INFORMACIÓN SOBRE LA POLÍTICA DE USO RESPONSABLE (RUP) Y FORMULARIO DE CONFIRMACIÓN PARA EMPLEADOS

Propósito

El propósito de la Política de Uso Responsable del Distrito ("RUP") consiste en evitar el acceso no autorizado y otras actividades ilícitas por parte de los usuarios en línea, evitar la divulgación no autorizada de información sensible o el acceso a la misma, y cumplir con la legislación, que incluye entre otras, la Ley de Protección de la Niñez en Internet (CIPA), la Ley de Protección de la Privacidad de la Niñez en Línea (COPPA), la Ley de Privacidad y Derechos Educativos de la Familia (FERPA), y la Ley de Privacidad de las Comunicaciones Electrónicas de California (CalECPA). Además, la política RUP aclara el propósito educativo de la tecnología del Distrito.

El término “usuario”, según se utiliza en esta política, incluye a cualquier persona que use computadoras, internet, correo electrónico, y todas las otras formas de comunicación electrónica o equipo proporcionado por el Distrito (la “red”), independientemente de la ubicación física del usuario. La política RUP se aplica incluso cuando el equipo proporcionado por el Distrito (computadoras portátiles, tabletas, etc.) se utiliza fuera de la propiedad del Distrito. Además, la política RUP corresponde cuando los dispositivos que no son del Distrito acceden a la red del Distrito o a información confidencial.

El Distrito utiliza medidas de protección tecnológica para bloquear o filtrar el acceso, en la medida razonablemente posible, de representaciones visuales y escritas que sean obscenas, pornográficas, o perjudiciales para los menores a través de la red. El Distrito se reserva el derecho de supervisar las actividades en línea de los usuarios y de acceder, revisar, copiar, almacenar, o eliminar cualquier comunicación o archivo y revelarlos a terceros si lo considera necesario. Los usuarios no deben tener ninguna expectativa de privacidad con respecto a su uso de los bienes del Distrito, la red y/o acceso a Internet o archivos, incluido el correo electrónico. Los usuarios entienden que el Distrito tiene derecho a recuperar en cualquier momento el equipo que pertenece al Distrito.

El Distrito tomará todas las medidas necesarias para proteger la red contra posibles amenazas de ciberseguridad. Esto puede incluir el bloqueo del acceso a las aplicaciones del Distrito, que incluye, entre otros, el correo electrónico, las herramientas de gestión de datos e informes, y otras aplicaciones web fuera de Estados Unidos y Canadá.

La política RUP también corresponde al uso de herramientas de inteligencia artificial (AI), que incluyen entre otras, herramientas de AI generativa que pueden generar contenidos nuevos, incluyendo texto, imágenes, video, audio, estructuras, código informático, datos sintéticos, etc. en respuesta a indicaciones generadas por los usuarios.

Responsabilidad del Empleado

Si usted está supervisando a estudiantes que usan tecnología, permanezca atento para cerciorarse de que los estudiantes cumplan con las disposiciones descritas en la política RUP.

Civismo Digital

- Todos los usuarios tienen la responsabilidad de practicar una conducta cívica digital que sea positiva.
- Los empleados tienen la responsabilidad de aplicar la política del Distrito sobre el tiempo de pantalla. Esto incluye supervisar el tiempo que los estudiantes pasan frente a la pantalla y garantizar que se respeten los límites según el nivel de grado y las restricciones de contenido.
- No generar ni distribuir a imágenes, grabaciones, videos o declaraciones que tergiversen o busquen desinformar a los demás.
- Los empleados que utilizan la tecnología de aula tienen la obligación explícita de impartir conceptos a los estudiantes sobre el civismo digital positivo.
- Lo que los empleados hagan y publiquen en línea no debe interrumpir las actividades escolares ni poner en juego la precaución y seguridad escolar.

Privacidad

- No compartir información personal sobre estudiantes y empleados, incluyendo, entre otros datos, nombres, direcciones, fechas de nacimiento, números de teléfono, números de identificación de estudiante, números de empleados, y elementos visuales.
- No compartir información confidencial, sensible o privada sobre usted mismo o sobre otras personas en las instrucciones dirigidas a la IA, incluidas las herramientas de IA generativa, que abarcan entre otros datos, la información contenida en los expedientes de estudiantes o empleados, así como imágenes, vídeos o grabaciones de voz de estudiantes o empleados.
- Utilizar únicamente cuentas de correo electrónico creadas y contenidas dentro de los sistemas de red del Distrito (p.ej., las que terminan en "@LAUSD.NET") para transmitir Información de Identificación Personal (PII) de los registros educativos de los estudiantes a otras cuentas de correo electrónico de empleados del Distrito que tengan un interés legítimo, ya sea educativo o administrativo, en la información.
- La transmisión de información estudiantil a entidades externas (incluyendo agencias públicas como el Departamento de Libertad Condicional del Condado de Los Ángeles, el Departamento de Servicios para Menores y Familias del Condado de Los Ángeles, la Oficina de Educación del Condado de Los Ángeles, etc.) por correo electrónico del Distrito, deberá estar encriptada.
- Las solicitudes de información por entidades externas deberán canalizarse a la oficina correspondiente del Distrito.
- No reenviar automáticamente mensajes de una cuenta de correo electrónico del Distrito a ninguna cuenta que no sea del Distrito con el fin de crear un archivo de correo electrónico personal o para usar una sola cuenta de correo electrónico a fin de acceder tanto al correo electrónico personal y del Distrito.
- Si la información protegida debe compartirse a través de un servicio de intercambio de archivos o colaboración, utilizar únicamente un servicio que el Distrito haya aprobado para compartir dicha información.
- Tener en cuenta la política de privacidad de los sitios web y cómo recopilan y comparten la

información del Distrito.
- Cumplir con todas las leyes, esta Política de Uso Responsable, y todas las políticas de seguridad del Distrito.

Contraseñas
- Cumplir con la política del Distrito en relación con la gestión de contraseñas.
- Bajo ninguna circunstancia se podrán utilizar las cuentas de correo electrónico proporcionadas por el Distrito para fines personales, no autorizados, no integrados en el SSO y/o no relacionados con el Distrito.
- Bajo ninguna circunstancia deberán compartirse con los demás los nombres de usuarios y/o contraseñas del Distrito, incluyendo a otros empleados del Distrito y estudiantes, ya sea directa o indirectamente.

Lenguaje profesional
- Utilizar un lenguaje profesional en todas las comunicaciones relacionadas con el trabajo, incluyendo correo electrónico, publicaciones en redes sociales, grabaciones de audio, conferencias, obras artísticas, e instrucciones para herramientas de IA, incluidas las herramientas de IA generativa.

Ciberacoso
- El acoso en cualquier forma, incluido el ciberacoso, es inaceptable tanto dentro como fuera de la escuela.
- Reportar todos los casos de acoso al administrador del plantel u otra autoridad.

Material inapropiado
- No buscar, mostrar, o distribuir material que sea discurso de odio, sexualmente explícito, o violento mientras se esté en la escuela o mientras se haya identificado como empleado del Distrito.
- Podrán hacerse excepciones en un contexto educativo apropiado.
- El uso de la red del Distrito para fines ilegales, políticos, o comerciales queda estrictamente prohibido.
- La transmisión de archivos grandes no relacionados con los asuntos del Distrito y que cause interrupción en la red del Distrito queda prohibida.

Seguridad
- Todos los usuarios se responsabilizan de respetar y mantener la seguridad de los recursos y redes electrónicas del Distrito.
- Solo utilizar software y hardware que haya sido autorizado por el Distrito.
- No utilizar la red o el equipo del Distrito para obtener información no autorizada, intentar acceder a información protegida por leyes de privacidad, o hacerse pasar por otros usuarios.
- No tratar de eludir la configuración de seguridad y los filtros, lo cual incluye el uso de servidores proxy para acceder a sitios web bloqueados por el Distrito.
- No instalar ni utilizar software o archivos ilegales, lo cual incluye software o apps no autorizados, en ninguna de las computadoras, tabletas, teléfonos inteligentes, u otras tecnologías nuevas del Distrito.

- El acceso remoto a la red del Distrito debe ocurrir a través de un canal autorizado como se describe en el documento BUL- 1597, Política de uso Aceptable para los Servicios de Red Privada Virtual (VPN) de ITD.
- Revisar todos los resultados generados por las herramientas de IA, especialmente las de IA generativa, para comprobar su precisión y adecuación, ya que se ha demostrado que estas herramientas pueden presentar información falsa como si fuera veraz.
- Los empleados deben orientar a los estudiantes sobre el uso ético y responsable de la IA, incluyendo la citación adecuada, en caso de que se les permita utilizar la IA para los trabajos de clase.

Seguridad de Equipos y Redes

- El equipo, la información o el software, independientemente de su forma o medio de almacenamiento, no pueden ser retirados del plantel sin el permiso previo por escrito del administrador de un empleado.
- Tomar todas las precauciones razonables para proteger el equipo del Distrito y si el equipo está autorizado para su uso fuera del plantel, solo debe ser controlado por la persona a la que se le concedió permiso para retirarlo del plantel.
- Tener cuidado al descargar archivos o abrir correos electrónicos, ya que los archivos adjuntos podrían contener virus o malware.
- El vandalismo en cualquier forma está prohibido y debe ser reportado al administrador correspondiente y/o personal técnico.
- Informar inmediatamente sobre equipos perdidos o robados al personal de seguridad de IT.
- Informar de las deficiencias del sistema o de los incidentes de seguridad relacionados con los datos protegidos del Distrito o con los sistemas de información que albergan datos protegido al personal de Seguridad de IT.

Retirar del Escritorio y la Pantalla

- Los empleados que no se encuentren en su lugar de trabajo asignado deben asegurarse de que todos los documentos protegidos en papel, así como los medios de almacenamiento de datos con información protegida, se retiren del escritorio o de otros lugares (por ejemplo, impresoras, faxes, fotocopiadoras, etc.) para evitar el acceso no autorizado.
- Los empleados que no se encuentren en su lugar de trabajo asignado deben asegurarse de que toda la información protegida se retire de la pantalla de su computadora, y se impida el acceso a todos los sistemas que el empleado esté autorizado a usar, ya sea cerrando la sesión de la red del Distrito, bloqueando la pantalla con una contraseña, o apagando la computadora.

Derechos de autor

- Si bien existen exenciones de uso justo, todos los usuarios deben respetar la propiedad intelectual.
- Seguir todas las directrices de derechos de autor cuando se utilice el trabajo de otros autores.
- No descargar música, software, aplicaciones, ni otras obras obtenidas ilegalmente.
- Citar material generado por herramientas de IA, incluidas las herramientas generativas de IA, cuando se utilicen.

Consecuencias del Uso Irresponsable

- El incumplimiento de las responsabilidades enumeradas anteriormente constituye uso indebido. El uso indebido de los dispositivos y redes del Distrito puede generar como resultado:
  - Acceso restringido o cancelación de la cuenta
  - Acción Disciplinaria
  - Acciones legales contra los empleados, que incluyen medidas disciplinarias o procesos penales por parte de las autoridades públicas.
  - El Distrito intentará adaptar cualquier acción disciplinaria a los asuntos específicos relacionados con cada violación.

Descargo de Responsabilidad

El Distrito no garantiza la calidad de los servicios prestados y se deslinda de todo reclamo, pérdida, daño, costo, u otras obligaciones derivadas del uso de la red o cuentas del Distrito. Los usuarios se hacen responsables de cualquier cargo incurrido durante el uso de los dispositivos del distrito y/o la red. Asimismo, el Distrito se deslinda de toda responsabilidad por la exactitud o calidad de la información obtenida a través del acceso de los usuarios. Cualquier declaración accesible en línea se entiende como el punto de vista individual del autor y no el del Distrito, sus afiliados o sus empleados.

Instrucciones:

Después de haber leído la información anterior, firmar a continuación y entregar el documento a su administrador o personal de supervisión designado.

He leído, comprendo, y acepto cumplir las disposiciones de la Política de Uso Responsable del Distrito Escolar Unificado de Los Ángeles.

Oficina/Escuela:_____

Nombre del Empleado:_____ Número de Empleado: _____

Firma del Empleado:_____ Fecha:_____

Favor de entregar este formulario a su supervisor o administrador, donde se mantendrá archivado. Se requiere para todos los empleados que vayan a utilizar una red de computación y/o acceso a Internet.