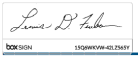
DISTRICT OF COLUMBIA PUBLIC SCHOOLS

This *Student and Staff Technology and Network Acceptable Use Policy* rescinds and supersedes all previous policy, memoranda, and/or guidance promulgated by DCPS on this subject matter.

Chancellor Approval: 

Effective: August 26, 2024

Política de uso aceptable de la red y tecnología para estudiantes y personal

I. PROPÓSITO Y OBEJTIVO

Las Escuelas Públicas del Distrito de Columbia (DCPS, por sus siglas en inglés) proporcionan a los estudiantes y al personal acceso a Internet, datos y sistemas de red (red de las DCPS). Las DCPS también proporcionan a los estudiantes y al personal acceso a computadoras, tabletas, dispositivos y otras tecnologías, como impresoras (dispositivos o tecnología de las DCPS). La red de las DCPS y la tecnología de las DCPS se proporcionan al personal con fines de planificación, enseñanza y administración; y se proporciona a los estudiantes con fines educativos, de investigación y de desarrollo profesional. Esta política tiene como objetivo:

- Establecer estándares para los usos aceptables de la red de las DCPS y la tecnología de las DCPS;
- Establecer expectativas en torno al uso responsable de la inteligencia artificial;
- Prevenir los usos no autorizados e ilegales de la red de las DCPS y la tecnología de las DCPS; y
- Cumplir con la Ley de Protección de los Niños en Internet de 2000 (CIPA, por sus siglas en inglés), la Ley de Protección de la Privacidad en Línea para Niños (COPPA, por sus siglas en inglés), la Ley de Protección de la Privacidad Digital de los Estudiantes y todas las demás leyes, reglamentos, políticas y procedimientos aplicables.

Esta política se aplica a todos los estudiantes, el personal, los visitantes y otras personas que usan la red o los dispositivos de las DCPS, y rescinde la previa Política de uso aceptable de la red y tecnología para estudiantes y personal de las DCPS (2021.)

II. AUTORIDAD Y LEY APLICABLE[1]

Fuente	**Referencia**
Ley Federal	- Ley de Protección de los Niños en Internet (CIPA), codificada en 47 U.S.C. § 254(h)(5) - Ley de Protección de la Privacidad en línea para Niños de 1998 (COPPA), codificada al 15 U.S.C. § 6501 *y siguientes*. - Ley de Protección de Internet para Niños del Vecindario, codificada al 47 U.S.C. § 254(l)
Reglamentos Federales	- Regla de protección de la privacidad en línea de los niños, 16 C.F.R. Parte 312
Ley del Distrito de Columbia	- Ley de Protección de la Privacidad Digital de los Estudiantes de 2016, Ley del Distrito de Columbia 21-218, codificado al Código Oficial del Distrito de Columbia 38-831.01 *y siguientes*.
Reglamentos Municipales del Distrito de Columbia	- 5-B DCMR § 2500 *y siguientes*. – Disciplina Estudiantil - 6-B DCMR § 1610 – Disciplina progresiva de los empleados

[1] Nada en esta política reemplaza las leyes federales, estatales o locales.

III. TÉRMINOS CLAVE Y DEFINICIONES

Inteligencia artificial (AI, por sus siglas en inglés) significa una rama de las ciencias de la computación que se ocupa de la simulación del comportamiento inteligente en las computadoras..

Red de las DCPS se refiere a los sistemas de Internet, datos y redes proporcionados por las DCPS a todos los estudiantes y personal de las DCPS.

Personal de las DCPS se refiere a todos los empleados de las DCPS (a tiempo completo o parcial), contratistas, agentes, representantes, voluntarios o cualquier otra persona que actúe en nombre de las DCPS y que tenga acceso a la red y la tecnología de las DCPS.

Tecnología de las DCPS se refiere a computadoras, tabletas, dispositivos y otra tecnología proporcionada por las DCPS a los estudiantes y al personal.

Expulsión significa la remoción de un estudiante de la escuela de inscripción del estudiante por razones disciplinarias por el resto del año escolar o más, de acuerdo con la política de la agencia educativa local.

Información personal se refiere a la información que, cuando se utiliza sola o en combinación con otros datos relevantes, puede identificar a una persona. La información personal incluye, entre otros, el nombre completo; domicilio u otra dirección física; nombre de "pantalla" o nombre de usuario cuando funciona como información de contacto en línea; y un archivo de foto, audio o video que contenga la imagen o la voz de una persona.

Disciplina progresiva significa un sistema disciplinario de los empleados que proporciona una gama gradual de respuestas a los problemas de desempeño y/o conducta de los empleados. Los pasos disciplinarios progresivos de las DCPS incluyen asesoramiento verbal, advertencia, reprimenda y acción adversa.

Suspensión significa la remoción temporal de un estudiante del horario regular de clases del estudiante como consecuencia disciplinaria, tiempo durante el cual el estudiante permanece en las instalaciones de la escuela bajo la supervisión del personal de la escuela o no se le permite ingresar a las instalaciones de la escuela.

IV. REQUISITOS

A. General

Las DCPS proporcionan y autorizan el uso de la red y la tecnología de las DCPS para el personal y los estudiantes. Al proporcionar y autorizar el uso de recursos tecnológicos, las DCPS no renuncian a la propiedad ni al control sobre la tecnología y los materiales de los sistemas proporcionados por las DCPS. A excepción de lo que se describe a continuación, no existe ninguna expectativa de privacidad

relacionada con la información almacenada o transmitida a través de la red de las DCPS o en los sistemas de las DCPS, y las DCPS se reservan el derecho de acceder, revisar, copiar, almacenar o eliminar cualquier archivo almacenado en la tecnología de las DCPS o en las cuentas de la red de las DCPS y todas las comunicaciones que utilicen la red de las DCPS. Los mensajes electrónicos y los archivos almacenados en las computadoras de las DCPS o transmitidos utilizando los sistemas de las DCPS pueden ser tratados como cualquier otra propiedad escolar. El personal de las DCPS puede revisar archivos y mensajes para llevar a cabo investigaciones, cumplir con los requisitos legales, mantener la integridad del sistema y, si es necesario, para garantizar que los usuarios de la tecnología y de la red actúen de manera responsable y alineada con esta política. Todas las cuentas creadas por las DCPS para los estudiantes o el personal pueden ser monitoreadas por las DCPS.

1. Estudiantes

Las DCPS notificarán esta política a través del proceso de inscripción anual, y se les pedirá a todos los padres y estudiantes adultos que acusen recibo de esta. Es posible que se requiera que los estudiantes y los padres firmen un Acuerdo de Uso Responsable de la Red y la Tecnología Estudiantil (Acuerdo de Uso Responsable del Estudiante), incluido en los Apéndices y disponible en el sitio web de las DCPS. El Acuerdo de Uso Responsable del Estudiante describe el uso responsable y las actividades prohibidas para los estudiantes que usan la tecnología de las DCPS o que acceden a la red de las DCPS. Las escuelas también pueden exigir a los estudiantes y a los padres que firmen acuerdos específicos de la escuela que detallen los procesos de registro de entrada y salida de la tecnología, identifiquen al personal de la escuela con funciones específicas relacionadas con la tecnología y establezcan reglas específicas de la escuela.

Las DCPS ofrecen a los estudiantes lecciones anuales sobre ciudadanía digital y seguridad en línea. Se requiere que los estudiantes realicen los cursos en el Centro de Estudiantes de Ciudadanía Digital y Alfabetización,[2] incluyendo el módulo sobre el uso y cuidado del dispositivo, y es posible que se requiera realizar un curso antes de que un estudiante reciba un dispositivo o cuenta de las DCPS.

El incumplimiento de estas reglas se abordará bajo los reglamentos y políticas disciplinarias de las DCPS, incluida la Política de Estudiantes Seguros y Positivos,[3] y puede resultar en la pérdida de acceso a la red las DCPS o a la tecnología de las DCPS durante períodos de tiempo cada vez mayores; siempre que los estudiantes puedan participar y hacer el trabajo de clase a través de medios alternativos y puedan recibir todos los servicios necesarios de educación especial y de aprendizaje de inglés. En algunos casos, la mala conducta también puede constituir una infracción penal.

2. Personal

Las DCPS notificarán esta política al personal nuevo a través del proceso de incorporación, y el Acuerdo de Uso Responsable de Tecnología del Personal (Acuerdo de Uso de Respuesta del Personal) incluido en los Apéndices, estará disponible en el sitio web de las DCPS como una referencia adicional y continua. También se le puede pedir al personal al que se le ha asignado un dispositivo de las DCPS que firme o vuelva a firmar un Formulario de Reconocimiento del Acuerdo de Uso Responsable de Tecnología del Personal antes o después de recibir su dispositivo.

[2] *Disponible en* https://dcps.instructure.com/enroll/Y8Y7KY.
[3] *Disponible en* https://dcps.dc.gov/page/dcps-policies.

El Gobierno del Distrito de Columbia, la Oficina del Director de Tecnología (OCTO, por sus siglas en inglés) del Distrito de Columbia y/o las DCPS pueden requerir que el personal realice la capacitación de los empleados relacionada con la ciberseguridad o temas relacionados. El personal que no realice esas capacitaciones de manera oportuna o no siga esta política puede estar sujeto a medidas disciplinarias progresivas.

B. Redes, correo electrónico y aplicaciones

1. Red

La red de las DCPS y la tecnología de las DCPS se proporcionan al personal con fines de planificación, enseñanza y administración; y se proporciona a los estudiantes con fines educativos, de investigación y de desarrollo profesional. La red de las DCPS permite al personal y a los estudiantes acceso interno a la información y los recursos de las DCPS, a las solicitudes aprobadas por las DCPS y al acceso externo a Internet. El acceso a la red de las DCPS, incluido el Internet, se proporciona a los estudiantes únicamente para apoyar la educación, la investigación y el desarrollo profesional de los estudiantes. El uso de la red las DCPS es un privilegio. El personal y los estudiantes que violen cualquier parte de esta política o políticas relacionadas pueden estar sujetos a la cancelación de sus privilegios para usar la red de las DCPS y posibles acciones disciplinarias.

El acceso a la red y el ancho de banda se proporcionan a las escuelas para servicios académicos y operativos. Las DCPS se reserva el derecho de priorizar el ancho de banda de la red y limitar ciertas actividades de la red que están afectando negativamente los servicios académicos y operativos. Los usuarios de la red tienen prohibido usar la red de las DCPS para acceder a contenido considerado inapropiado o ilegal, incluido, entre otros, contenido pornográfico, obsceno, ilegal o que promueva la violencia.

Las DCPS no garantizan que las funciones o la calidad de los servicios de red que proporciona estén libres de errores o defectos. Las DCPS no son responsables de ningún reclamo, pérdida, daño, costo u otras obligaciones que surjan del uso de la red o las cuentas. Cualquier cargo en el que incurra una persona debido al uso de la red correrá a cargo únicamente de la persona. Las DCPS no son responsables de la exactitud o calidad de la información obtenida a través del uso del sistema, a menos que la información sea contenido producido por las DCPS. Cualquier declaración no producida por las DCPS que sea accesible en la red o en Internet se entiende que es el punto de vista individual del autor y no el de las DCPS, el Gobierno del Distrito de Columbia, sus afiliados o empleados.

2. Filtros y monitoreo

Según lo exige la Ley de Protección de los Niños en Internet (CIPA, por sus siglas en inglés), las DCPS deben proteger a los estudiantes y educarlos sobre las amenazas en línea, bloquear el acceso a contenido inapropiado y monitorear el uso de Internet por parte de los menores en las redes escolares.[4]

Las DCPS utilizan la protección tecnológica para bloquear o filtrar el acceso a Internet a representaciones visuales obscenas, pornográficas o dañinas para los menores. A excepción de lo

[4] 47 U.S.C. 254(h)(5)(B).

descrito en la Sección IV.G a continuación, las DCPS se reservan el derecho de supervisar y monitorear las actividades en línea de los estudiantes y de acceder, revisar, copiar, almacenar o eliminar cualquier información o archivo electrónico, así como divulgarlos a otros según lo considere necesario. Los estudiantes no tienen ninguna expectativa de privacidad con respecto al uso de la propiedad de las DCPS, la red informática de las DCPS o Internet, archivos o correo electrónico mientras están dentro de la red, excepto según lo establecido por la Ley de Protección de la Privacidad Digital de los Estudiantes (consulte la Sección IV.G a continuación).

Las DCPS también utilizan un sistema de gestión de seguridad para analizar y revisar el contenido que se encuentra en el almacenamiento de archivos de los estudiantes en línea, el correo electrónico entrante y saliente de las DCPS, los archivos adjuntos de correo electrónico de las DCPS y los enlaces a sitios web. Este sistema bloquea el contenido y las imágenes potencialmente dañinos y notifica al personal de las DCPS en circunstancias de emergencia, como amenazas o violencia contra uno mismo o contra otros.

3. Aplicaciones

La Ley de Protección de la Privacidad en Línea para Niños (COPPA, por sus siglas en inglés) requiere que los operadores de sitios web o servicios en línea dirigidos a niños menores de 13 años, y los operadores de otros sitios web o servicios en línea que tengan conocimiento real de que están recopilando información personal en línea de un niño menor de 13 años, obtengan el consentimiento verificable de los padres antes de recopilar. Usar o divulgar información personal de niños.[5]

Cuando las DCPS contratan un sitio web o un servicio en línea para recopilar información personal para el uso y beneficio de las DCPS y para ningún otro propósito comercial, el operador puede obtener el consentimiento de las DCPS y no está obligado a obtener el consentimiento directamente de los padres.[6] Las DCPS proporcionarán a los padres un aviso de consentimiento proporcionado por las DCPS a través de un inventario electrónico en el sitio web de las DCPS de todos los sitios web y servicios en línea que cumplen con COPPA con los que las DCPS tienen contratos y/o requiere que los estudiantes menores de 13 años accedan, incluido un enlace a la política de privacidad de cada operador y un proceso a través del cual los padres pueden optar por no participar. Al personal de las DCPS no se le permite exigir a los estudiantes menores de 13 años que accedan a sitios y servicios que no cumplan con COPPA o a cualquier sitio y servicio que cumpla con COPPA donde los padres hayan optado por no participar en la recopilación de información personal.

4. Control de acceso

Las DCPS implementan medidas de control de acceso de seguridad para garantizar el acceso adecuado a la red y la tecnología para todos los usuarios y bloquear el acceso no autorizado y las amenazas potenciales. Las DCPS asignan el acceso de los usuarios a la red de las DCPS, a las cuentas de correo electrónico de las DCPS y a las aplicaciones autorizadas por las DCPS según el nivel de grado y/o la solicitud de la escuela o el maestro de la siguiente manera:

[5] *Consultar* 16 C.F.R. Parte 312.5. Este requisito también se aplica a cualquier cambio sustancial en las prácticas de recopilación, uso o divulgación a las que un padre haya dado su consentimiento previamente. Los operadores también deben dar a los padres la opción de dar su consentimiento para la recopilación y el uso de la información personal del niño sin dar su consentimiento para la divulgación de su información personal a terceros.
[6] Para obtener información adicional sobre el cumplimiento de COPPA, consultar https://www.ftc.gov/tipsadvice/business-center/guidance/complying-coppa-frequently-asked-questions.

- **Acceso**: Todos los estudiantes y el personal deben usar sus nombres de usuario y contraseñas personalizadas para iniciar sesión en los sistemas y dispositivos de las DCPS.
- **Correo electrónico**: A los estudiantes de 9º grado y superiores se les proporcionan cuentas de correo electrónico de las DCPS después de realizar con éxito un curso de Ciudadanía Digital. A los estudiantes de otros grados se les pueden proporcionar cuentas de correo electrónico de las DCPS después de realizar un curso de Ciudadanía Digital a discreción del personal de las DCPS. Los estudiantes con ciertas discapacidades deben tener acceso a las pruebas y adaptaciones en el salón enumeradas en su IEP para realizar el curso de Ciudadanía Digital, que puede incluir lectura en voz alta y repetición de instrucciones, legibilidad reducida del texto, simplificación del contenido y otras adaptaciones.
- **Aplicaciones**: Las DCPS proporcionan acceso a un conjunto estándar de aplicaciones aprobadas para todo el personal y los estudiantes de las DCPS. El acceso del personal se proporciona en función de la responsabilidad del trabajo y, para ciertas aplicaciones, en función de la solicitud del director. A los estudiantes se le proporciona acceso a un conjunto de aplicaciones aprobadas. Los estudiantes pueden recibir acceso a otras aplicaciones más allá de la suite aprobada por la escuela y la solicitud del maestro.
- **Graduación o cancelación de la inscripción:** Los estudiantes que se gradúen o se den de baja de las DCPS ya no tendrán acceso a la tecnología o los sistemas de las DCPS, incluidas las aplicaciones y los materiales almacenados.

5. Contraseñas

Se requiere protección con contraseña en toda la tecnología emitida por las DCPS para evitar el uso por parte de cualquier persona no autorizada por las DCPS, y se requiere que los usuarios cumplan con los requisitos de contraseña de las DCPS cuando inicien sesión en las computadoras, redes y sistemas en línea de la escuela. A los usuarios se les pedirá automáticamente que cumplan con estos requisitos de contraseña de las DCPS como parte del proceso de actualización periódica de su contraseña.

Los estudiantes y el personal no están autorizados a compartir su contraseña o la contraseña de cualquier otro estudiante o miembro del personal de las DCPS que puedan haber aprendido, ya sea inocentemente o en violación de esta política, y deben tener especial cuidado para evitar estafas por correo electrónico que solicitan contraseñas u otra información personal. Las DCPS requieren que los estudiantes participen en lecciones de ciudadanía digital y seguridad en línea para aprender cómo evitar estas estafas y otras buenas prácticas para el uso seguro de la tecnología.

Los estudiantes con discapacidades que no puedan dominar las lecciones de ciudadanía digital están excluidos de estos requisitos de contraseña.

Las sanciones por el uso prohibido de contraseñas pueden dar lugar a restricciones al acceso a la red o a la cancelación de cuentas. Además, las violaciones pueden dar lugar a acciones disciplinarias y/o legales para los estudiantes, incluida la suspensión, la expulsión y el enjuiciamiento penal.

6. Acceso a la telesalud/telemedicina

El personal y los estudiantes de las DCPS pueden acceder a las sesiones de telesalud en los dispositivos de las DCPS. Aunque las DCPS no tiene intención de monitorear activamente las sesiones de telesalud, la ley federal requiere que los distritos escolares escaneen los datos y monitoreen la actividad de los

estudiantes en los dispositivos emitidos por la escuela, que podrían incluir registros médicos u otros documentos guardados en los discos duros de los dispositivos. Las sesiones de telesalud en vivo no serán monitoreadas. Si los datos confidenciales se almacenan en los discos duros de los dispositivos, se eliminarán cuando los dispositivos vuelvan al inventario.

7. Videoconferencia

La videoconferencia ocurre cuando el personal y los estudiantes de las DCPS se comunican entre sí en tiempo real mediante una aplicación de videoconferencia. Los maestros y el personal pueden grabar la videoconferencia y ponerla a disposición de ellos mismos y del estudiante más tarde.

El personal no debe divulgar información de identificación personal sobre los estudiantes durante las sesiones de videoconferencia.

El personal y los estudiantes deben reportar cualquier comportamiento inapropiado o preocupante que pueda ocurrir durante una videoconferencia a la Oficina de Integridad de las DCPS.[7] El personal y los estudiantes deben continuar siguiendo la Política de Derechos y Responsabilidades de los Empleados de las DCPS,[8] Política de las Redes Sociales,[9] y cualquier otra política, regulación y ley aplicable con respecto a las interacciones entre el personal y los estudiantes.

8. Inteligencia Artificial (AI, por sus siglas en inglés)

Al igual que con toda la tecnología, los estudiantes y el personal deben usar la *AI* de manera responsable y ética. Los estudiantes y el personal deben utilizar las herramientas de IA como un complemento, no como un sustituto, del aprendizaje. Las DCPS proporcionarán a los estudiantes lecciones sobre los beneficios y riesgos de la *AI* a través de cursos específicos de ciudadanía digital y *AI*.

Aunque se abordan en otras partes de esta política, los siguientes usos de la *AI* están específicamente prohibidos y serán objeto de un escrutinio adicional:

- Intimidación escolar (bullying) y acoso: Los estudiantes tienen prohibido usar la *AI* de una manera que pueda dañarse a sí mismos o a otros. Está prohibido el uso de herramientas de *AI* para manipular medios de comunicación para hacerse pasar por otros.
- Plagio y trampas: Los estudiantes tienen prohibido enviar trabajos generados por *AI* como su trabajo original o usar *AI* para responder preguntas de exámenes, exámenes u otras tareas (a menos que su maestro se lo indique).

De acuerdo con la Política de Escuelas Seguras y Positivas de las DCPS,[10] el personal debe implementar respuestas disciplinarias, comenzando con la respuesta apropiada menos severa dentro del rango de respuestas disciplinarias permisibles. Este rango podría variar desde brindar la oportunidad de volver a enviar el trabajo hasta la reducción de la calificación.

a. Consideraciones adicionales para el uso de la *AI* por parte del personal

[7] Puede comunicarse con la Oficina de Integridad llenando el formulario de referencia en línea, disponible en https://dcps.dc.gov/page/office-integrity o enviando un correo electrónico a dcps.cio@k12.dc.gov.
[8] *Disponible en* https://dcps.dc.gov/page/dcps-policies.
[9] *Disponible en* https://dcps.dc.gov/page/dcps-policies.
[10] *Disponible en* https://dcps.dc.gov/publication/safe-and-positive-schools-policy.

Las DCPS mantienen una lista de herramientas aprobadas mejoradas por *AI* para el aprendizaje de los estudiantes y proporcionará desarrollo profesional para apoyar la implementación adecuada de estas herramientas. Si los maestros y líderes escolares desean usar una herramienta de *AI* fuera de la lista seleccionada por el equipo de EdTech de las DCPS, debe cumplir con los criterios establecidos por el Equipo de EdTech y deben enviar el Formulario de aprobación de herramientas de *AI* antes de comprarla y usarla en una clase o en una tarea. Estos criterios y el formulario están disponibles en el sitio web de EdTech SharePoint en https://dck12.sharepoint.com/sites/DCPSEdTechInformationResources.

El personal está obligado a verificar la veracidad de cualquier contenido producido por la *AI* utilizando fuentes fiables, ya que el contenido generado por la *AI* puede contener errores o sesgos. Cuando se utiliza la *AI* para las comunicaciones, como la redacción de correos electrónicos a los padres, el personal es responsable de garantizar que el lenguaje sea profesional y esté libre de imprecisiones y prejuicios. El personal debe revisar y reflexionar críticamente sobre todo el contenido generado por *AI* antes de usarlo.

C. Tecnología (incluyendo computadoras, computadoras portátiles (laptops), tabletas)

1. Ayuda con los dispositivos

Las DCPS proporcionan instalación básica, sincronización y apoyo de software para la tecnología de las DCPS. Los dispositivos deben estar conectados a la red de las DCPS de forma regular para recibir actualizaciones de software y/o para fines de inventario. Se requiere protección con contraseña en toda la tecnología emitida por las DCPS para evitar el uso no autorizado en caso de pérdida o robo.

2. Daños, pérdidas o robos

El personal es administrador de la tecnología de las DCPS y puede ser considerado financieramente responsable por daños, pérdida o robo de propiedad debido a negligencia. Los ejemplos de negligencia incluyen, pero no se limitan a:

- Daños como resultado de dejar la tecnología de las DCPS en un vehículo u otro lugar que esté expuesto al calor, el frío o la humedad;
- Daños debidos a bebidas o alimentos derramados; o
- Robo como resultado de dejar el dispositivo de las DCPS desatendida o en un lugar inseguro.

Un miembro del personal de las DCPS solo debe usar el dispositivo que le asignó el equipo de tecnología informática de las DCPS y tiene prohibido tomar o usar dispositivos asignados a otros empleados actuales o anteriores.

Los estudiantes deben tomar medidas razonables para evitar que un dispositivo se dañe, se pierda o sea robado. Si el dispositivo de un estudiante está dañado, el personal de las DCPS en la escuela del estudiante puede investigar para determinar si el daño a los dispositivos fue el resultado de negligencia o actos intencionales de vandalismo. Esta investigación debe tener en cuenta los factores que afectan si el estudiante puede entender el cuidado adecuado del dispositivo, incluida la edad y cualquier discapacidad relevante. Los ejemplos de daños resultantes de *negligencia o actos intencionales de vandalismo* incluyen, entre otros,:

- Dibujar en dispositivos con un rotulador permanente, grabar palabras/gráficos con un objeto

afilado, o marcas de mordeduras de animales en el dispositivo;
- Daños en varios lugares debido a que los dispositivos se manipulan mal o no se cuidan (por ejemplo, la pantalla está rota, el teclado está dañado, faltan teclas o la carcasa exterior de la computadora portátil muestra signos de impacto en varias ubicaciones o la computadora portátil / tableta se devuelve en varias piezas);
- Daños contundentes, daños causados por impacto con objetos afilados o duros, o daños por objetos atascados en los puertos USB o de alimentación de la computadora portátil;
- El dispositivo estaba completamente sumergido en agua u otros líquidos; o
- Patrón repetido de daño si el estudiante ha causado daños a tres (3) o más dispositivos en un año escolar.

Las respuestas disciplinarias para los estudiantes por daños a dispositivos que resultaron de negligencia o actos intencionales de vandalismo se determinarán bajo la Política de Escuelas Seguras y Positivas de las DCPS[11] reglamentos disciplinarios y la ley, y esta Política de Uso Aceptable.

Los estudiantes no pueden ser penalizados por daños resultantes del desgaste normal o accidentes no intencionales. Los ejemplos de daños en el dispositivo que resultan del *desgaste normal* incluyen, entre otros,:
- Tecla(s) faltante(s) en el teclado;
- Pantalla agrietada debido a caídas accidentales;
- Daños aislados en una pequeña parte del dispositivo, como esquinas/lados de la pantalla, que podrían ser el resultado de caídas accidentales;
- Derrames accidentales de líquido en el teclado; o
- Daños causados por una subida de tensión.

Si la tecnología de las DCPS se pierde, es robada o dañada, los estudiantes deben notificar a un maestro o líder escolar; el personal debe notificar a su supervisor y a un punto de contacto de *DCPS Technology* o Tecnología de las DCPS. Las DCPS tomarán todas las medidas razonables para recuperar la propiedad perdida y garantizar la seguridad de cualquier información contenida en el dispositivo. Las DCPS pueden decidir en implementar software de rastreo de ubicación en los dispositivos para localizar los dispositivos identificados como perdidos o robados o desactivar de forma remota los dispositivos que no se devuelven a pedido. Los dispositivos dañados deben devolverse al equipo de Informática de las DCPS (AssetAdmin@k12.dc.gov) y no debe ser desechado por los estudiantes, las familias o el personal. El dispositivo debe ser evaluado primero por el equipo de Informática de las DCPS y OCTO antes de su reemplazo.

3. Uso nocturno o en casa por parte de los estudiantes

El personal escolar de las DCPS pueden proporcionar a los estudiantes dispositivos de las DCPS para uso nocturno o en el hogar a discreción del director de la escuela o del equipo del IEP, cuando corresponda y de acuerdo con esta política. Los estudiantes de las DCPS y un padre/tutor deben firmar el Acuerdo de Uso Aceptable del Estudiante adjunto (consulte los Apéndices) antes de que se les asigne y se les entregue un dispositivo para uso nocturno o en el hogar. El personal escolar de las DCPS deben cumplir con los requisitos de privacidad bajo la Ley de Protección de la Privacidad Digital de los Estudiantes, y los padres y estudiantes deben tener en cuenta que estos dispositivos pueden ser monitoreados y

[11] *Disponible en* https://dcps.dc.gov/page/dcps-policies.

accedidos por el personal de las DCPS.[12]

La tecnología de asistencia puede irse a casa con el estudiante si el equipo del IEP del estudiante, en colaboración con el Equipo de Tecnología de Asistencia de las DCPS, determina que el estudiante requiere estos apoyos para realizar los deberes educativos en casa(por ejemplo, hacer la tarea, usarlo como medios de comunicación). Los estudiantes deben seguir todas las políticas de las DCPS en el uso de esta tecnología en casa, tal como lo harían si usaran la tecnología en la escuela. Para obtener información adicional sobre la tecnología de asistencia, consulte el sitio web de Tecnología de asistencia de las DCPS[13] o envíe un correo electrónico a DCPS.AssistiveTech@k12.dc.gov o el equipo del IEP del estudiante.

D. Conducta y uso aceptable

Al utilizar la red de las DCPS y la tecnología de las DCPS, el personal y los estudiantes acuerdan seguir todas las normas pertinentes del Gobierno del Distrito de Columbia; OCTO; y los reglamentos, políticas y pautas de las DCPS. El personal y los estudiantes deben informar sobre el uso indebido o el incumplimiento de los protocolos a los maestros, supervisores apropiados, administradores o empleados de Servicios Centrales tan pronto como tengan conocimiento del uso indebido o incumplimiento.[14]

El personal y los estudiantes no deben usar la red de las DCPS o la tecnología de las DCPS, incluido el acceso a Internet, intranet, herramientas de colaboración, herramientas de comunicación masiva, redes sociales o correo electrónico para usar, grabar, compartir, cargar, publicar, enviar por correo, mostrar, almacenar o transmitir de cualquier otra manera cualquier contenido, comunicación o información que:

1. Sea odioso, acosador, amenazante, calumnioso o difamatorio;
2. Sea ofensivo o discriminatorio para las personas por motivos de raza, color, religión, origen nacional, sexo, edad, estado civil, apariencia personal, orientación sexual, identidad o expresión de género, estado familiar, responsabilidades familiares, matriculación, afiliación política, información genética, discapacidad, fuente de ingresos, estado como víctima de un delito intrafamiliar, lugar de residencia o negocio, o estado como víctima o miembro de la familia de una víctima de violencia doméstica, un delito sexual o acecho;
3. Constituya o promueva cualquier delito penal o dé lugar a responsabilidad civil en virtud de cualquier ley aplicable, incluidas las leyes de control de exportaciones de los Estados Unidos o las leyes de patentes, marcas comerciales o derechos de autor de los Estados Unidos;
4. Constituya el uso o en apoyo de cualquier propósito obsceno o pornográfico, incluidos, entre otros, la transmisión, recuperación o visualización de cualquier material profano, obsceno o sexualmente explícito;
5. Constituya un uso para solicitar o distribuir información con la intención de incitar a la violencia, causar daños personales o lesiones corporales, o acosar, amenazar o acechar a otra persona;
6. Contenga un virus, troyano, Ransomware u otro componente dañino o código malicioso;
7. Constituya correo basura, phishing, spam o correo electrónico de difusión no autorizado;
8. Viole la seguridad de cualquier otro dispositivo o red de las DCPS, o constituya un acceso no autorizado a cualquier dispositivo o red de las DCPS o intente eludir cualquier medida de

[12] *Consultar* Código Oficial del Distrito de Columbia § 38-831.03(a).
[13] *Available at* https://dcps.dc.gov/page/assistive-technology%E2%80%AF.
[14] For additional information on filing reports and complaints, please see Section V.

seguridad;

9. Obtiene acceso o proporciona a un tercero no autorizado acceso a la cuenta, archivos o datos de la red DCPS de otro usuario, o modifica sus archivos, datos o contraseñas;
10. Se hace pasar por cualquier persona, organización, empresa u otra entidad autorizada viva o muerta con la intención de engañar;
11. Degrade el rendimiento, provoque un riesgo de seguridad o amenace de otro modo la integridad o el funcionamiento eficiente de la red o tecnología de las DCPS;
12. Priva a un usuario autorizado del acceso a la red o tecnología de las DCPS;
13. Obtiene tecnología de las DCPS o acceso a la red del Distrito de Columbia más allá de los autorizados;
14. Participe en la entrada no autorizada o ilegal en un sistema de red de las DCPS;
15. Divulgue información confidencial o de propiedad, incluida la información de los registros de los estudiantes, sin autorización o sin las medidas de seguridad adecuadas;
16. Divulgue o transmita información, videos y fotografías de identificación personal del estudiante sin autorización o sin las medidas de seguridad adecuadas;
17. Comparte información confidencial sobre estudiantes o personal de las DCPS de una manera que viole la ley del Distrito de Columbia, la ley federal, los reglamentos, la política o las directrices;
18. Comparte direcciones de correo electrónico o listas de distribución de las DCPS para usos que violan esta política o cualquier otra política de las DCPS;
19. Permita o constituya apuestas o juegos de azar de cualquier tipo;
20. Instale, descargue o utilice software o sistema de terceros no autorizado o sin licencia;
21. Acceda, distribuya, descargue o utilice juegos, programas, archivos, medios electrónicos o aplicaciones independientes no autorizadas de Internet que puedan causar una amenaza a la red de las DCPS;
22. Promueva o participe de cualquier manera en rifas o eventos de recaudación de fondos no autorizados;
23. Promueva o participe de cualquier manera en actividades políticas partidistas;
24. Promueva o participe de cualquier manera en actividades políticas o electorales internas relacionadas con un sindicato u otra organización que represente a los empleados;
25. Se dedica a negocios privados, comerciales u otras actividades para obtener ganancias financieras personales;
26. Distribuya información no autorizada sobre las contraseñas o los sistemas de seguridad de otros usuarios;
27. Falsifique, manipule o realice cambios, adiciones o eliminaciones no autorizadas a los datos ubicados en la red de las DCPS o en cualquier sistema escolar;
28. Accede o utiliza datos ubicados en una red de las DCPS para usos personales;
29. Promueva o participe en cualquier actividad o relación con un estudiante que no esté relacionada con actividades académicas o extracurriculares patrocinadas por la escuela, a menos que el director y el padre/tutor del estudiante lo autoricen por adelantado por escrito;
30. Viole los términos de uso especificados para una tecnología, aplicación o sistema de red de las DCPS en particular;
31. Constituya un uso que interrumpa el funcionamiento adecuado y ordenado de una escuela u oficina;
32. Participa en la piratería informática (es decir, obtener acceso intencionalmente por medios ilegales o sin autorización) a la red de las DCPS para acceder a información no autorizada o para eludir los sistemas de seguridad de la información;

33. Se involucra en conductas sexuales inapropiadas, incluido el contacto sexual no deseado, la exposición indecente, la transmisión de imágenes sexualmente sugerentes u otras actividades sexuales; o
34. Viole cualquier prohibición señalada en esta política o en cualquier otra política de las DCPS.

Los estudiantes, el personal y otros usuarios no deben compartir su dispositivo emitido por las DCPS o su información de inicio de sesión de red emitida por las DCPS con ninguna otra persona. Está estrictamente prohibido usar el dispositivo emitido por las DCPS de otra persona o la información de inicio de sesión de red emitida por las DCPS, permitir que usuarios no autorizados usen el dispositivo emitido por las DCPS o la información de inicio de sesión de red emitida por las DCPS, o facilitar el uso no autorizado del dispositivo emitido por las DCPS de otra persona o la información de inicio de sesión de red emitida por las DCPS mediante el intercambio de información de inicio de sesión o cualquier otro medio.

E. Tecnología de medios personales

No se permite el uso de tecnología personal por parte de los estudiantes en la red de las DCPS sin la autorización expresa por escrito del Canciller o de la persona que éste designe. Las DCPS no son responsables del mantenimiento y la seguridad de los dispositivos electrónicos personales de los estudiantes y no asume ninguna responsabilidad por pérdida o robo. Las DCPS, OCTO y su personal no están obligados a proporcionar apoyo técnico a los estudiantes que buscan usar dispositivos electrónicos personales en la escuela o en la red de las DCPS, o a acceder a cuentas de medios personales en dispositivos de las DCPS que no sean compatibles con aplicaciones basadas en la web aprobadas por las DCPS en uso en esos dispositivos personales. A excepción de lo que se describe a continuación en esta sección, las DCPS se reservan el derecho de aplicar medidas de seguridad en los dispositivos personales cuando se utilicen para acceder a la red de las DCPS y eliminar los dispositivos que infrinjan la política de las DCPS.

F. Privacidad de las cuentas de medios personales y la tecnología de los estudiantes

1. Políticas tecnológicas y de cuentas de medios personales de estudiantes específicas de la escuela

Los directores deben notificar a los estudiantes y a los padres por escrito si su escuela tiene reglas adicionales relacionadas con las cuentas de medios personales de los estudiantes y los dispositivos tecnológicos.

2. Privacidad general de las cuentas de medios personales y los dispositivos tecnológicos de los estudiantes

Aparte de las excepciones en la Sección IV.G.3, las DCPS no tomarán ni amenazarán con tomar medidas contra un estudiante o posible estudiante, incluyendo medidas disciplinarias, expulsión, cancelación de inscripción, negativa a admitir o participación prohibida en una actividad curricular o extracurricular, porque el estudiante o posible estudiante se negó a:

- Divulgar un nombre de usuario, contraseña u otro medio de autenticación de cuenta utilizado para acceder a la cuenta de medios personal o dispositivo tecnológico personal del estudiante;
- Acceder a la cuenta de medios personales o al dispositivo tecnológico personal del estudiante

en presencia del personal de la escuela de una manera que permita al personal de la escuela observar los datos de la cuenta o el dispositivo;
- Agregar una persona a la lista de usuarios que pueden ver la cuenta de medios personal del estudiante o acceder al dispositivo tecnológico personal de un estudiante; o
- Cambiar la configuración de privacidad asociada con la cuenta de medios personales o el dispositivo tecnológico personal del estudiante.[15]

Si las DCPS reciben inadvertidamente el nombre de usuario, contraseña u otro medio de autenticación de la cuenta para la cuenta de medios personales o el dispositivo tecnológico personal de un estudiante o posible estudiante a través de medios legales, las DCPS:
- No utilizar la información para acceder a la cuenta de medios personales o dispositivo tecnológico personal del estudiante o futuro estudiante;
- No compartir la información con nadie; y
- Eliminar la información inmediatamente o tan pronto como sea razonablemente posible.[16]

Nada en esta sección impide que las DCPS:
- Acceder a información sobre un estudiante o posible estudiante que esté disponible públicamente;
- Solicitar a un estudiante o posible estudiante que comparta voluntariamente contenido específico accesible desde una cuenta de medios personal o un dispositivo tecnológico personal con el fin de garantizar el cumplimiento de las leyes aplicables o las políticas de las DCPS, siempre que la solicitud cumpla con los requisitos de esta política;
- Prohibir que un estudiante o posible estudiante acceda u opere una cuenta de medios personales o un dispositivo tecnológico personal durante el horario escolar o mientras se encuentre en la propiedad escolar;
- Monitorear el uso de la red de las DCPS; o
- Revocar el acceso de un estudiante, en su totalidad o en parte, a la red de las DCPS o a la tecnología de las DCPS.[17]

3. Excepciones a la privacidad de las cuentas de medios personales y la tecnología de los estudiantes

El personal de las DCPS pueden buscar en la cuenta de medios personales o en el dispositivo tecnológico personal de un estudiante, u obligar a un estudiante a producir datos accesibles desde la cuenta de medios personales o el dispositivo tecnológico personal del estudiante en los siguientes casos de violaciones de la política o amenaza inminente a la vida o la seguridad.

a. Violaciones de políticas

El personal de las DCPS puede buscar en la cuenta de medios personales o en el dispositivo tecnológico personal de un estudiante, u obligar a un estudiante a presentar datos accesibles desde la cuenta de medios personales, o el dispositivo tecnológico personal del estudiante si el personal de las DCPS tiene una sospecha razonable de que el estudiante ha usado o está usando la cuenta de medios personales o

[15] Código Oficial del Distrito de Columbia § 38-831.04(a).
[16] Código Oficial del Distrito de Columbia § 38-831.04(b).
[17] Código Oficial del Distrito de Columbia § 38-831.04(e).

el dispositivo tecnológico personal del estudiante en apoyo de una violación de la política de las DCPS, y tiene una sospecha razonable de que la cuenta de medios personales o el dispositivo tecnológico personal contiene evidencia de la presunta violación.[18]

Antes de llevar a cabo dicha búsqueda u obligar al estudiante a presentar dichos datos, el personal de las DCPS debe:

- Documentar la sospecha razonable que da lugar a la necesidad del registro o la presentación; y
- Notificar al estudiante y al padre/tutor del estudiante de la presunta violación y los datos o componentes que se buscarán o que el estudiante se verá obligado a presentar.[19]

Las DCPS pueden confiscar el dispositivo tecnológico personal de un estudiante para evitar la eliminación de datos en espera de esta notificación requerida solo si el período de incautación previo a la notificación no es mayor de 48 horas y el dispositivo tecnológico personal se almacena de forma segura en la propiedad de las DCPS y no se accede a él durante el período de incautación previo a la notificación.[20]

El registro o la producción forzada deben limitarse a los datos accesibles desde la cuenta o el dispositivo o los componentes del dispositivo que razonablemente puedan arrojar evidencia de la presunta infracción, y no se puede permitir que ninguna persona copie, comparta o transfiera datos obtenidos en virtud de un registro o producción forzada que no esté relacionada con la presunta violación que provocó el registro.[21]

b. Amenaza inminente a la vida o la seguridad

El personal de las DCPS pueden registrar la cuenta de medios personales o el dispositivo tecnológico personal de un estudiante u obligar a un estudiante a producir datos accesibles desde la cuenta de medios personales o el dispositivo tecnológico personal del estudiante si es necesario hacerlo en respuesta a una amenaza inminente a la vida o la seguridad.[22]

El alcance de cualquier registro o producción forzada debe limitarse a este propósito y las DCPS deben, dentro de las 72 horas posteriores al registro o producción forzada, proporcionar al estudiante y a los padres del estudiante una descripción por escrito de la amenaza precisa que provocó el registro y los datos a los que se accedió.[23]

V. REQUISITOS DE IMPLEMENTACIÓN DE POLÍTICAS

Todos los estudiantes y el personal de las DCPS deben cumplir con los requisitos establecidos en esta política. Para apoyar su implementación, se espera que los directores informen anualmente al personal sobre las actividades requeridas y los plazos. La aplicación de esta política se reforzará mediante un proceso central de supervisión que incluye exámenes periódicos de los datos, muestreo de registros y

[18] Código Oficial del Distrito de Columbia § 38-831.04(c)(1)(A).
[19] Código Oficial del Distrito de Columbia § 38-831.04(c)(1)(B).
[20] Código Oficial del Distrito de Columbia § 38-831.04(d).
[21] Código Oficial del Distrito de Columbia § 38-831.04(c)(1)(C)-(D).
[22] Código Oficial del Distrito de Columbia § 38-831.04(c)(2)(A).
[23] Código Oficial del Distrito de Columbia § 38-831.04(c)(2)(B)-(C).

exámenes de la documentación subyacente y visitas al sitio (según sea necesario). Este marco garantizará que juntos construyamos un sistema de mejora continua y evitemos el incumplimiento. Para obtener orientación y apoyo clave con preguntas, capacitación o implementación, consulte dcps.dc.gov.

Las DCPS se comprometen a servir a cada estudiante con equidad, excelencia, transparencia y responsabilidad. Para cualquier inquietud o para denunciar posibles violaciones de esta directiva, comuníquese con el Director de Integridad llenando el Formulario de referencia en línea[24] o enviando un correo electrónico a dcps.cio@k12.dc.gov.

[24] *Disponible en* https://dcps.dc.gov/page/office-integrity.

APÉNDICES

Los siguientes documentos se incluyen como apéndices:

- Acuerdo de Uso Responsable de Tecnología para Estudiantes;
- Formulario de Reconocimiento del Acuerdo de Uso Responsable de Tecnología del Estudiante; y
- Formulario de Reconocimiento del Acuerdo de uso Responsable de Tecnología del Personal.

Acuerdo de Uso Responsable de Tecnología para Estudiantes

Como usuario responsable de la tecnología:

A. Trataré mi dispositivo de las DCPS con respeto, teniendo cuidado de no dejarlo caer ni dañarlo.
- ❑ Seguiré las reglas de la escuela sobre el préstamo y la devolución de mi dispositivo de las DCPS.
- ❑ Informaré inmediatamente a un maestro o miembro del personal si mi dispositivo de las DCPS está dañado o no funciona correctamente.
- ❑ Mantendré mi dispositivo en el interior en un lugar seguro siempre que no lo esté usando.

B. Protegeré mi información personal.
- ❑ No compartiré mi dispositivo, nombre de usuario o contraseña de las DCPS con nadie (a menos que sea un estudiante de la primera infancia o un estudiante que necesite apoyo para usar mi cuenta).
- ❑ Guardaré mi trabajo en mi *DCPS Office365 OneDrive* y cerraré sesión en mis cuentas y programas cuando termine de trabajar.
- ❑ Informaré a un maestro inmediatamente si creo o sé que alguien ha utilizado mi cuenta.

C. Usaré mi dispositivo solo para trabajos escolares.
- ❑ Solo descargaré, instalaré o usaré software, aplicaciones, extensiones de navegador o archivos multimedia, si mi maestro me da permiso para hacerlo.
- ❑ Evitaré recursos que sean inapropiados, ofensivos o ilegales. Si veo material inapropiado en línea, lo reportaré inmediatamente a un maestro o miembro del personal.

D. Usaré mis habilidades ciudadanía digital y trataré a las personas con amabilidad.
- ❑ Usaré un lenguaje respetuoso y apropiado.
- ❑ Referenciaré adecuadamente el trabajo de otros y no plagiaré.
- ❑ Verificaré la información antes de compartirla en línea.
- ❑ Usaré la inteligencia artificial (*AI*) de una manera responsable y étnica que respete la privacidad de todos, no intimide ni acose a otros, y no plagie ni haga trampa en las tareas escolares.

Resultados del uso irresponsable de la tecnología

Perderá el acceso a la red de las DCPS o a la tecnología de las DCPS durante períodos de tiempo cada vez mayores según los reglamentos y políticas de disciplina estudiantil de las DCPS. Bajo ciertas circunstancias, se puede permitir que el personal de las DCPS busque y acceda a todos los archivos ubicados en la red de las DCPS o guardados en dispositivos de las DCPS en cualquier momento. Bajo ciertas circunstancias, el personal de las DCPS puede estar autorizado a buscar en su cuenta o dispositivo de medios personales o a exigirle que presente datos de mi cuenta o dispositivo de medios personales.

Protocolo para dispositivos robados o dañados accidentalmente

Si su dispositivo fue robado o dañado, debe notificar inmediatamente a un maestro o miembro del personal lo antes posible porque las DCPS debe presentar un informe policial dentro de los cinco días calendario posteriores a un presunto robo para que se rastree el dispositivo. Usted no será responsable de los costos asociados con el dispositivo robado o dañado accidentalmente. Su asociación con las DCPS es muy apreciada en esta situación.

Ejemplos de uso inaceptable de la tecnología:

- Comer o beber cerca de un dispositivo de las DCPS;
- Escribir, dibujar o pegar calcomanías en un dispositivo de las DCPS;
- Descargar, instalar o ejecutar cualquier tipo de archivo, incluidos archivos de música y video, sitios web, software, aplicaciones, extensiones de navegador o medios, a menos que un maestro otorgue permiso;
- Usar aplicaciones o complementos para intentar cambiar la configuración de seguridad o los filtros de contenido de Internet;
- Insertar unidades USB (por ejemplo, unidades flash) en un dispositivo a menos que un maestro lo apruebe;
- Buscar, guardar, hacer circular o exhibir recursos que estén basados en el odio, lascivos, vulgares, etc.;
- Usar la red de las DCPS para participar en actos ilegales o delictivos;
- Acceder a juegos en línea, redes sociales, aplicaciones de mensajería o chats grupales, a menos que estas actividades estén relacionadas con el trabajo escolar y un maestro o miembro del personal esté supervisando la actividad;
- Intimidar, acosar, amenazar o intimidar a otras personas;
- Usar el nombre de usuario o contraseña de otra persona; y
- Crear o publicar imágenes, grabaciones de audio o video de otras personas sin su permiso..

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

Formulario de Reconocimiento del Acuerdo de Uso Responsable de Tecnología del Estudiante

Estudiantes: He leído la Política de Uso Aceptable de la Tecnología y la Red para Estudiantes y Personal de las DCPS y el Acuerdo de Uso Responsable de la Tecnología para Estudiantes, o alguien me lo ha leído y me lo ha explicado.

Padres/Tutores: He leído y discutido con mi estudiante la Política de Uso Aceptable de la Tecnología y la Red para Estudiantes y Personal de las DCPS y el Acuerdo de Uso Responsable de la Tecnología para Estudiantes.

1. Acepto usar todos los dispositivos de las DCPS y la red de las DCPS de manera responsable bajo las reglas enumeradas en el Acuerdo y la Política de Uso Aceptable. Entiendo que si no sigo estas reglas, puedo recibir consecuencias bajo las reglas y políticas disciplinarias de las DCPS y mi capacidad para usar los dispositivos de las DCPS y la red de las DCPS puede ser restringida.

2. Entiendo que si veo o me doy cuenta de que alguien está usando un dispositivo de las DCPS o la red de las DCPS para intimidar, amenazar, acosar o lastimar a otra persona, informaré esto a un maestro o miembro del personal. Entiendo que mi informe se mantendrá confidencial y que las DCPS no tolerarán ninguna represalia en mi contra por hacer un informe.

3. Si se me entrega un dispositivo, entiendo que se me presta solo y de acuerdo con la Política de Uso Aceptable de la Tecnología y la Red para Estudiantes y Personal de las DCPS. Las DCPS recopilan datos y monitorea el uso de la computadora portátil de conformidad con la Ley de Protección de la Privacidad Digital de los Estudiantes de 2016.

4. Si pierdo o daño intencionalmente o por negligencia un dispositivo de las DCPS, puedo enfrentar una acción disciplinaria apropiada de las DCPS. Se me pedirá que me reúna con las DCPS para determinar el motivo de la pérdida o daño y aprender prácticas responsables de cuidado del dispositivo.

5. Si se me entrega un dispositivo, entiendo que debe devolverlo al Punto de Contacto Tecnológico de mi escuela o al equipo de informática de las DCPS (AssetAdmin@k12.dc.gov) previa solicitud. Si no devuelvo el dispositivo según lo solicitado, es posible que el dispositivo se desactive de forma remota y se le cobre una tarifa a mi familia.

6. Entiendo que ya no tendré acceso a la tecnología o red de las DCPS una vez que me gradúe o cancele mi inscripción en las DCPS.

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

Formulario de Reconocimiento del Acuerdo de Uso Responsable de Tecnología del Personal

He leído la Política de Uso Aceptable de la Tecnología y la Red para Estudiantes y Personal de las DCPS.

1. Acepto usar la red de las DCPS y cualquier dispositivo de las DCPS que se me entregue de manera responsable bajo las reglas enumeradas en la Política de uso aceptable. Entiendo que si no sigo estas reglas, puedo recibir consecuencias bajo las reglas y políticas disciplinarias de las DCPS y las leyes y reglamentos del Distrito de Columbia.

2. Si las DCPS me entregan una computadora portátil (laptop), reconozco que la computadora portátil es propiedad de las DCPS. La computadora portátil me es prestada para ser utilizada únicamente con fines laborales y de acuerdo con la Política de Uso Aceptable de la Tecnología y Red para Estudiantes y Personal de las DCPS.

3. Si las DCPS me entregan una computadora portátil, soy responsable de cualquier costo asociado con la reparación de daños causados por mi negligencia o acciones intencionales mientras la computadora portátil está en mi posesión como dispositivo prestado.

4. Si las DCPS me entregan una computadora portátil, la computadora portátil debe devolverse al equipo de informática de las DCPS (AssetAdmin@k12.dc.gov) si me retiro de la organización o si se me pide que la devuelva. Si no devuelvo este dispositivo cuando las DCPS lo soliciten, es posible que se me cobre una tarifa.