deshabilitar los filtros de tecnología de contenido en dispositivos emitidos por el distrito o usar herramientas para eludir el filtro de contenido es una violación de esta directiva.

Traiga su Propio Dispositivo/Aparato ("BYOD"). Algunas escuelas del Distrito permiten a los estudiantes o al personal llevar su propia tecnología – incluyendo teléfonos celulares, teléfonos inteligentes (Smart), tabletas, e-readers, laptops, u otras computadoras móviles – de uso aprobado en el ambiente escolar. Cada escuela decide por propia cuenta ya sea sí o no se les permite llevar su propio dispositivo/aparato (BYOD). Si los Aprendices llevan su propio dispositivo, todavía están sujetos a esta póliza AUP hasta la extensión que su dispositivo usa los Servicios del Distrito y Redes de comunicación (con conexión o inalámbricas) para acceso interno o internet basada en información y datos.

Aprendizaje y trabajadores a distancia. Entiendo que estoy obligado por la Política de Uso Aceptable (AUP) independientemente de mi ubicación física. También reconozco que FUSD tiene una capacidad limitada para ayudar en problemas relacionados con la red. El Distrito puede solicitar el reembolso por equipo perdido, robado o dañado si es por negligencia. A petición, los usuarios deben traer su dispositivo proporcionado por el Distrito ocasionalmente para un chequeo, limpiar la memoria de la computadora u apoyo.

Se proporcionan computadoras al personal y una computadora por estudiante. Las computadoras portátiles y computadoras proporcionadas a los estudiantes y al personal siguen siendo propiedad del Distrito. Entiendo que soy responsable de mantener el dispositivo seguro y sólo se utiliza para su propósito mientras está a mi cuidado. El Distrito puede dar mantenimiento al dispositivo de forma remota instalando software, actualizando software o instalando reparación de seguridad.

Traiga su propio dispositivo ("BYOD"). Algunos estudiantes pueden optar por traer su propia tecnología. Los dispositivos BYOD deben cumplir o exceder las especificaciones mínimas establecidas por el Distrito para un aprendizaje efectivo. Consulte el sitio web del Distrito de Fresno para conocer las especificaciones mínimas actuales. Si los alumnos traen sus propios dispositivos, siguen estando sujetos a este AUP en la medida en que su dispositivo utilice los Servicios y Redes del Distrito (cableados o inalámbricos) para acceder a información y datos internos o basados en Internet. El acceso a Internet desde dispositivos BYOD se filtrará contenido mientras esté en la red del Distrito. El Distrito no filtra los dispositivos BYOD mientras está fuera de la red del Distrito. Los estudiantes y los padres deben ser conscientes de que los dispositivos pueden estar sujetos a la búsqueda por parte de los administradores de la escuela si el dispositivo es sospechoso de una violación de mala conducta del estudiante. Si el dispositivo está bloqueado o protegido con contraseña, se le puede pedir al estudiante que desbloquee el dispositivo a petición de un administrador de la escuela. El Distrito no es responsable de daños o daños a personas, archivos, datos, hardware o interrupciones del servicio mientras los estudiantes están usando su dispositivo. El propietario asume cualquier riesgo o pérdida al traer su dispositivo.

Tabletas de dispositivos complementarios de aprendizaje electrónico (LCD). Los dispositivos emitidos desde la iniciativa eLearning Companion Device (LCD) vienen con un filtro de contenido e informan del uso de las aplicaciones educativas preinstaladas. Deshabilitar los de contenido de tecnología en dispositivos complementarios de aprendizaje o usar herramientas para eludir el filtro de contenido es una violación a la póliza. El Distrito no informa sobre la actividad o ubicación de Internet en el hogar en tabletas de LCD.

Obligaciones. Los estudiantes y otros usuarios deben seguir esta política e informar cualquier uso indebido de la Tecnología del Distrito, incluyendo la red del Distrito o Internet a un supervisor u otro personal apropiado del Distrito. El acceso a la tecnología del distrito se proporciona principalmente para la educación y los negocios del distrito. El personal puede utilizar Internet para uso personal incidental durante el horario de servicio.

Violaciones. Las violaciones de estas pólizas pueden ser el resultado de uno o más de lo

siguiente: Acción disciplinaria y/o despido del empleado y personal temporario, terminación de contratos para consultantes o contrato de empleados; reembolso al Distrito por gastos no permitidos o despido de internos y voluntarios. En el caso de una violación del estudiante, la violación puede resultar en acción disciplinaria según se considere apropiado por la administración escolar hasta e incluyendo remover los privilegios de tecnología, ser removido de la clase, suspensión y expulsión. Además, las personas están sujetas a la pérdida de privilegios de acceso, civil, y si está justificado, proceso penal. El Distrito intentará adaptar cualquier acción disciplinaria a los problemas específicos relacionados con cada violación.

Usos No Aceptables de la Tecnología del Distrito

Enlistados en la parte de abajo hay varios ejemplos de actividades inapropiadas del uso de la Tecnología del Distrito. La lista no significa que todo sea inclusivo, más bien representa el uso inapropiado. El Distrito reserva el derecho de tomar acción inmediata en relación con las actividades inapropiadas que (1) crean problemas de seguridad y/o asuntos de seguridad del Distrito, estudiantes, empleados, escuelas, red de comunicación o recursos de computadoras; 2) ampliar los recursos del Distrito en el contenido de que el Distrito en su única discreción determina la falta legítima del contenido/propósito educativo; o 3) de otra manera son determinadas por el Distrito como inapropiadas.

Actividades inapropiadas incluyen:

1. Violar cualquier ley estatal o federal u ordenanza municipal, como: Acceso o transmitir pornografía, descripciones obscenas, materiales dañinos a menores, materiales que motivan a otros a violar la ley, información confidencial o materiales de derecho de autor.
2. Actividades criminales que pueden ser castigadas bajo la ley.
3. Venta o comprar artículos o substancias ilegales.
4. Obtener y/o usar correos electrónicos anónimos, o “anonimatos” de las escuelas, especialmente con el propósito de evadir los sistemas de filtración del contenido del Distrito; mensajes no solicitados, o propagar virus; o conducir actividades fraudulentas.
5. Causar perjuicio o daño a la propiedad de otros.
6. Usar lenguaje grosero, abusivo o descortés, acoso cibernético incluyendo amenazas, hostigamiento, o hacer daño o declaraciones falsas acerca de otros o acceso, transmiti o bajar materiales ofensivos, hostigamiento o materiales denigrantes.
7. Borrar, copiar, modificar, o falsificar el nombre de otros usuarios, correo electrónico (emails),
8. Dañar de cualquier manera el equipo de computadora, archivos, información o la red de comunicación, incluyendo acceso intencional, transmitir o bajar virus de computadora u otros archivos perjudiciales o programas, o interrumpir la ejecución de cualquier sistema de computadora
9. Usar cualquier tecnología del Distrito para “piratear (hacking)” ya sea en forma interna o externa del Distrito o intentar el acceso de información protegida por las leyes de privacidad.
10. Acceso, transmitir o bajar archivos de mucha información –en particular, pero no limitado a uso “torrente” del programa software para ilegalmente bajar materiales digitales con derecho de autor –o uso de comunicación valiosa para actividades no académicas tales como juegos de red electrónica (network) o servir como anfitrión de dichas actividades.
11. Usar el correo electrónico u otros servicios de internet para distribuir “cadena de cartas” o cualquier otro tipo de “esquemas de pirámides”.
12. Uso de sitios de internet, correos electrónicos, red de comunicación, u otra tecnología para uso

político o beneficio personal, incluyendo publicidad, o promoción de sitios de internet no del distrito o esfuerzos comerciales y eventos. El internet y propiedad del internet no debe ser usada para beneficio personal. Los aprendices no deben intencionalmente tener acceso, crear, guardar o transmitir material que puede ser considerado ofensivo, indecente, obsceno, intimidador, u hostil; o material el cual acosa, insulta o ataca a otros. Los aprendices no deben violar ninguna de las leyes de derecho de autor aplicable. Esto incluye, pero no es limitado a, instalación de programas de software en las computadoras del distrito para la cual los aprendices no tienen una licencia válida y vigente del programa software.

Información de Apoyo u Obligaciones Adicionales

La siguiente información u obligaciones apoyan la Tecnología del Distrito AUP.

Seguridad de la Red de Comunicación y Pólizas de la Contraseña

1. Los aprendices deben reportar cualquier debilidad de seguridad en el internet del Distrito, o cualquier incidente de posible mal uso o violación de este acuerdo a la Red Maestra del Distrito, a través de enviar correos electrónicos al: webmaster@fresnounified.org.
2. Los aprendices no deben intentar el acceso a ninguna información o programa en los cuales no tienen autorización o consentimiento explícito.
3. La Tecnología del Distrito incluye redes de comunicación y servicios que son recursos compartidos. Los aprendices no deben participar a propósito en actividades que degraden deliberadamente la ejecución de los sistemas de Tecnología del Distrito e Información de Tecnología relacionada a la propiedad; privar un acceso autorizado a un Aprendiz del Distrito a un recurso; obtener recursos extras más allá de aquellos que son autorizados o eludir las medidas de seguridad del Distrito.
4. Los aprendices no deben bajar, instalar o correr programas de seguridad o utilidades que revelan o explotan las debilidades de la seguridad de los sistemas de Información Tecnológica del Distrito y la propiedad relacionada a la Tecnología.
5. Toda la información privada se debe mantener en forma confidencial y segura por el aprendiz. El hecho de que la información puede ser guardada electrónicamente no cambia el requisito de mantener la información en forma confidencial y segura. Más bien, el tipo de información o la información a sí misma es la base para determinar si debe ser guardada en forma confidencial y segura. Si esta información es guardada en un papel o en formato electrónico, o si la información es copiada, imprimidamente o transmitida electrónicamente el dato todavía puede ser protegido en forma confidencial y segura.
6. Todos los programas de la computadora, aplicaciones, código de origen, código objetivo, documentación e información deben ser vigilados y protegidos.
7. El Distrito se reserva el derecho para remover cualquier contenido (organizacional o personal) en el internet o intranet en cualquier momento, sin causa o aviso.
8. No hay garantía de privacidad personal o acceso a la Tecnología del Distrito. El distrito reserva el derecho para buscar y/o monitorear/supervisar cualquier información creada, tener acceso, enviada, recibida, y/o guardada en cualquier formato por cualquier empleado del distrito en el equipo del distrito o cualquier equipo conectado a la red de comunicación del distrito.
9. Todos los programas software comerciales de la Tecnológica del Distrito son con derechos de autor y designados para el uso del Distrito. Los aprendices deben acatar/obedecer todos los acuerdos de la licencia.

Póliza de la Contraseña

1. La contraseña debe ser tratada como información confidencial.
2. A todos los Aprendices que se les provee una identificación (ID) y una Contraseña debe mantener su contraseña en forma privada y no compartirla con nadie más. Ningún personal deberá pedir, o dar, la contraseña de otro Aprendiz, aun con el propósito de apoyo.
3. Se recomienda que la contraseña debe ser cambiada por lo menos cada 180 días. Sin embargo, el distrito puede a discreción única, imponer periódicamente los cambios de la contraseña basados en la responsabilidad y uso.
4. Las contraseñas provisionales deben ser cambiados dentro de un día.
5. La complejidad de la póliza de la contraseña debe ajustarse a la Póliza de la contraseña basada en la responsabilidad de la función, uso o apropiado a la edad del estudiante/aprendiz.
6. las contraseñas no deben incluir el número del empleado, nombre, Número de Seguro Social (SSN), número de teléfono, fecha de nacimiento, o el nombre de su departamento o escuela.
7. Las contraseñas de la cuenta del aprendiz deben ser protegidas por los mismos del uso a través o dar a conocer a cualquier individuo u organización. Todas las violaciones de seguridad deben ser reportadas a la escuela o departamento administrativo.
8. El personal proporcionará a Recursos Humanos (HR) o las fuerzas del orden público contraseñas, frases de contraseña, códigos de acceso y números de acceso (PIN) de dispositivos tecnológicos emitidos por el distrito según sea necesario.

Control de Acceso, Información de Seguridad y Responsabilidad

1. Los departamentos y las escuelas que tienen Tecnología del Distrito deben proveer control de acceso adecuado a fin de poder supervisar y proteger los datos del negocio y programas asociados del mal uso.
2. Todos los aprendices son responsables de administrar su propio uso de la Tecnología del Distrito y son responsables de sus acciones relacionadas a la seguridad. Los aprendices tienen la misma responsabilidad de reportar cualquier violación que se sospeche o se confirme de esta póliza al administrador responsable apropiado del sistema de Tecnología a cargo de incidentes de seguridad de FUSD.
3. Pueden llevarse a cabo evaluaciones periódicas de la ciberseguridad de los usuarios para medir la preparación de la organización o para apoyar al personal en la educación sobre seguridad cibernética.
4. El acceso a los equipos de Tecnología de la Información FUSD debe estar debidamente documentado, autorizado y controlado.
5. El acceso de autoridad para cada aprendiz será revisado regularmente, así como también en cada cambio de estatus de trabajo como: transferencia, asenso, descenso o terminación del servicio.
6. Las escuelas y Departamentos responsables de la custodia y funcionamiento de la Tecnología del Distrito deben ser responsables de la autorización apropiada y relacionada al uso de tecnología, el establecimiento de uso eficaz y de reportar la ejecución al administrador.
7. Algunos empleados del Distrito están obligados a usar una VPN u otros procedimientos de seguridad de red aprobados para acceder a sistemas internos o datos cuando trabajan de forma remota.
8. Sobre la terminación de la relación con el FUSD todas las pólizas de seguridad aplican y permanecen en vigor sucumbiendo la relación terminada.

Retención de Documento

Es responsabilidad de todos los empleados guardar y/o archivar los correos electrónicos que él/ella recibe y desea después tener acceso, o que son archivos del Distrito y es requerido que sean retenidos por ley. Los correos electrónicos deben ser guardados en su correo electrónico en de internet solamente en el archivo del correo electrónico en inbox o archive, o en un SharePoint apropiado o en un OneDrive Repositorio de documentos. Está prohibido archivar los correos electrónicos relacionados al distrito fuera del sistema del Distrito Escolar Unificado de Fresno.

Si usted guarda dichos documentos fuera de su lugar requerido, usted puede ser sujeto a acciones disciplinarias.

Uso Incidental

Como una conveniencia para los Aprendices de la comunidad del Distrito, el uso personal incidental de la tecnología del Distrito es permitido. La Póliza del AUP todavía aplica el uso incidental además de las siguientes limitaciones:

1. El uso incidental personal de la tecnología del Distrito por los aprendices no se extiende a los miembros de la familia o a otros conocidos.
2. El uso incidental personal no debe ser el resultado de un costo directo para el Distrito.
3. El uso incidental personal no debe interferir con la ejecución normal de las obligaciones de trabajo de un empleado o del aprendizaje de un estudiante.

Cumplimiento/ Reglamento Contribuido por medio de esta Póliza

Esta Póliza de Uso Aceptable depende en parte en los requerimientos o conceptos de lo siguiente:

1. Ley de Derechos de Educación Familiar y Privacidad de 1974 (FERPA)
2. La Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996 (HIPAA)
3. Ley de Protección de Internet de los Niños de 2000 (CIPA)
4. Enmienda de protección de los derechos de los alumnos (PPRA)
5. Ley de Derecho de Autor de 1976
6. Ley de Prácticas Corruptas en el Extranjero de 1977
7. Ley de Fraude y Abuso Informático de 1986
8. Ley de Seguridad Informática de 1987
9. Código de Educación de California
10. Ley de Protección de La Información Personal en Línea del Estudiante (SB1177)

Aceptación

Por medio de la firma de esta Póliza de Uso Aceptable usted reconoce la importancia de la responsabilidad personal al unirse a estas pólizas.

Responsabilidades del Padre/Tutor:

- Supervisar el uso del dispositivo por parte de su estudiante fuera de la red del Distrito.
- Revisar y discutir la Política de Uso Aceptable (AUP) del Distrito con su estudiante.
- Devuelva el dispositivo si se le solicita, o su estudiante se va o se gradúa del Distrito de Fresno.
- Pagar las tarifas asociadas con el reemplazo o reparación de computadoras dañadas.

“Yo comprendo y estoy de acuerdo en cumplir con las pólizas del distrito y de la escuela mencionadas en la parte de arriba y los procedimientos y lo relacionado a las pólizas de la Junta Directiva 0440.1 y 6162.7 y sus Reglamentos Administrativos de apoyo.”

Fecha _____

Fecha _____

Nombre de Padre/Tutor _____ ID del Estudiante _____

Firma del Padre/Tutor _____ Nombre del Estudiante _____

Correo Electrónico del Padre/Tutor _____ Firma del Estudiante _____

Teléfono del Padre/Tutor _____