Dunkirk City School District

Take home guide for 1:1 Chromebook program

This guide is to help the parents, students and teachers know and understand the policies of the district for all students who are part of the 1:1 Chromebook program. If anyone has any questions or concerns they can contact the Technology Department using the contact information below.

Jeremy Dobek **Technology Coordinator** **support@Dunkirkcsd.org** **716-366-9300 ext: *2025**	**Tara Jakse** **Technology Secretary** **support@Dunkirkcsd.org** **716-366-9300 ext: *2021**

Distribution

Students in grades 3-12 will be part of the District 1:1 Chromebook program.

Chromebooks will be distributed during the parent/student orientation and will be collected at the end of school year.

A Signature sheet (at the end of this booklet) must be signed before chromebooks will be distributed.

Requirements for being assigned a Chromebook:

1. The agreement sheet signed by parents and students.

Equipment distribution list: (it is the student's personal responsibility to take care of the device loaned to them and to turn in everything at the end of the school year)

1. Chromebook
2. Power adapter (charger)
3. Carrying case (grades 3-5) or backpack (grades 6-12)

Daily Expectation

Parents are expected to report any issues or missing chromebooks immediately to the Technology Department. You may report any issues through phone or emails listed at the beginning and the end of this document.

Care / Damage

Students are responsible for the equipment assigned to them. This includes the Chromebook and the charger. Proper care of assigned chromebooks is necessary for the longevity of the device. Students should follow these necessary steps while the devices are in their possession.

Do not walk with an open Chromebook.
Do not set on the floor where it can be stepped on or kicked.
Do not use or have chromebooks out around liquids (including drinks).
Never force close or open a screen and only open the screen by the side bezel, never by the screen itself.
Always place the Chromebook on a solid surface like a desk or table.
Never let anyone borrow their assigned device.

The Technology Department must be notified immediately when there is an issue with their device. Any device that has an issue that is not reported immediately to the Technology Department will be classified as mistreatment/neglect.

The Technology Department will inspect all devices that are turned in for repairs and will make the determination as to whether the cause of the issue is due to mechanical malfunction/defect or from neglect/abuse. Cost of repairs are for the cost of parts only and not for labor.

Devices with issues due to defect:

If a device has an issue due to defect and must be turned in for repairs, the parent will need to contact the technology department to see if there is a replacement available. ***A replacement may not be immediately available***.

Examples of issues due to mechanical malfunction/defect or from normal wear:

Backlight went out and very dark picture on screen.
Lines through screen when powered on.
Will not charge anymore.

Devices with issues due to mistreatment/neglect:

If a device has an issue due to mistreatment/neglect and must be turned in for repairs, the parent will need to contact the technology department to see if there is a replacement available. ***A replacement may not be immediately available***. Depending on the damage of the device charges may be incurred.

Examples of Issues due to mistreatment/neglect:

Cracked/broken screen
Water damage
Lost charger

Lost and stolen devices:

If a device is lost then the parent will need to contact the technology department to see if there is a replacement available. ***A replacement may not be immediately available***. If lost there will be a charge of $300 that can be paid at the administration/business office. Any costs will be communicated and collected through the business office. If a device is stolen a police report ***MUST*** be made. If no police report is made then the device will be considered lost and procedures for a lost device will apply.

Filtering / Blocking / Monitoring

DCSD uses a number of filtering methods both while on school grounds and while off school grounds. Filters are set at a minimum and block the categories of pornography, hate, shopping, social media and piracy, to name a few. While filters catch a great deal, none is foolproof and such content may get through. As an added layer of security, all websites the student goes to while on DCSD owned devices are recorded and kept for review and periodically audited. *This logging is done regardless of where the device is used*.

Students and parents/guardians must keep in mind that just because a website is not blocked does not mean it is appropriate to be viewed on a school owned device. Gaming sites, social media sites and any sites that may go against the school general decency code are strictly prohibited. Disciplinary action will be taken for any student who knowingly and continually visits these sites. Remember ALL web activity on school owned devices are recorded and subject to monitoring and review.

Any student may be transferred to a higher level of filtering due to any of the reasons listed below. Only the school principals, school administrators or the parents may authorize a higher restriction on a student. If there is a need for a higher restriction on a student, that restriction will be communicated to the parents, as well as, all of that student's teachers.

Cause for higher level of restriction:

1. At the request of a parent. (A parent may request a restriction level once in a school year).
2. Not keeping on task during school hours.
3. Bullying.
4. Falling grades (when it has been determined that home or school usage of device may be affecting grade levels).
5. Accessing non age-appropriate sites.
6. When part of an IEP plan.
7. General device mistreatment.
8. Borrowing from the technology department and not returning (example, chargers)

This higher level of filtering blocks students from all web activity except for what is on a very specific whitelist. Any faculty member may submit a website to be added to this whitelist. Faculty members submit whitelist requests via e-mail. This same whitelist applies to all students on this higher restriction. A copy of the current whitelist can be obtained upon request.

During the hours of 7:30 am and 3:00 pm, faculty have the ability to pull up, in real time, what is on a student's Chromebook screen. They also have the ability to lock the student's computer screen, take a screenshot of what is on the student's computer screen and close and open website tabs as needed. What the faculty DOES NOT have access to is the webcam on the student's computers. DCSD as a whole does not maintain the ability nor does it approve of the ability to access student devices attached webcam or microphone.

E-MAIL

All students have access to the districts email system. However, this is primarily used to email teachers and receive educational resources. No outside emails can be sent or received.

Questions / Concerns

If there are any questions, comments or concerns at any time please contact the Technology Department

Jeremy Dobek **Technology Coordinator** **support@Dunkirkcsd.org** **716-366-9300 ext: *2025**	**Tara Jakse** **Technology Secretary** **support@Dunkirkcsd.org** **716-366-9300 ext: *2021**

SUBJECT: STUDENT ACCEPTABLE USE POLICY (AUP)

The Board will provide access to various computerized information resources through the District's computer system ("DCS") consisting of software, hardware, computer networks, and electronic communications systems. This may include access to email, on-line services, and the Internet. It may include the opportunity for some students to have independent access to the DCS from their home or other

remote locations. All use of the DCS, including independent use off school premises, will be subject to this policy. Further, all DCS use must be in support of education or research and consistent with the goals and purposes of the District.

Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

This policy is intended to establish general guidelines for the acceptable student use of the DCS and also to give students and parents or guardians notice that student use of the DCS will provide student access to external computer networks not controlled by the District. The District cannot screen or review all of the available content or materials on these external computer networks, thus, some of the available content or materials on these external networks may be deemed unsuitable for student use or access by parents or guardians.

It is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access this content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events. Parents and guardians should establish boundaries and standards for the appropriate and acceptable use of technology and communicate these boundaries and standards to their children. The acceptable use standards outlined in this policy apply to student use of technology via the DCS or any other electronic media or communications, including by means of a student's own personal technology or electronic device on school grounds or at school events.

Standards of Acceptable Use

Generally, the same standards of acceptable student conduct which apply to any school activity apply to use of the DCS. This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage.

District students must also adhere to the laws, policies, and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and student rights of privacy created by federal and state law.

Students who engage in unacceptable use of the DCS may lose access in accordance with applicable due process procedures, and may be subject to further discipline in accordance with the District *Code of Conduct*.

Student data files and other electronic storage areas are considered District property subject to control and inspection. The Computer Coordinator may access all files and communications without prior notice to ensure system integrity and that users are complying with the requirements of this policy. Students should not expect that information stored on the DCS will be private.

Notification

The District's AUP will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and students' obligations when accessing the DCS.

General Obligations Law § 3-112

Adopted: 7/5/18

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING

In compliance with the Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the District will ensure the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. These technology protection measures apply to Internet access by both adults and minors

with regard to visual depictions that are obscene, pornographic, or, with respect to the use of computers by minors, considered harmful to students. The District will provide for the education of students regarding appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms and regarding cyberbullying awareness and response. Further, appropriate monitoring of online activities of minors, as determined by the building or program supervisor, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the Board's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the District, including the selection of appropriate instructional materials and activities to enhance the schools' programs and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing any inappropriate sites. Proper safety procedures, as deemed appropriate by the applicable administrator or program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet may include, but will not be limited to, the following guidelines:

a) Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using email, chat rooms, instant messaging, and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of email, chat rooms, as well as social networking websites, may be blocked as deemed necessary to ensure the safety of students;

b) Monitoring logs of access in order to keep track of the websites visited by students as a measure to restrict access to materials harmful to minors;

c) In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy (AUP), unauthorized access, and other unlawful activities by minors are prohibited by the District and student violations of these policies may result in disciplinary action; and

d) Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use, and dissemination of personal identification information regarding students.

(Continued)

The determination of what is "inappropriate" for minors will be determined by the District and/or designated school official(s), the definition of which may vary depending on the circumstances of the situation and the age of the students involved in online research.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measure," "sexual act," and "sexual contact" will be as defined in accordance with CIPA and other applicable laws or regulations.

Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the District.

The District will provide certification, in accordance with the requirements of CIPA, todocument the District's adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking or filtering of access to certain material on the Internet) for all District computers with Internet access.

Internet Safety Instruction

In accordance with New York State Education Law, the District may provide to students in grades K through 12 instruction designed to promote the proper and safe use of the Internet. The Commissioner will provide technical assistance in the development of curricula for this course of study which will be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information, and support to aid in the safe usage of the Internet.

Additionally, students will be educated on appropriate interactions with other individuals on social networking websites and in chat rooms, as well as cyberbullying awareness and response.

Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

Despite the existence of District policy, regulations, and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access this content or material from their home, other locations off school premises, and/or with a student's own personal technology or electronic device on school grounds or at school events.

The District is not responsible for inappropriate content or material accessed via a student's own personal technology or electronic device or via an unfiltered Internet connection received through a student's own personal technology or electronic device.

(Continued)

Notification/Authorization

The District's AUP will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet.

The District has provided reasonable public notice and has held at least one public hearing or meeting to address this policy prior to Board adoption. Additional public notice and a hearing or meeting is not necessary if and when amendments are made to this policy.

This policy must be made available to the FCC upon request. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of this policy as well as any other District policies relating to the use of technology.

This policy is required to be retained by the school for at least five years after the funding year in which the policy was relied upon to obtain E-rate funding.

20 USC § 7131
47 USC §§ 254(h) and 254(l)
47 CFR Part 54
Education Law § 814

NOTE: Refer also to Policies #7315 -- Student Acceptable Use Policy (AUP)

Adopted: 7/5/18

Review the guide at: https://www.dunkirkcsd.org/Page/4914 DCSD 2020-2021 School Year **Please Read and Initial For Each Item Below:**	**Student Initial**	**Parent Initial**
1- I will not loan my Chromebook out to anyone, or leave it unattended unless it is locked in a secure place. My family is responsible for the cost of a replacement ($300) should my Chromebook become lost or stolen due to "gross negligence".		
2- I will report any damage immediately to the teacher/technology department. In the event of theft or damage by fire I will file a police report within 5 days of the incident. My family is responsible for the cost of a replacement or repair fees should the administration determine that damage or loss was caused by my vandalism or "gross negligence."		
3- I understand that I have no expectation of privacy on the Chromebook and that my use and content is monitored. I also understand that my Chromebook will be filtered and managed at home and at school and I will not try to access inappropriate material.		
4- I have read and understand our School District Code of Conduct and Acceptable Use Policy as approved by our Board of Education and agree to follow them at all times. I will not attempt to go around existing security measures such as internet filters.		
5- I agree to be a good digital citizen and not harass, bully, or be insensitive to others when I am online. This includes protecting my identity and passwords and not placing myself or others at risk by sharing personal information online.		
6- I understand that I will need to return the Chromebook and AC adaptor at the end of the school year . I will be charged $20 for any charger not returned.		
7- I have read and understand the attached Acceptable Use Policy and Internet Safety/Internet Content Filtering and give permission for my student to use District technology resources as required by the district.		

Student Name: (print clearly) _____ **Grade Level:** _____

Parent/Guardian Name: (print clearly) _____ **Relation to student:** _____

Parent Signature: _____ **Date:** _____

Chromebook Serial Number: _____ **Asset Tag Number:** _____

Distrito Escolar de la Ciudad de Dunkerque

Guía para llevar a casa para 1: 1 Programa de Chromebook

Esta guía es para ayudar a los padres, estudiantes y maestros a conocer y comprender las políticas del distrito para todos los estudiantes que forman parte del programa Chromebook 1: 1. Si alguien tiene alguna pregunta o inquietud, puede comunicarse con el Departamento de Tecnología utilizando la información de contacto a continuación.

Jeremy Dobek **Technology Coordinator** **support@Dunkirkcsd.org** **716-366-9300 ext: *2025**	**Tara Jakse** **Technology Secretary** **support@Dunkirkcsd.org** **716-366-9300 ext: *2021**

Distribución

Los estudiantes de los grados 3-12 serán parte del programa Chromebook 1: 1 del Distrito.

Los Chromebooks se distribuirán durante la orientación para padres / estudiantes y se recogerán al final del año escolar.

Se debe firmar una hoja de firmas (al final de este folleto) antes de que se distribuyan los Chromebooks.

Requisitos para que se le asigne un Chromebook:

1. La hoja de acuerdo firmada por padres y estudiantes

Lista de distribución de equipo: (es responsabilidad personal del estudiante cuidar el dispositivo que se le prestó y entregarlo todo al final del año escolar)

1. Chromebook
2. Adaptador de corriente (cargador)
3. Estuche de transporte (grados 3-5) o mochila (grados 6-12)

Expectativa diaria

Se espera que los padres informen inmediatamente al Departamento de Tecnología de cualquier problema o que falte chromebooks. Usted puede reportar cualquier problema a través del teléfono o correos electrónicos enumerados al principio y al final de este documento.

Cuidado / Daño

Los estudiantes son responsables del equipo asignado a ellos. Esto incluye el Chromebook y el cargador. El cuidado adecuado de los chromebooks asignados es necesario para la longevidad del dispositivo. Los estudiantes deben seguir estos pasos necesarios mientras los dispositivos están en su posesión.

No camines con un Chromebook abierto.

No se coloque en el suelo donde se puede pisar o patear.

No use ni tenga chromebooks alrededor de líquidos (incluidas las bebidas).

Nunca fuerce el cierre o la apertura de una pantalla y sólo abra la pantalla por el bisel lateral, nunca por la propia pantalla.

Coloque siempre el Chromebook sobre una superficie sólida como un escritorio o una mesa.

Nunca deje que nadie tome prestado su dispositivo asignado.

El Departamento de Tecnología debe ser notificado inmediatamente cuando hay un problema con su dispositivo. Cualquier dispositivo que tenga un problema que no se informe inmediatamente al Departamento de Tecnología se clasificará como maltrato/negligencia.

El Departamento de Tecnología inspeccionará todos los dispositivos que se entregen para reparaciones y tomará la determinación de si la causa del problema se debe a un mal funcionamiento o defecto mecánico o a negligencia/abuso. El costo de las reparaciones es solo por el costo de las piezas y no por la mano de obra.

Dispositivos con problemas debidos a defectos:

Si un dispositivo tiene un problema debido a un defecto y debe ser entregado para reparaciones, el padre tendrá que ponerse en contacto con el departamento de tecnología para ver si hay un reemplazo disponible. Es posible que un reemplazo no esté disponible de inmediato.

Ejemplos de problemas debidos a un mal funcionamiento/defecto mecánico o por desgaste normal:

La luz de fondo se apagó y la imagen muy oscura en la pantalla.
Líneas a través de la pantalla cuando se enciende.
No cobrará más.

Dispositivos con problemas debidos al maltrato/negligencia:

Si un dispositivo tiene un problema debido al maltrato/negligencia y debe ser entregado para reparaciones, el padre tendrá que ponerse en contacto con el departamento de tecnología para ver si hay un reemplazo disponible. Es posible que un reemplazo no esté disponible inmediatamente. Dependiendo de los daños de los cargos del dispositivo pueden incurrir en.

Ejemplos de problemas debido al maltrato/negligencia:

Pantalla rota / rota
Daños por agua
Cargador perdido

Dispositivos perdidos y robados:

Si se pierde un dispositivo, el padre tendrá que ponerse en contacto con el departamento de tecnología para ver si hay un reemplazo disponible. Es posible que un reemplazo no esté disponible inmediatamente. Si se pierde habrá un cargo de $300 que se puede pagar en la oficina de administración/ negocios. Cualquier costo será comunicado y cobrado a través de la oficina de negocios. Si un dispositivo es robado, **debe** hacerse un informe policial. Si no se hace ningún informe policial, el dispositivo se considerará perdido y se aplicarán los procedimientos para un dispositivo perdido.

Fi filtrado / bloqueo / monitoreo

DCSD utiliza una serie de métodos de filtrado tanto en los terrenos de la escuela como fuera de la escuela. Los filtros se establecen como mínimo y bloquean las categorías de pornografía, odio, compras, redes sociales y piratería, por nombrar algunas. Mientras que los filtros capturan mucho, ninguno es infalible y dicho contenido puede llegar a través. Como una capa adicional de seguridad, todos los sitios web a los que va el estudiante mientras que en los dispositivos propiedad de DCSD se registran y se mantienen para su revisión y se auditan periódicamente. Este registro se realiza independientemente de dónde se utilice el dispositivo.

Los estudiantes y los padres/tutores deben tener en cuenta que el hecho de que un sitio web no esté bloqueado no significa que sea apropiado ser visto en un dispositivo propiedad de la escuela. Los sitios de juegos, los sitios de redes sociales y cualquier sitio que pueda ir en contra del código de decencia general de la escuela están estrictamente prohibidos. Se tomarán medidas disciplinarias para cualquier estudiante que visite a sabiendas y

continuamente estos sitios. Recuerde que TODAS las actividades web en los dispositivos propiedad de la escuela están registradas y sujetas a monitoreo y revisión.

Cualquier estudiante puede ser transferido a un nivel más alto de filtrado debido a cualquiera de las razones enumeradas a continuación. Solo los directores de la escuela, los administradores de la escuela o los padres pueden autorizar una restricción más alta a un estudiante. Si hay una necesidad de una restricción más alta para un estudiante, esa restricción será comunicada a los padres, así como, a todos los maestros de ese estudiante.

Causa de un mayor nivel de restricción:

1. A petición de un padre. (Un padre puede solicitar un nivel de restricción una vez en un año escolar).
2. No mantener se en la tarea durante el horario escolar.
3. Intimidación.
4. Bajar las calificaciones (cuando se ha determinado que el uso en el hogar o en la escuela del dispositivo puede estar afectando los niveles de grado).
5. Acceso a sitios no adecuados para la edad.
6. Cuando forma parte de un plan del IEP.
7. Maltrato general del dispositivo.
8. Préstamo del departamento de tecnología y no devolución (ejemplo, cargadores)

Este nivel más alto de filtrado bloquea a los alumnos de toda la actividad web, excepto por lo que hay en una lista blanca muy específica. Cualquier miembro de la facultad puede enviar un sitio web para ser agregado a esta lista blanca. Los miembros de la facultad envían solicitudes de lista blanca por correo electrónico. Esta misma lista blanca se aplica a todos los estudiantes en esta restricción más alta. Se puede obtener una copia de la lista blanca actual a petición.

Durante las horas de 7:30 am y 3:00 pm, los profesores tienen la capacidad de levantar, en tiempo real, lo que está en la pantalla de Un estudiante Chromebook. También tienen la capacidad de bloquear la pantalla de la computadora del estudiante, tomar una captura de pantalla de lo que está en la pantalla de la computadora del estudiante y cerrar y abrir las pestañas del sitio web según sea necesario. Lo que la facultad NO tiene acceso a es la cámara web en las computadoras del estudiante. DCSD en su conjunto no mantiene la capacidad ni aprueba la capacidad de acceder a los dispositivos de los estudiantes conectados webcam o micrófono.

E-MAIL

Todos los estudiantes tienen acceso al sistema de correo electrónico de los distritos. Sin embargo, esto se utiliza principalmente para enviar un correo electrónico a los profesores y recibir recursos educativos. No se pueden enviar o recibir correos electrónicos externos.

Preguntas / preocupaciones

Si hay alguna pregunta, comentario o inquietud en cualquier momento, póngase en contacto con el Departamento de Tecnología

Jeremy Dobek **Technology Coordinator** **support@Dunkirkcsd.org** **716-366-9300 ext: *2025**	**Tara Jakse** **Technology Secretary** **support@Dunkirkcsd.org** **716-366-9300 ext: *2021**

ASUNTO: POLÍTICA DE USO ACEPTABLE PARA ESTUDIANTES (AUP)

La Junta proporcionará acceso a varios recursos de información computarizados a través del sistema informático del Distrito ("DCS") que consiste en software, hardware, redes informáticas y sistemas de comunicaciones electrónicas. Esto puede incluir acceso al correo electrónico, servicios en línea e Internet. Puede incluir la oportunidad para que algunos estudiantes tengan acceso independiente al DCS desde su hogar u otras ubicaciones remotas. Todo uso del DCS, incluido el uso independiente fuera de las instalaciones de la escuela, estará sujeto a esta política. Además, todo el uso de DCS debe ser en apoyo de la educación o la investigación y consistente con las metas y propósitos del Distrito.

Acceso a Contenido/Material Inapropiado y Uso de Tecnología Personal o Dispositivos Electrónicos

Esta política está destinada a establecer pautas generales para el uso aceptable del estudiante del DCS y también para dar a los estudiantes y padres o tutores aviso de que el uso de los estudiantes del DCS proporcionará a los estudiantes acceso a redes informáticas externas no controladas por el Distrito. El Distrito no puede examinar o revisar todo el contenido o materiales disponibles en estas redes informáticas externas, por lo tanto, parte del contenido o materiales disponibles en estas redes externas pueden considerarse inadecuados para el uso o el acceso de los estudiantes por parte de los padres o tutores.

Es prácticamente imposible impedir por completo el acceso a contenido o material que pueda considerarse inapropiado para los estudiantes. Los estudiantes pueden tener la capacidad de acceder a este contenido o material desde su casa, otros lugares fuera de las instalaciones de la escuela y / o con la tecnología personal o dispositivo electrónico de un estudiante en los terrenos de la escuela o en eventos escolares. Los padres y tutores deben establecer límites y normas para el uso apropiado y aceptable de la tecnología y comunicar estos límites y normas a sus hijos. Las normas de uso aceptables descritas en esta política se aplican al uso de la tecnología por parte de los estudiantes a través del DCS o cualquier otro medio electrónico o comunicaciones, incluso por medio de la propia tecnología personal o dispositivo electrónico de un estudiante en los terrenos escolares o en eventos escolares.

Estándares de uso acceptable

Generalmente, los mismos estándares de conducta aceptable de los estudiantes que se aplican a cualquier actividad escolar se aplican al uso del DCS. Esta política no intenta articular todos los usos requeridos y/o aceptables del DCS; ni es la intención de esta política definir todo uso inapropiado.

Los estudiantes del distrito también deben adherirse a las leyes, políticas y reglas que rigen las computadoras, incluidas, entre otras, las leyes de derechos de autor, los derechos de los editores de software, los acuerdos de licencia y los derechos de privacidad de los estudiantes creados por las leyes federales y estatales.

Los estudiantes que participan en un uso inaceptable del DCS pueden perder el acceso de acuerdo con los procedimientos de debido proceso aplicables, y pueden estar sujetos a mayor disciplina de acuerdo con el Código de Conducta del Distrito.

Los archivos de datos de los estudiantes y otras áreas de almacenamiento electrónico se consideran propiedad del Distrito sujetas a control e inspección. El Coordinador de

Computación puede acceder a todos los archivos y comunicaciones sin previo aviso para garantizar la integridad del sistema y que los usuarios cumplen con los requisitos de esta política. Los estudiantes no deben esperar que la información almacenada en el DCS sea privada.

Notificación

El AUP del Distrito se difundirá a los padres y estudiantes con el fin de proporcionar aviso de los requisitos, expectativas y obligaciones de los estudiantes de la escuela al acceder al DCS.

Ley General de Obligaciones§ 3-112

Adoptado: 7/5/18

ASUNTO: FILTRADO DE CONTENIDO DE INTERNET/SEGURIDAD EN INTERNET

De conformidad con la Ley de Protección de Internet de los Niños (CIPA) y el Reglamento de la Comisión Federal de Comunicaciones (FCC), el Distrito garantizará el uso de medidas de protección tecnológica (es decir, filtrado o bloqueo del acceso a cierto material en Internet) en todos los ordenadores del Distrito con acceso a Internet. Estas medidas de protección tecnológica se aplican al acceso a Internet tanto por parte de adultos como de menores con respecto a las representaciones visuales obscenas, pornográficas o, con respecto al uso de computadoras por parte de menores, consideradas perjudiciales para los estudiantes. El Distrito proporcionará la educación de los estudiantes con respecto al comportamiento apropiado en línea, incluyendo interactuar con otras personas en los sitios web de redes sociales y en las salas de chat y con respecto a la conciencia y respuesta del ciberacoso. Además, también se aplicará un seguimiento adecuado de las actividades en línea de los menores, según lo determine el programa o supervisor del programa, para garantizar la seguridad de los estudiantes al acceder a Internet.

Además, la decisión de la Junta de utilizar medidas de protección tecnológica y otros procedimientos de seguridad para el personal y los estudiantes al acceder a Internet fomenta la misión educativa del Distrito, incluida la selección de materiales y actividades de instrucción adecuados para mejorar los programas de las escuelas y ayudar a garantizar la seguridad del personal y los estudiantes mientras está en línea.

Sin embargo, ninguna tecnología de filtrado puede garantizar que el personal y los estudiantes podrán acceder a sitios inapropiados. Se proporcionarán procedimientos de seguridad adecuados, según lo considere apropiado por el administrador o supervisor del programa correspondiente, para garantizar el cumplimiento de la CIPA.

Además del uso de medidas de protección tecnológica, el seguimiento de las actividades en línea y el acceso de los menores a materia inapropiada en Internet pueden incluir, pero no se limitarán a, las siguientes directrices:

a) Asegurar la presencia de un maestro y/u otro personal apropiado del Distrito cuando los estudiantes están accediendo a Internet, incluyendo, pero no limitado a, la supervisión de los menores al usar correo electrónico, salas de chat, mensajería instantánea y otras formas de comunicaciones electrónicas directas. Según lo determine el administrador del edificio apropiado, el uso de correo electrónico, salas de chat, así como sitios web de redes sociales, puede ser bloqueado como se considere necesario para garantizar la seguridad de los estudiantes;

b) Monitoreo de registros de acceso con el fin de realizar un seguimiento de los sitios

web visitados por los estudiantes como una medida para restringir el acceso a materiales dañinos para los menores;

c) En cumplimiento con esta Política de Seguridad en Internet, así como con la Política de Uso Aceptable (AUP) del Distrito, el acceso no autorizado y otras actividades ilegales por parte de menores están prohibidos por el Distrito y las violaciones de estas políticas por parte de los estudiantes pueden resultar en medidas disciplinarias; Y

d) Supervisión y notificación apropiadas a los menores con respecto a la prohibición de la divulgación, uso y difusión no autorizados de información de identificación personal con respecto a los estudiantes.

La determinación de lo que es "inapropiado" para los menores será determinada por el Distrito y/o los funcionarios escolares designados, la definición de los cuales puede variar dependiendo de las circunstancias de la situación y la edad de los estudiantes involucrados en la investigación en línea.

Los términos "menor", "pornografía infantil", "nocivo para los menores", "obsceno", "medida de protección tecnológica", "acto sexual" y "contacto sexual" serán los definidos de acuerdo con la CIPA y otras leyes o reglamentos aplicables.

Bajo ciertas circunstancias específicas, las medidas de tecnología de bloqueo o filtrado pueden ser desactivadas para adultos involucrados en investigaciones de buena fe u otros propósitos legales. El poder de inhabilitar sólo puede ser ejercido por un administrador, supervisor u otra persona autorizada por el Distrito.

El Distrito proporcionará certificación, de acuerdo con los requisitos de cipA, para documentar la adopción y aplicación por parte del Distrito de su Política de Seguridad en Internet, incluyendo el funcionamiento y la aplicación de medidas de protección tecnológica (es decir, bloqueo o filtrado de acceso a cierto material en Internet) para todos los ordenadores del Distrito con acceso a Internet.

Instrucciones de seguridad en internet

De acuerdo con la Ley de Educación del Estado de Nueva York, el Distrito puede proporcionar a los estudiantes en los grados K a 12 instrucción diseñada para promover el uso adecuado y seguro de Internet. El Comisionado proporcionará asistencia técnica en el desarrollo de planes de estudio para este curso de estudio que serán apropiados para la edad y se desarrollarán de acuerdo con las necesidades y capacidades de los estudiantes en los niveles de grado sucesivos con el fin de proporcionar conciencia, habilidades, información y apoyo para ayudar en el uso seguro de Internet.

Además, los estudiantes serán educados sobre interacciones apropiadas con otras personas en sitios web de redes sociales y en salas de chat, así como conciencia y respuesta sobre ciberacoso.

Acceso a contenido / material inapropiado y uso de tecnología personal o dispositivos electrónicos

A pesar de la existencia de políticas, regulaciones y pautas del Distrito, es prácticamente imposible impedir completamente el acceso a contenido o material que pueda considerarse inapropiado para los estudiantes. Los estudiantes pueden tener la capacidad de acceder a este contenido o material desde su casa, otros lugares fuera de las instalaciones de la escuela y/o con la tecnología personal o dispositivo electrónico de un estudiante en los terrenos de la escuela o en eventos escolares.

El Distrito no es responsable de contenido o material inapropiado al que se acceda a través de la propia tecnología personal o dispositivo electrónico de un estudiante o a través de una conexión a Internet sin filtrar recibida a través de la propia tecnología personal o dispositivo electrónico de un estudiante.

Notificación / Autorización

El AUP del Distrito se difundirá a los padres y estudiantes con el fin de proporcionar aviso de los requisitos, expectativas y obligaciones de los estudiantes al acceder a Internet.

El Distrito ha proporcionado un aviso público razonable y ha celebrado al menos una audiencia o reunión pública para abordar esta política antes de la adopción de la Junta. No es necesario un aviso público adicional y una audiencia o reunión si se hacen modificaciones a esta política y cuando se.

Esta política debe ponerse a disposición de la FCC previa solicitud. Además, se tomarán las medidas apropiadas para garantizar la disponibilidad al público de esta política, así como cualquier otra política del Distrito relacionada con el uso de la tecnología.

Esta política debe ser retenida por la escuela durante al menos cinco años después del año de financiación en el que se basó la política para obtener financiación a tipo Electrónico.

20 USC § 7131
47 USC §§ 254(h) and 254(l)
47 CFR Part 54
Ley de Educación § 814

NOTA: Consulte también las Políticas # 7315 - Política de uso aceptable del estudiante (AUP)

Adoptado: 7/5/18

Revise la guía en: https://www.dunkirkcsd.org/Page/4914 **DCDS 2020-2021 año escolar** favor Lea y inicial para cada elemento continuación:	**Estudiante Inicial**	**Padre Inicial**
1- No prestaré mi Chromebook a nadie, ni lo dejaré desatendido a menos que esté bloqueado en un lugar seguro. Mi familia es responsable del costo de un reemplazo ($300) en caso de que mi Chromebook se pierda o sea robado debido a una "negligencia grave".		
2- Reportaré cualquier daño inmediatamente al departamento de maestros/tecnología. En caso de robo o daño por incendio presentaré un informe policial dentro de los 5 días posteriores al incidente. Mi familia es responsable del costo de un reemplazo o cargos de reparación en caso de que la administración determine que el daño o pérdida fue causado por mi vandalismo o "negligencia grave".		
3- Entiendo que no tengo ninguna expectativa de privacidad en el Chromebook y que mi uso y contenido es monitoreado. También entiendo que mi Chromebook será filtrada y administrada en casa y en la escuela y no voy a tratar de acceder a material inapropiado.		
4- He leído y entiendo nuestro Código de Conducta del Distrito Escolar y la Política de Uso Aceptable según lo aprobado por nuestra Junta de Educación y acepto seguirlos en todo momento. No intentaré ir alrededor de las medidas de seguridad existentes, como los filtros de Internet.		
5- Acepto ser un buen ciudadano digital y no acosar, intimidar o ser insensible a los demás cuando estoy en línea. Esto incluye proteger mi identidad y contraseñas y no ponerme a mí mismo o a otros en riesgo compartiendo información personal en línea.		
6- Entiendo que tendré que devolver el Chromebook y el adaptador de CA al final del año escolar. Se me cobrará $ 20 por cualquier cargador no devuelto		
7- He leído y entiendo la Política de Uso Aceptable adjunta y el Filtrado de Contenido de Seguridad de Internet/Internet y doy permiso para que mi estudiante use los recursos tecnológicos del Distrito según lo requiera el distrito.		

Nombre del estudiante: (imprime claramente) _____ **Nivel de grado:** _____

Nombre del Padre de Familia / Guardian: (imprime claramente) _____ **Relación con el alumno:** _____

Firma de los padres: _____ **Fecha:** _____

Número de serie de la Chromebook: _____ **Número de etiqueta de activo:** _____

District Wi-Fi Hotspot locations / Ubicaciones de puntos de acceso Wi-Fi del distrito

The district Wi-Fi hotspots will allow our district chromebooks to connect automatically to the internet when they are in range of the signal. / Los puntos de acceso Wi-Fi del distrito permitirán que nuestros chromebooks de distrito se conecten automáticamente a Internet cuando estén dentro del alcance de la señal

Dunkirk High School

Dunkirk Middle School

School #3

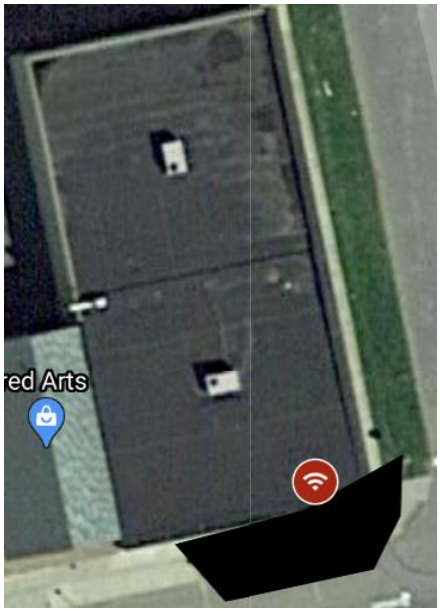
School #4

District Wi-Fi Hotspot locations / Ubicaciones de puntos de acceso Wi-Fi del distrito

School #5

School #7

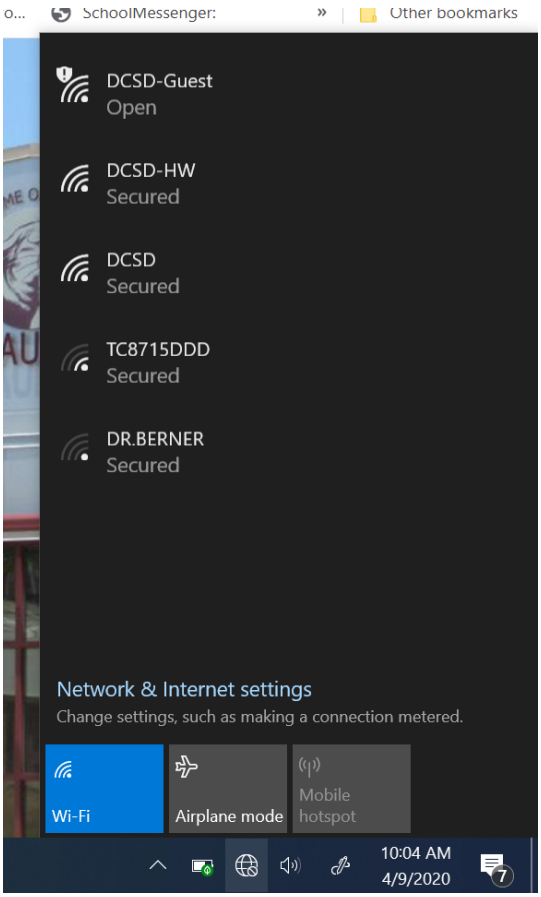
Boorady Center



District Wi-Fi Hotspot locations / Ubicaciones de puntos de acceso Wi-Fi del distrito

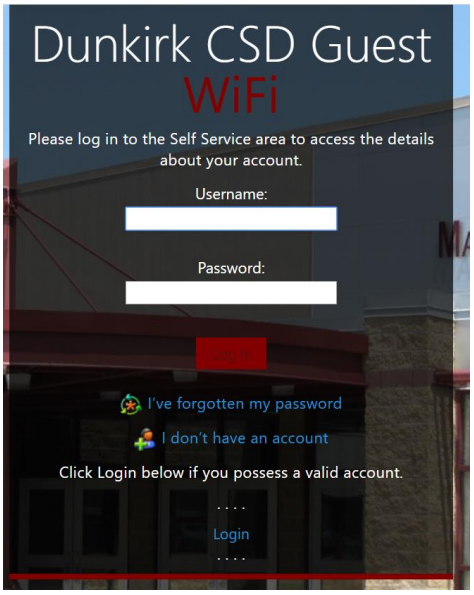
Connect to our hotspot on a personal computer / Conéctese a nuestro punto de acceso en una computadora personal

1) When in range of our hotspot, go to your wifi list and connect to “DCSD-Guest” / Cuando esté dentro del alcance de nuestro punto de acceso, vaya a su lista de wifi y conéctese a "DCSD-Guest"

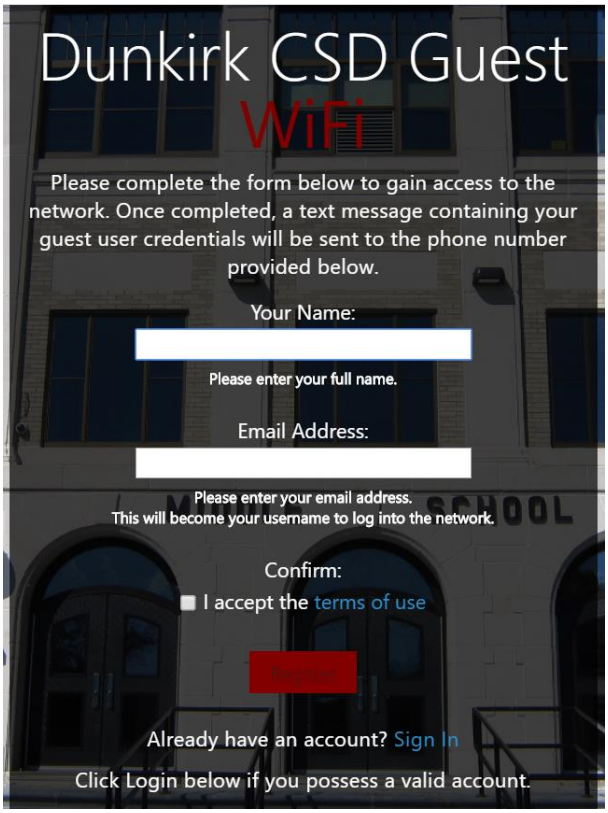


District Wi-Fi Hotspot locations / Ubicaciones de puntos de acceso Wi-Fi del distrito

2) Enter your username and pin code if you have already created an account or click on the "I don't have an account" link / Ingrese su nombre de usuario y código PIN si ya ha creado una cuenta o haga clic en el enlace "I don't have an account"

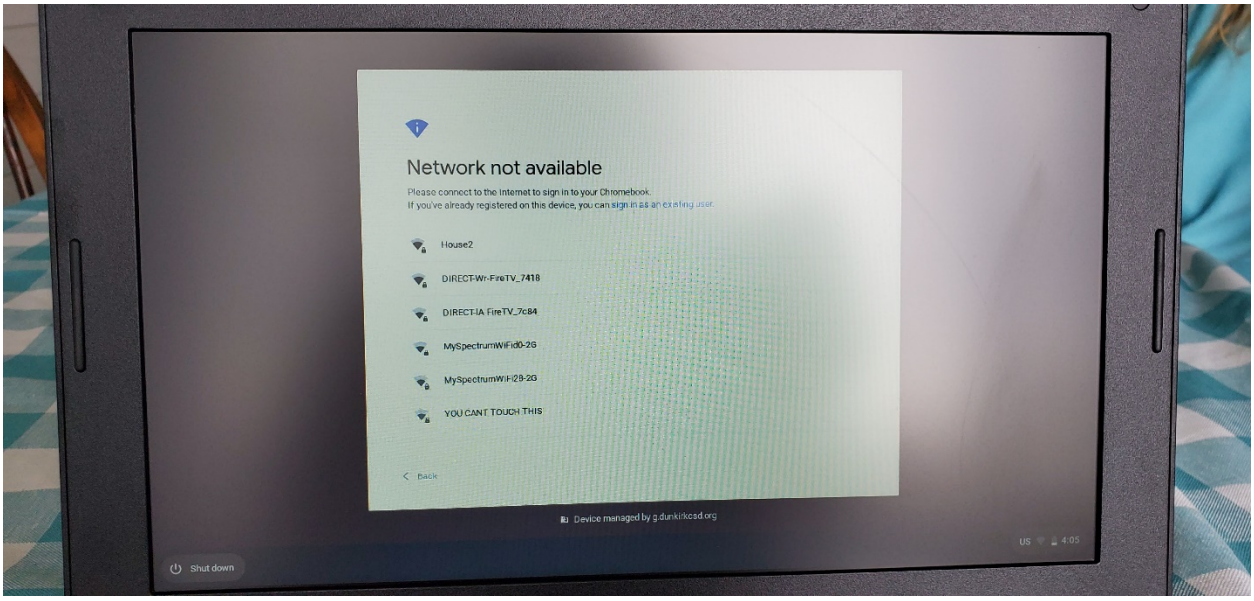


3) Fill out the form and check your email for login information. / Complete el formulario y revise su correo electrónico para obtener información de inicio de sesión



How to connect Chromebook to Wi-Fi / Cómo conectar Chromebook a Wi-Fi

1. Power on Chromebook then find your Wi-Fi name on the list / Enciende Chromebook y encuentra tu nombre de Wi-Fi en la lista



2. Select your Wi-Fi name and enter password / Selecciona tu nombre de Wi-Fi e introduce la contraseña