DISTRITO ESCOLAR UNIFICADO DE HAMILTON

Departamento de Tecnología | Acuerdo de Uso Aceptable de Tecnología y Política de Dispositivos (SY 2026–2027) — Página 1

Nota: Las configuraciones operativas, las aplicaciones aprobadas y las medidas de seguridad pueden cambiar durante el año escolar en respuesta a requisitos operativos, educativos, legales o de ciberseguridad.

1. AUTORIZACIÓN, PROPÓSITO Y PROPIEDAD DEL DISTRITO

El Distrito Escolar Unificado de Hamilton (HUSD) autoriza a los estudiantes y al personal ("usuarios") a acceder a los recursos tecnológicos del distrito—incluyendo la infraestructura de red, Chromebooks, cuentas de Google Workspace, acceso a Internet y software educativo—exclusivamente con fines educativos y administrativos legítimos. El acceso a la tecnología es un privilegio permitido a discreción del Distrito, sujeto a la Política de la Mesa Directiva BP 4040, las Regulaciones Administrativas y esta Política de Uso Aceptable (AUP).

Propiedad del Distrito: Todas las computadoras, la infraestructura de red, los dispositivos móviles, las cuentas de usuario electrónicas (`@husdschools.org`) y los archivos creados/almacenados siguen siendo propiedad exclusiva del Distrito Escolar Unificado de Hamilton. El Distrito se reserva el derecho de recolectar, inspeccionar, alterar o revocar el acceso a cualquier tecnología del distrito en cualquier momento sin previo aviso.

2. CONTROLES DE SEGURIDAD ADMINISTRADOS, CONFIDENCIALIDAD Y CONTROL DE APLICACIONES

Para proteger la privacidad de los estudiantes y salvaguardar las redes del distrito contra amenazas cibernéticas, HUSD aplica un modelo de controles de seguridad administrados (marco de modelo Zero Trust / Confianza Cero):

- **Confidencialidad de la Cuenta:** Los usuarios son los únicos responsables de sus cuentas asignadas. Las contraseñas deben mantenerse estrictamente confidenciales. Queda estrictamente prohibido compartir cuentas o acceder a la cuenta de otra persona.
- **Controles de Aplicaciones Administradas:** Las cuentas de los estudiantes tienen restringida la autenticación en aplicaciones de terceros externas mediante Google Sign-In u OAuth sin aprobación previa de TI. Todo el software educativo externo debe pasar por una revisión de privacidad e identificarse en alineación con los Acuerdos de Privacidad de Datos de Estudiantes de California (CA-NDPA).
- **Complementos de Automatización Prohibidos:** Las herramientas de automatización de correo electrónico no aprobadas, complementos de combinación de correspondencia y extensiones de navegador no verificadas están bloqueadas en todo el dominio para reducir riesgos de phishing.
- **Registro Aprobado:** La lista completa de herramientas aprobadas por el distrito se mantiene en vivo en: **https://www.husdschools.org/departments/technology/approved-third-party-google-apps**

3. GOBERNANZA DE INTELIGENCIA ARTIFICIAL GENERATIVA (IA)

HUSD reconoce el valor educativo de la Inteligencia Artificial al tiempo que mantiene rigurosas barreras de privacidad e instrucción:

- **Plataforma Oficial del Distrito: Gemini en Google Workspace for Education** (administrado bajo las cuentas de Google Workspace de HUSD) es la herramienta de IA generativa oficialmente aprobada por el Distrito. Los datos de Workspace procesados a través de Gemini están excluidos del entrenamiento de modelos públicos de IA.
- **Estándar de Control Humano:** Las herramientas de IA sirven para aumentar, no reemplazar, el pensamiento crítico humano y el juicio educativo. Todo contenido generado por IA debe ser revisado y verificado antes de su uso.
- **Prohibición Estricta de Datos Sensibles:** Queda estrictamente prohibido ingresar Información de Identificación Personal (PII) de estudiantes (nombres, IDs, direcciones, datos de IEP), registros confidenciales de empleados, expedientes disciplinarios, información médica, documentos legales o comunicaciones de abogado-cliente en cualquier plataforma de IA.
- **IA de Consumo Prohibida:** Las herramientas de IA no verificadas de nivel de consumo (ej. ChatGPT comercial, Claude, bots de calificación no aprobados) están bloqueadas para estudiantes y restringidas para el personal para evitar la recolección comercial de datos.

Nota: Las configuraciones operativas, las aplicaciones aprobadas y las medidas de seguridad pueden cambiar durante el año escolar en respuesta a requisitos operativos, educativos, legales o de ciberseguridad.

4. CONTENIDO EXTERNO Y PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (COPIA PLANA)

Para mitigar macros maliciosas y la ejecución de código en segundo plano desde repositorios no verificados (ej. Teachers Pay Teachers / TPT):

> **Requisito de Importación Sanitizada:** El personal que compre o descargue materiales educativos de terceros en dispositivos personales del hogar debe convertir los archivos en copias estáticas y planas (ej. "Imprimir en PDF" o "Guardar como imagen/JPEG") antes de transferirlos a computadoras escolares. Se prohíbe el enlace directo de cuentas de Google Drive con mercados de archivos externos.

5. CIUDADANÍA DIGITAL, SEGURIDAD Y CUMPLIMIENTO LEGAL

Los usuarios deben adherirse a altos estándares de ciudadanía digital. Las siguientes conductas están estrictamente prohibidas y constituyen violaciones de la política:

- **Material Nocivo u Obsceno:** Acceder, crear o difundir material obsceno, sexualmente explícito, discriminatorio o nocivo para menores (Cód. Penal de Cal. 313).
- **Acoso Cibernético:** Amenazar, intimidar o acosar a estudiantes, personal o miembros de la comunidad mediante correo electrónico, Documentos compartidos, chat o plataformas en línea.
- **Acceso No Autorizado al Sistema ("Hacking"):** Intentar evadir los filtros web, alterar configuraciones del sistema, elevar privilegios, ejecutar herramientas de explotación o acceder a sistemas confidenciales de registros estudiantiles (Cód. Penal de Cal. 502).
- **Uso Comercial y Derechos de Autor:** Utilizar las redes del distrito para lucro comercial personal, cabildeo político o descarga no autorizada de medios con derechos de autor.

6. EXPECTATIVAS DE PRIVACIDAD Y MONITOREO TECNOLÓGICO

Expectativas de Privacidad: Los dispositivos, cuentas y redes propiedad del distrito están sujetos a monitoreo, inspección y registro con fines educativos, operativos y de seguridad legítimos. Los usuarios no deben esperar privacidad personal al utilizar los recursos tecnológicos del Distrito. Las herramientas de monitoreo incluyen:

- **Firewall Palo Alto de Última Generación:** Inspección de tráfico de red y filtrado web.
- **Sistemas de Aula y Seguridad GoGuardian:** Visibilidad de pantalla en tiempo real, registro de actividades y alertas de seguridad.
- **Seguridad de Puntos Finales y API:** Protección contra amenazas en puntos finales y registros administrativos de Google Admin.

Nota: Las configuraciones operativas, las aplicaciones aprobadas y las medidas de seguridad pueden cambiar durante el año escolar en respuesta a requisitos operativos, educativos, legales o de ciberseguridad.

7. NORMAS DE USO DE CHROMEBOOKS Y DISPOSITIVOS Y TABLA DE TARIFAS POR DAÑOS

Los estudiantes asignados a un Chromebook o dispositivo de HUSD deben cumplir con las normas de cuidado: traer el dispositivo completamente cargado diariamente en su funda protectora, no dejar dispositivos desatendidos ni colocar calcomanías o marcas en el equipo, y reportar la pérdida o daño físico a la oficina de la escuela de inmediato.

Tabla de Tarifas por Daños de Chromebooks / Dispositivos HUSD (SY 2026–2027)

Nivel de Incidente	Cobertura del Distrito	Responsabilidad Financiera del Padre/Usuario
1.ª Infracción (Accidental)	El Distrito cubre el 100% del costo de reparación / reemplazo.	**Costo $0** (Dispositivo Completo, Cargador, Pantalla, Teclado)
2.ª Infracción (Repetida)	El Distrito cubre el 50% del costo de reparación / reemplazo.	Dispositivo Completo: **$200** | Pantalla: **$75** | Teclado: **$50** | Cargador: **$25**
3.ª Infracción y Abuso Intencional	El usuario es responsable del 100% del costo de reparación / reemplazo.	Dispositivo Completo: **$400** | Pantalla: **$150** | Teclado: **$100** | Cargador: **$50**

Bloque de Firma de Acuerdo del Estudiante y Padre/Madre/Tutor

He leído, entiendo y acepto cumplir con los términos del Acuerdo de Uso Aceptable de Tecnología de HUSD y la Política de Dispositivos para el año escolar 2026–2027. Entiendo que la violación de estas reglas puede resultar en la revocación de privilegios tecnológicos, medidas disciplinarias o responsabilidad financiera por equipos dañados.

Nombre del Estudiante (letra de molde): _____ **Grado Escolar:** _____

Firma del Estudiante: _____ **Fecha:** _____

Nombre del Padre/Madre/Tutor (letra de molde): _____

Firma del Padre/Madre/Tutor: _____ **Fecha:** _____