

Política de Uso Aceptable de Tecnología del Distrito

El uso aceptable de la Tecnología del Distrito tiene lugar cuando el propósito principal de dicho uso es mejorar el aprendizaje de los estudiantes y preparar a los estudiantes graduados listos para una carrera.

Al usar la tecnología y las redes del Distrito, los estudiantes aceptan incondicionalmente los términos de esta Política de Uso Aceptable. Si un estudiante no está seguro de si el uso en particular es aceptable, el/ella debe consultar al maestro/a, administrador/a u otro personal apropiado del Distrito.

De conformidad con el aviso establecido en el MANUAL DE AVISO E INFORMACIÓN PARA PADRES/TUTORES/ALUMNOS y las políticas y regulaciones de Tecnología del Distrito (por ejemplo, 0440.1, 6163.4) y la participación de los estudiantes en la Tecnología del Distrito, el presente aviso es para resaltar que los padres, tutores y estudiantes aceptan la Política de Uso Aceptable y acuerdan no responsabilizar al Distrito o a cualquier personal del Distrito por la falla de cualquier medida de protección de Tecnología del Distrito, violaciones de cualquier restricción legal, o errores o negligencia del usuario. Además, en virtud de este aviso, también aceptan indemnizar y eximir de responsabilidad al Distrito y al personal del Distrito por cualquier daño o costo que surja del uso de la Tecnología del Distrito o esté relacionado con este y/o cualquier violación de la Política de Uso Aceptable.

RESUMEN: Esta Política de Uso Aceptable ("AUP") fue escrita para informar a los estudiantes, sus familias y personal del Distrito sobre las formas aceptables en que se puede usar la tecnología de la información del Distrito Escolar Unificado de Fresno ("Distrito"). La tecnología y los sistemas de información del Distrito se referirán como "Tecnología del Distrito" en el resto de este documento.

Uso Responsable de la Tecnología del Distrito

Soy responsable de practicar una ciudadanía digital positiva y una conducta ética.

- Practicaré el comportamiento y las contribuciones apropiadas en sitios web, redes sociales, foros de discusión, sitios de intercambio de medios y todas las demás comunicaciones electrónicas, incluyendo nuevas tecnologías.
- Seré honesto en toda la comunicación digital.
- Comprendo que lo que hago y público en línea no debe interrumpir las actividades escolares ni comprometer la seguridad escolar.
- Usaré un lenguaje apropiado para la escuela en todas las comunicaciones electrónicas, incluyendo el correo electrónico, publicaciones en las redes sociales, grabaciones de audio, videoconferencias y trabajos artísticos.

- No enviaré y/o distribuiré comunicaciones digitales que inciten al odio, discriminación o acoso, ni participaré en mensajes de texto explícitamente sexuales.
- Comprendo que el acoso en cualquier forma, incluyendo el ciberacoso, es inaceptable.
- No buscaré, mostraré ni circularé material que sea discurso de odio, sexualmente explícito o violento.
- No compartiré información personal acerca de mí mismo ni de los demás, incluyendo, entre otra, nombres, domicilios, números de teléfono, Fecha de Nacimiento o imágenes visuales como fotos, videos y dibujos con fines no educativos o negocios no relacionados con el Distrito.
- No publicaré fotos, trabajos de estudiantes u otros artículos que violen la Ley FERPA*.
- Comprendo que el uso de la tecnología del Distrito con fines ilegales, políticos o comerciales está estrictamente prohibido.

Soy responsable del uso y cuidado de mi computadora.

- Llevaré mi computadora todos los días a la escuela, cargada y lista para aprender.
- Me aseguraré de que la computadora esté segura y protegida.
- Discutiré con mis padres o tutores las expectativas con respecto al uso de Internet y el dispositivo/aparato.
- Regresaré cualquier dispositivo prestado antes de la transferencia, retirarme, o graduarme del Distrito Escolar Unificado de Fresno.
- No alteraré, desfiguraré ni eliminaré ninguna etiqueta del distrito en mi computadora.*
- Regresaré los dispositivos/aparatos prestados en las mismas condiciones en las cuales me los entregaron.*

*Las escuelas pueden establecer directrices para daños repetidos, pérdida o robo de dispositivos/aparatos, incluyendo un plan de éxito para el uso de dispositivos/aparatos por parte de los estudiantes.

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

- No compartiré ningún nombre de usuario ni contraseña de la escuela o del distrito con nadie.
- No accederé a la información de la cuenta de otras personas.
- Cerraré la sesión de equipos y cuentas desatendidas para mantener la privacidad y la seguridad.
- Comprendo que los dispositivos entregados a los estudiantes y al personal son para el aprendizaje o para asuntos del Distrito.

Soy responsable de respetar los trabajos de los demás.

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

*La Ley de Derechos Educativos y Privacidad de la Familia (FERPA, es una ley federal que requiere confidencialidad de la información de los estudiantes. Publicar información personal de los estudiantes, registros de estudiantes o calificación de los trabajos es una violación de la ley FERPA. Para obtener más información acerca de la ley FERPA más allá del uso responsable y la publicación en línea, visite: <https://studentprivacy.ed.gov/>.

Definiciones: Así como se usa en este documento, la palabra "Aprendiz" incluye cualquier persona (empleados, estudiantes, padres, proveedores e invitados) que usan la tecnología del Distrito. Solo los Aprendices que están de acuerdo con este Reglamento de Uso Aceptable están autorizados a usar la tecnología del Distrito.

El uso de la Tecnología del Distrito se ofrece a los estudiantes con fines educativos, como un privilegio que debe ser salvaguardado por todos los estudiantes aprendices. El Distrito está comprometido a mejorar el rendimiento estudiantil y preparar a todos los estudiantes a graduarse listos para una carrera y usan la Tecnología del Distrito para este propósito. La tecnología del distrito se entrega al personal apropiado para llevar a cabo sus deberes laborales.

La Tecnología del distrito incluye, entre otros, Teléfonos Celulares, hardware de computadoras, laptops, paneles de muestra en el salón de clase, cámaras de documentos, tabletas, e-readers, Programa de software (incluyendo Recursos the cloud), hotspots, redes locales con cable e inalámbricas y acceso a internet. Estos artículos proveen herramientas que se pueden usar para acceder a la información y comunicarse con las personas, amplían el aprendizaje y permiten que el distrito funcione de manera eficaz. La tecnología y el uso que las personas hacen de ella están en constante cambio, por lo que es fundamental que el Distrito asegure un ambiente de aprendizaje seguro para los estudiantes y el personal; salvaguarde la privacidad de los datos electrónicos; y proteja los valores de la tecnología del Distrito. La Tecnología del Distrito permanece como propiedad del Distrito. en todo momento.

Uso Aceptable de la Tecnología

Esta Política de Uso Aceptable deberán ajustarse a las políticas existentes del distrito, incluyendo las Políticas de la Junta 0440 y 0440.1 (Políticas y Reglamentos de Tecnología y Administrativos de la Junta), así como a los procedimientos establecidos y las leyes de derechos de autor. Si alguna parte de estas políticas entra en conflicto con las leyes federales, estatales o locales, ellas tienen prioridad, dejando las políticas restantes en esta AUP en pleno efecto.

Esta tecnología AUP tiene la intención de:

- Prevenir o desanimar el acceso no autorizado y otras actividades ilegales en línea;
- Prevenir o desalentar la divulgación o el acceso no autorizado a información delicada;
- Cumplir con la Ley de Protección de los Niños en Internet de 1997 ("CIPA");
- Definir las políticas para la administración de los documentos electrónicos que son propiedad del Distrito.
- Mejorar la enseñanza y el aprendizaje;

- Aumentar la seguridad de los estudiantes y el personal;
- Mejorar la eficiencia de los sistemas tecnológicos de los distritos;
- Asegurar la alineación con las Creencias y Compromisos Fundamentales del Distrito;
- Garantizar el cumplimiento de las políticas del distrito aplicables, leyes estatales y federales; y
- Educar a los estudiantes, personal y a otras personas que usan la tecnología del Distrito

Filtrado. El Distrito usará una variedad de medidas de protección tecnológica en las redes del Distrito para bloquear o filtrar, hasta la extensión posible, el acceso a imágenes visuales que sean obscenas, pornográficas o dañinas para los menores u otro contenido que no sea académicamente relevante. Se instalarán medidas de filtrado en los dispositivos del distrito para proteger al usuario y al dispositivo/aparato que opera fuera de la red del distrito. Los estudiantes aprendices no deben tener ninguna expectativa de privacidad con relación a su uso de la propiedad, red y/o el acceso a Internet o los archivos del Distrito, incluyendo el correo electrónico u otras formas de comunicación usando la tecnología del Distrito. Aunque nuestra intención es hacer que el acceso a la computadora esté disponible para los estudiantes para apoyar su crecimiento educativo, los estudiantes también pueden encontrar formas de acceder a material inapropiado. Finalmente, los padres y tutores son responsables de establecer y comunicar los estándares que sus estudiantes deben seguir cuando usan la tecnología. Deshabilitar las tecnologías de filtrado de contenido en los dispositivos facilitados por el Distrito o usar herramientas para evitar el filtro de contenido es una violación de esta política.

Aprendizaje y Empleados a Distancia. Comprendo que estoy sujeto al Reglamento de Uso Aceptable (AUP), independientemente de mi ubicación física. También reconozco que el FUSD tiene una capacidad limitada para ayudar en asuntos relacionados con la red. El Distrito puede solicitar un reembolso por equipo perdido, robado o dañado si es negligente. A petición, se requiere que los usuarios traigan su dispositivo proporcionado por el Distrito ocasionalmente para una revisión, nueva imagen o apoyo.

Computadoras Facilitadas al Personal y Computadoras Individuales. Las laptops y computadoras que se prestan a los estudiantes y al personal siguen siendo propiedad del Distrito. Comprendo que soy responsable de mantener el dispositivo seguro y solo se usa para su propósito mientras esté bajo mi cuidado. El Distrito puede mantener el dispositivo de forma remota mediante la instalación de software, actualización del software o la instalación de parches de seguridad.

Traiga su propio dispositivo ("BYOD"). Algunos estudiantes pueden optar por traer su propia tecnología. Los dispositivos BYOD deben cumplir o superar las especificaciones mínimas establecidas por el Distrito Escolar Unificado de Fresno para un aprendizaje eficaz. Consultar el sitio web del Distrito Escolar Unificado de Fresno para las especificaciones mínimas vigentes. Si los estudiantes traen sus propios dispositivos, aún están sujetos a esta Política de Uso Aceptable (AUP) hasta la extensión que su dispositivo use los Servicios y Redes del Distrito (con cables o inalámbricos) para acceso a datos internos o de internet. El acceso a internet desde

dispositivos BYOD se filtrará mientras estén en la red del Distrito. El Distrito no filtra el contenido de los dispositivos BYOD fuera de la red del Distrito. Los estudiantes y sus padres deben saber que los administradores escolares pueden revisar los dispositivos si se sospecha que infringen la conducta del estudiante. Si el dispositivo está bloqueado o protegido con contraseña, se le pedirá al estudiante que lo desbloquee a petición de un administrador escolar. El Distrito no se hace responsable de daños a personas, archivos, información, datos, hardware ni interrupciones del servicio mientras los estudiantes usen su dispositivo. El propietario asume cualquier Riesgo o pérdida al traer su dispositivo.

Administración Digital del Salón de Clase. Como parte de nuestro compromiso de proveer un ambiente de aprendizaje seguro y propicio, el distrito escolar usa Programa de computadora de administración de salones de clase para apoyar a los maestros en la administración efectiva de los salones de clase. El Programa de computadora de administración de salones de clase se usa exclusivamente durante las clases presenciales y en computadoras emitidas por el distrito escolar conectadas a la red del distrito escolar. Este sistema permite la visualización de las pantallas de los estudiantes en dispositivos emitidas por la escuela, el intercambio de contenido y la administración de configuraciones del salón de clase. Se espera que los estudiantes se adhieran a las líneas guía establecidas en el Reglamento de uso aceptable de tecnología, que incluye el uso responsable del Programa de software de administración de salones de clase. Para preguntas o preocupaciones, comuníquese con su Maestro o administrador de la escuela.

Dispositivos perdidos o robados. Se presentará un reporte a la policía por los dispositivos perdidos o robados y el dispositivo se bloqueará de forma remota si es posible. Es responsabilidad del personal reportar los dispositivos perdidos o robados inmediatamente a la Administración de Riesgos. Los padres reportan dispositivos perdidos o robados a servicios de asistencia (help desk) para padres y estudiantes.

Obligaciones. Se requiere que los estudiantes y otros usuarios sigan esta política y reporten 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 provee principalmente para la educación y los asuntos del distrito. El personal puede usar Internet para uso personal incidental durante el tiempo libre laboral.

Violaciones. La violación de estas políticas puede resultar en una o más de las siguientes: acción disciplinaria y/o despido para los empleados y el personal temporal; la terminación de los contratos para los consultores o los empleados contratados; reembolso al Distrito por los cargos no permitidos; o despido para los pasantes y voluntarios. En caso de una violación por parte de un estudiante, la violación puede resultar en una acción disciplinaria según lo considere apropiado la administración de la escuela, incluyendo eliminación de los privilegios de tecnología, ser removido de la clase, suspensión y expulsión. Además, la persona está sujeta a la pérdida de privilegios de acceso, acción civil y si corresponde, a acción penal. El Distrito intentará adaptar cualquier acción disciplinaria a los problemas específicos relacionados con cada violación.

Usos Inaceptables de la Tecnología del Distrito

En la parte de abajo se enlistan varios ejemplos de actividades inapropiadas usando la Tecnología del Distrito. La lista no pretende ser exhaustiva, pero es representativa de usos inapropiados. El Distrito se reserva el derecho de tomar medidas inmediatas con relación a actividades inapropiadas que (1) creen problemas de seguridad y/o protección para el Distrito, los estudiantes, empleados, escuelas, la red o los recursos informáticos; (2) gasten los recursos del Distrito en contenido que el Distrito, a su entera discreción, determine que carece de contenido/propósito educativo legítimo; o (3) que el Distrito determine de otro modo como inapropiadas.

Las actividades inapropiadas incluyen:

1. Violar cualquier ley estatal o federal u ordenanza municipal, como acceder o transmitir pornografía; representaciones obscenas; materiales dañinos para los menores; materiales que animen a otros a violar la ley; información confidencial; o materiales protegidos por derechos de autor.
2. Actividades delictivas que pueden ser castigadas por la ley.
3. Vender o comprar artículos o sustancias ilegales.
4. Obtener o usar correo electrónico anónimo o sitios de “anónimos”, especialmente con el propósito de evadir los sistemas de filtrado de contenido del distrito; enviar correo electrónico no deseado a cuentas de correo electrónico; propagar virus; o realizar ataques de phishing.
5. Causar daño a otros o daños a su propiedad.
6. Usar lenguaje profano, abusivo o descortés; el acoso cibernético, el cual incluye amenazar, acosar o hacer declaraciones dañinas o falsas sobre otros; o acceder, transmitir o descargar materiales ofensivos, acosadores o despectivos.
7. Eliminar, copiar, modificar o falsificar los nombres, correos electrónicos, archivos o datos de otros usuarios que disfracen la identidad de uno, hacerse pasar por otros usuarios o enviar correos electrónicos anónimos.
8. Dañar la tecnología, el equipo, los archivos, los datos o la red de alguna manera, incluyendo el acceso, la transmisión o la descarga intencional de virus informáticos u otros archivos o programas dañinos o la interrupción del rendimiento de cualquier sistema de informática.
9. Usar cualquier Tecnología del Distrito para perseguir la “piratería”, ya sea en objetivos internos o externos al distrito o intentar acceder a información protegida por las leyes de privacidad.
10. Acceder, transmitir o descargar archivos de gran tamaño, en particular, pero no limitado a, el uso de Programa de software “torrent” para descargar ilegalmente materiales digitales protegidos por derechos de autor, o el uso de alcance insuficiente valioso para actividades no académicas como juegos en red o servir de anfitrión para dichas actividades.
11. Usar el correo electrónico o los servicios web para distribuir "cartas en cadena" o cualquier tipo de "esquemas piramidales".

12. Usar sitios web, correo electrónico, redes u otra tecnología con fines políticos o beneficio personal, incluyendo publicidad, o promover sitios web o eventos y esfuerzos comerciales que no sean del distrito. La propiedad de Internet e intranet del distrito no debe usarse para beneficio personal. Los estudiantes no deben acceder, crear, almacenar o transmitir intencionalmente material que pueda considerarse ofensivo, indecente, obsceno, intimidante u hostil; o material que acose, insulte o ataque a otros. Los estudiantes no deben violar ninguna de las leyes de derechos de autor aplicables. Eso incluye, pero no limitado a, la instalación de software en las computadoras del distrito para el cual el estudiante no tiene una licencia de software válida y vigente.

Información de Apoyo u Obligaciones Adicionales

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

Políticas de Seguridad y Contraseñas de la red

1. Los estudiantes deben informar cualquier debilidad en la seguridad de Internet e intranet del Distrito o algún incidente de posible uso indebido o violación de este acuerdo al Webmaster del Distrito, enviando un correo electrónico a:webmaster@fresnounified.org.
2. Los estudiantes no deben intentar acceder a ningún dato o programa para el que no tengan autorización o consentimiento explícito.
3. La tecnología distrital incluye redes y servicios que son recursos compartidos. Los estudiantes no deben participar en actividades que degraden deliberadamente el rendimiento de los sistemas de Tecnología del Distrito y la propiedad de Tecnología de la Información relacionada; privar a un Estudiante autorizado del Distrito de acceso a un recurso del Distrito; obtener recursos adicionales a los asignados; o eludir las medidas de seguridad del Distrito.
4. Los estudiantes no deben descargar, instalar o ejecutar programas de seguridad o utilidades que revelen o exploten debilidades en la seguridad de los sistemas de Tecnología de la Información del Distrito y la propiedad de Tecnología de la Información relacionada.
5. Todos los datos privados deben ser mantenidos en forma confidencial y seguros por el Estudiante. El hecho de que los datos puedan almacenarse electrónicamente no cambia el requisito de mantener la confidencialidad y seguridad de la información. Más bien, el tipo de información o la información en sí es la base para determinar si los datos deben mantenerse en forma confidencial y seguros. Si estos datos se almacenan en documento o en formato electrónico, o si los datos son copiados, imprimidos o transmitidos electrónicamente, los datos deben seguir estando protegidos si son confidenciales y seguros.
6. Todos los programas de software, aplicaciones, código de recursos, código de objetivo, documentación y datos deben ser guardados y protegidos.
7. El Distrito se reserva el derecho de eliminar cualquier contenido (organizacional o personal) en Internet o intranet en cualquier momento, sin motivo ni aviso.

8. No hay garantía de privacidad personal o acceso a la tecnología del Distrito. El distrito se reserva el derecho de buscar y/o supervisar cualquier información creada, accedida, enviada, recibida y/o almacenada en cualquier formato por cualquier empleado del distrito sobre el equipo del distrito o cualquier equipo conectado a la red del distrito.
9. Todo el software comercial usado en los sistemas sobre la Tecnología del Distrito está protegido por derechos de autor y designada para el uso del Distrito. Los estudiantes deben acatar todos los acuerdos de licencia.

Inteligencia Artificial

El uso de la tecnología de Inteligencia Artificial (AI) en nuestro ambiente educativo tiene como objetivo mejorar las experiencias de aprendizaje y fomentar la innovación. La tecnología de Inteligencia Artificial (AI) se define e incluye, pero no se limita a, Modelos de Lenguaje Grande (LLM), Aprendizaje Automático (ML) y Plataformas de Procesamiento de Lenguaje Natural (NLP). Se espera que todos los estudiantes usen los Recursos de Inteligencia Artificial (AI) de forma responsable y ética. Esto incluye respetar la privacidad de las personas, revisar todo el contenido generado por IA y comparar las afirmaciones factuales con las fuentes verificables, y abstenerse de usar AI con fines maliciosos o inapropiados.

1. Los estudiantes seguirán todas las directrices establecidas por los maestros y el personal escolar en relación con el uso del AI como parte de la planificación, la instrucción y el aprendizaje.
2. Los estudiantes deben adherirse con los términos de servicio (TOS) de la plataforma de AI y las leyes federales y estatales de privacidad de información de los estudiantes, y los maestros y el personal deben solicitar el Consentimiento de los padres cuando sea necesario.
3. Se prohíbe a los estudiantes usar cualquier sistema de AI para acceder, crear o mostrar material dañino, engañoso o inapropiado que sea amenazante, obsceno, disruptivo o sexualmente explícito, o que pueda interpretarse como acoso o menosprecio hacia otros en base a sexo, raza percibida, color, ascendencia, origen nacional, edad, credo religioso, estado civil, embarazo, discapacidad física o mental, condición médica, información genética, condición militar y estatus de veterano, orientación sexual, género, identidad de género, o asociación con una persona o grupo con una o más de estas características reales o percibidas, o interactuar con la AI de una manera que apoye cualquiera de lo mencionado anteriormente.
4. Los estudiantes no deben compartir información confidencial o información personal identificable con un sistema de AI sobre ellos mismos, estudiantes, miembros del personal u otros. La información de identificación personal incluye, entre otras, el nombre de una persona, domicilio, dirección de correo electrónico, número de teléfono, número de Seguro Social u otra información de identificación personal.
5. Los estudiantes no emplearán sistemas AI para tomar decisiones de alto riesgo que impacten significativamente la vida de las personas sin la debida supervisión humana, transparencia o la posibilidad de Apelación.
6. Los estudiantes no permitirán que los sistemas AI funcionen sin supervisión y tomen

decisiones que pueden poner en peligro la seguridad en ambientes industriales peligrosos, vehículos, infraestructuras, etc.

7. Se espera que los alumnos acrediten adecuadamente cualquier información generada por la IA cuando se utilice en trabajos profesionales, académicos o creativos.

Política de contraseñas

1. Las contraseñas deben tratarse como información confidencial.
2. Ningún miembro del personal debe pedir ni recibir otra contraseña de estudiante, ni siquiera con el propósito de ayudar.
3. La contraseña se deberá cambiar al menos cada 180 días. Sin embargo, el distrito puede, a su entera discreción, imponer cambios periódicos de contraseña basado en la responsabilidad y el uso de la función.
4. Las contraseñas predeterminadas se deben cambiar dentro de un día.
5. La complejidad de la contraseña debe ajustarse a la política de contraseñas según las funciones, la responsabilidad, o lo apropiado para la edad del estudiante.
6. Las contraseñas no deberán incluir su número de empleado, nombre, número de seguro social, número de teléfono, fecha de nacimiento, ni el nombre de su departamento o escuela.
7. Todas las violaciones de seguridad deberán ser reportadas a la escuela o al administrador/a del departamento.

Controles de acceso, Seguridad de la Información y Responsabilidad

1. Los departamentos y escuelas que cuentan con Tecnología del Distrito deben proveer controles de acceso apropiados para supervisar y proteger los datos de negocios y los programas asociados contra el mal uso indebido.
2. Todos los estudiantes son responsables de administrar su propio uso de la Tecnología del Distrito y son responsables de sus acciones relacionadas con la seguridad. Los estudiantes también, son responsables de reportar cualquier violación sospechada o confirmada de esta política a la administración apropiada responsable del manejo de incidentes de seguridad del sistema de Tecnología de la Información de FUSD.
3. Se pudieran llevar a cabo evaluaciones con regularidad de la ciberseguridad de los usuarios para medir la preparación de la organización o para apoyar al personal en la educación en seguridad cibernética.
4. El acceso a los equipos de tecnología de la información del FUSD deben estar debidamente documentados, autorizados y controlados.
5. La autoridad de acceso para cada estudiante se revisará de forma regular, así como en cada cambio de estado laboral, como: una transferencia, promoción, degradación o terminación del servicio.
6. Las Escuelas y Departamentos responsables de la custodia y operación de la tecnología del Distrito deberán ser responsables de la autorización adecuada y el uso de la tecnología relacionada, el establecimiento del uso eficaz y la presentación de reportes de desempeño a la administración.

7. Algunos miembros del personal del Distrito deben usar una VPN u otros procedimientos de seguridad de red aprobados para acceder a los sistemas o datos internos cuando trabajan de forma remota.
8. Al finalizar la relación con el FUSD, se aplican todas las políticas de seguridad de FUSD y permanecen en vigor después de que se termina la relación.
9. Es posible que se requiera que el personal que acceda a los recursos del distrito use la autenticación multifactor (MFA).
10. Se requerirá que el personal use inicios de sesión con acceso elevado cuando acceda a Recursos susceptibles del distrito para asegurar un acceso limitado y controlado dentro del ecosistema de tecnología empresarial de la organización.
11. El uso indebido de cuentas no humanas, que son cuentas de usuario creadas para el acceso automatizado o programático a sistemas y servicios, está estrictamente prohibido. Esto incluye el acceso no autorizado, la manipulación o el desarrollo de bots automatizados, procesos o scripts por parte de los empleados para llevar a cabo actividades no autorizadas.
12. El acceso a los recursos en línea del distrito puede estar bloqueado desde ubicaciones fuera de los Estados Unidos.
13. El personal ya no tendrá acceso a ningún sistema de los distritos ni a tecnología física después de su último día laboral.

Retención de Documentos

Es responsabilidad de cada empleado guardar y/o archivar el correo electrónico que recibe y al que desea acceder posteriormente o que son registros del Distrito y que la ley requiere que se conserven. Los correos electrónicos deben ser guardados únicamente en la bandeja de entrada de correo electrónico en línea o en la carpeta de archivo, o en un Repositorio de Documentos SharePoint o OneDrive apropiado. Está prohibido archivar correos electrónicos relacionados con el distrito fuera de un sistema del Distrito Escolar Unificado de Fresno.

Si almacena dichos documentos fuera de sus ubicaciones requeridas, puede estar sujeto a medidas disciplinarias.

Uso Incidental

Para conveniencia de la comunidad de estudiantes del Distrito, se permite el uso personal incidental de la tecnología del Distrito. La Política de AUP se sigue aplicando al uso incidental con la adición de las siguientes limitaciones:

1. El uso personal incidental de la tecnología del Distrito por parte de los estudiantes no se extiende a los miembros de la familia u otros conocidos.
2. El uso personal incidental no debe resultar en costos directos para el Distrito.
3. El uso personal incidental no debe interferir con el desempeño normal de las obligaciones laborales de un empleado o el aprendizaje del estudiante.

Cumplimiento / Reglamento a la que contribuye esta Política

Esta Política de Uso Aceptable se basa, en parte, en los requisitos o conceptos de lo siguiente:

1. Ley de Derechos Educativos y Privacidad Familiar (FERPA) de 1974
2. Ley de Portabilidad y Responsabilidad del Seguro Médico de (HIPAA) 1996
3. Ley de Protección de los Niños en Internet (CIPA) de 2000 (CIPA)
4. Enmienda Sobre la 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 Información Personal Estudiantil en Línea (SB1177)

Aceptación

Con base en este aviso y el uso de la Tecnología del Distrito por parte de su estudiante, padres y estudiantes esta Política de Uso Aceptable también aceptan y reconocen la importancia de la responsabilidad personal con estas políticas, incluyendo, entre otras, las siguientes.

Responsabilidades de los Padres/Tutores:

- Supervise el uso del dispositivo por parte de su estudiante fuera de la red del Distrito.
- Revise y discuta la Política de Uso Aceptable (AUP, por sus siglas en inglés) del Distrito con su estudiante.
- Regresar el dispositivo si lo solicitó, o si su estudiante se da de baja o se gradúa del Distrito Escolar Unificado de Fresno.
- Pagar las cuotas asociadas con el reemplazo o reparación de computadoras dañadas.
- Indemnizar y eximir de responsabilidad al Distrito y al personal del Distrito por cualquier daño o costo que surja de o esté relacionado con una violación de la Política de Uso Aceptable.