Verona Area School District Administrative Rules
Section: Instruction
Rule: 471 - Student Internet Safety/Appropriate Use of Technology
Last Updated: May 30, 2023
Formerly Board Policy 363.2 Exhibit
(Aligned with OE 11: Instructional Program)

STUDENT INTERNET SAFETY/APPROPRIATE USE OF TECHNOLOGY RULES

A. General

1. The District's technology resources, including District-owned mobile devices, software, networks, and network connections, are open to regulated use by students as a privilege. Each student who uses the District's technology resources is required to follow the District's established expectations for appropriate use.

2. Students should approach their use of technology resources with the understanding that all of the school rules and expectations that apply to in-person interactions and to the student's general conduct while at school or while under the supervision of a school authority also apply to their use of District technology, their online conduct, and their electronic communications. This rule and various other District policies, rules, and regulations include additional requirements and expectations that are directly related to the use of technology resources, including District-owned mobile devices. If a student has a question concerning any policy, rule, regulation, or directive that relates to technology resources, or if a student encounters a situation in which they are uncertain about any expectation for appropriate use or about how to proceed, the student should contact a teacher or an administrator to obtain appropriate guidance.

3. Because the District's technology resources belong to the District, users have no privacy expectation in the contents of any of their personal files, including but not limited to email and other electronic communications, on the District's technology resources. Users also have no privacy expectations on any of the websites that they may visit by using the District's technology resources. Usage of the District's technology resources may be monitored without notice to determine compliance with the District's Internet safety and appropriate use policy and rules. Through such a monitoring process, the District may inadvertently obtain access information for a student's personal Internet account through the use of an electronic device or program that monitors the District's network or through an electronic communications device supplied or paid for in whole or in part by the District. If such personal Internet access information is obtained by the District, the District shall not use that access information to access the student's personal Internet account unless permitted by law. Routine maintenance and monitoring of the District's technology resources may also lead to the discovery that the user has or is violating the District's policy, rules, or law. An individual search will be conducted if there is a reasonable suspicion that a user has violated the law or the District's Internet safety and appropriate use policy and/or rules. The search will be conducted consistent with legal requirements.

4. The District makes no guarantees of any kind, either expressed or implied that the functions

of the services provided by or through the District technology resources will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the District's technology resources.

5. The use of AI technology in the Verona Area School District must comply with the district's Acceptable Use Policy (AUP). AI technology can be a resource for enhancing learning and teaching experiences, but it must be used responsibly and ethically. Students, teachers, and staff members must ensure that any AI systems they use are age-appropriate and that they do not violate the privacy of other individuals. The use of AI for academic purposes should align with the district's curriculum and instruction goals. Additionally, students, teachers, and staff must use AI tools responsibly, avoiding any form of plagiarism or cheating. Failure to follow these guidelines may result in disciplinary action. By following these guidelines, we can ensure that AI technology is used appropriately and safely within the Verona Area School District.

B. Parental Role and Responsibilities

1. Upon consultation with the site administrator, and consistent with rules governing the confidentiality of student records, parents/guardians may investigate the contents of their children's technology use files upon request.

2. There is a wide range of material available on the Internet, some of which may not fit with a particular family's values. Although the District has an Internet filtering measure in place, it is impossible to ensure complete protection from access to inappropriate material. It is not possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the District's technology resources.

3. In accordance with the Acceptable Use Policy for VASD students, parents/guardians are responsible for ensuring that they monitor the child's use of the internet and technology resources during non-school hours. This includes but is not limited to, student devices, district-issued email accounts, online learning spaces, collaboration tools and applications, and educational resources. Parent(s)/guardian(s) need to set clear expectations on the appropriate use of electronic devices during non-school hours. If your child is not following these rules, you have the right to limit access while the device is at home.

C. Appropriate Use Rules

1. <u>Personal Safety</u>
    a. Students will not post personal contact information about themselves or other people on the Internet. Personal contact information includes but is not limited to, home address and telephone number. Exceptions may be made for career or post-secondary educational research purposes, or with approval by an instructor.

b. Students will not agree to meet with someone they have met online without their parent (s)/guardian(s) approval and participation.

c. Students must immediately disclose to their teacher or other staff members present any electronic communications (e.g., messages) they receive that are inappropriate or that make them feel uncomfortable.

2. Social Networking

a. Web resources that emphasize collaboration and sharing, such as online chat rooms, wikis, blogs, forums, and other Web 2.0 tools, may be used for educational or school-related purposes as determined by District instructional or administrative staff. All other use of social networking sites and resources by students is prohibited.

3. Unauthorized Activities

a. Students may not use the District's technology resources for commercial purposes, including, but not limited to, purchasing, selling, or advertising goods or services.

b. Students will not attempt to gain unauthorized access to the District's technology resources or to any other computer system through the District's technology resources or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files.

c. There shall be no downloading or installing of programs or applications onto District technology resources, including District-owned mobile devices, without teacher permission. Students are not allowed to load personal software onto District technology resources, including a District-owned mobile device, at any time.

d. Students will not make deliberate attempts to disrupt the District's technology resources' performance or destroy data by intentionally spreading computer viruses or by any other means.

e. Students will not use the District's technology resources to engage in any illegal act or other action that violates any other District policy or rule.

f. Mobile devices come with a standardized image already loaded. Any other image set as the desktop background or screensaver must be in line with District policies and rules. Inappropriate media may not be used, which includes any presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, or gang-related symbols.

g. Mobile devices come equipped with special functions such as a webcam. Webcams are to be used for educational purposes only, under the direction of the teacher. Listening to music or watching movies on the device is not allowed during school hours without permission from the teacher. Permission will be given only for media used to complete a school project or assignment. Students may be permitted to listen to music or watch a movie on a District-owned mobile device during non-instructional time and off school premises.

h. Online gaming, music downloads and streaming, and video downloads and streaming are not allowed on District technology equipment, including District-owned mobile devices, except with teacher permission and only if such activity is in support of

education, as determined by instructional staff. Online gambling is strictly prohibited.

4. System Security and Data Management
    a. Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their personal accounts. Students may only log in to their assigned mobile device or District network under their assigned username. Students may not share their log-in and password with other students or individuals. Students may share their log-in and password with their parents/guardians.

    b. Students will immediately notify the site Educational Technology Coordinator if they have identified a possible security problem. Students will not search for security problems because this may be construed as an unauthorized attempt to gain access, i.e. computer hacking.

    c. All students have access to a network drive and a Google cloud-based drive on which to store data. It is the responsibility of the student to manage their files, saving them as needed to either the network drive or Google Cloud.

5. Cyber Bullying/Respect for Privacy
    a. Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. Restrictions against inappropriate language apply to public messages, private messages, and material posted on websites.

    b. Students will not post information that, if acted upon, could endanger the health, safety, or welfare of other individuals.

    c. Students will not engage in personal attacks, including but not limited to, prejudicial or discriminatory attacks.

    d. Students will not harass or bully another person. “Harassment” refers to physical or verbal conduct, or psychological abuse, by any person that disrupts or interferes with a student’s school performance, or creates an intimidating, hostile, or offensive learning environment. If a user is told by a person to stop sending him/her messages, he/she must stop.

    e. Students will not engage in cyberbullying. “Cyberbullying” includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings that are materially or substantially disruptive or violate District policy. In situations in which the cyberbullying originated from a non-school computer or other communication devices such as a cell phone and is brought to the attention of school officials, any disciplinary action taken shall be based upon whether the conduct is determined to be substantially disruptive of the educational process so that it markedly interrupts or substantially impedes the day-to-day operations of a school. In addition, such conduct must also be in violation of a publicized school policy. Such conduct includes but is not limited to, harassment or making a threat off school grounds that is intended to endanger the health, safety, or property of others at

school or at a school-related activity wherever held, or toward a District employee or School Board member.

f. Students will not knowingly or recklessly post false or defamatory information about a person or organization.

6. Plagiarism and Copyright Infringement
   a. Students will not plagiarize. Plagiarism is taking the works of others and presenting them as if they were original to the user. District policies on plagiarism will govern the use of material accessed through District technology resources.

   b. Students will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies acceptable use of that work, the user must follow the expressed requirements. If the user is unsure whether or not he/she can use a work, he/she should request permission from the copyright owner and appropriately reference it. District policies on copyright govern the use of material accessed through District technology resources.

7. Inappropriate Access to Material
   a. Students will not use the District's technology resources to access or view material that is profane or obscene (i.e., pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

   b. If a student inadvertently accesses or views such information, he/she should immediately disclose the inadvertent access in a manner specified by his/her teacher. This will protect users against an allegation that they have intentionally violated District policy and rules.

   c. If a student receives inappropriate material through electronic transmission (e.g., email), the student should notify the sender that such material is forbidden and should delete the material. If the sender continues to send such material, the student should notify his/her teacher or site administrator.

D. Personally-Owned Laptops and Other Computing or Communications Devices

1. A personally-owned laptop computer, handheld computer, or other computing or communications device may be connected to the Internet at school only through the District's public wireless network, which allows filtered web-only access to the Internet. Connecting a laptop or other device to a non-networked device is allowed for instructional purposes.

2. The laptop computer, handheld computer, or other computing or communications device is to be used in compliance with District policies and rules, including but not necessarily limited to those applicable to Internet safety and appropriate use of District technology resources. Any violation of such policies or rules may result in the exclusion of the device from school and/or discipline of the person who has violated the policy and/or rule.

3. Any student who brings a laptop computer, handheld computer, or other computing device to school must use it as an instructional tool and only for the school curriculum. It may not be

used as an entertainment system. Students must turn off and put away a personally-owned laptop, handheld computer, or other computing device when directed by a staff person.

4. Personally-owned devices will not be able to access district printers or copiers.

5. If a personally-owned technology device (e.g., cell phone) is found, or is confiscated, the person recovering the device is not authorized to view the contents of the device. District protocol requires staff to place the device in a secure location, label it with the time/date, and turn it into the office. The district administrative staff or agent and/or a law enforcement representative are the only ones authorized to view the contents, and any search or review of the contents of the device must be consistent with legal requirements.

6. The District may examine personally-owned computers and other communications devices and search their contents if there is a reason to believe that school policies, rules or regulations, or laws have been violated. The scope of the search will be limited to the violation of which the student is accused, and the search will be conducted in a manner consistent with legal requirements. Individuals have no expectation of privacy in the use of the District's wireless network or technology systems and such use is subject to being monitored.

7. Students are not required to bring personally-owned laptop computers or other communications devices to school. The District accepts no responsibility for the loss, theft, or damage of personal property brought to school by students. Any laptop computer, handheld computer, or other communications device is the responsibility of the student who brought the device to school.

E. Policy and Rule Violations

1. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the District technology resources.

2. In the event there is an allegation that a student has violated the District Internet Safety and Appropriate Use Policy and/or rules, staff will investigate and meet with the appropriate individuals. The student will be given an opportunity to be heard in the manner set forth in the building disciplinary codes. Disciplinary actions are tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Consequences of violations of the Internet safety and acceptable use policy and rules include but are not limited to:

   - Suspension of network privileges
   - Revocation of network privileges
   - Suspension of Internet privileges
   - Revocation of Internet privileges
   - School suspension and/or expulsion
   - Legal action and prosecution by the authorities
   - Other disciplinary action

Normas administrativas del Distrito Escolar del Área de Verona
Sección: Instrucción
Norma: 471 - Seguridad estudiantil en internet/Uso apropiado de la tecnología
Última actualización: 30 de mayo 2023
Anteriormente Política de la Junta Directiva, Punto 363.2
(Alineado con OE 11: Programa instructivo)

SEGURIDAD ESTUDIANTIL EN INTERNET/USO APROPIADO DE LA TECNOLOGÍA

A. General

1. Los recursos tecnológicos del distrito, incluidos los dispositivos móviles, el software, las redes y las conexiones a las redes propiedades del distrito, están a la disposición - con uso regulado y como privilegio - de los estudiantes. Se exige que todo estudiante que utilice los recursos tecnológicos del distrito siga las expectativas establecidas por el distrito en cuanto a su uso apropiado.

2. Los estudiantes deben contemplar su uso de los recursos tecnológicos con el entendimiento de que todas las normas y expectativas escolares aplicables a las interacciones en persona y a la conducta general dentro del recinto escolar o bajo la supervisión de autoridades escolares también son aplicables a su uso de la tecnología del distrito, su conducta en línea y sus comunicaciones electrónicas. Esta norma, junto con las otras políticas, normas y regulaciones del distrito, incluyen exigencias y expectativas adicionales directamente relacionadas con el uso de recursos tecnológicos, incluyendo los dispositivos móviles propiedades del distrito. Si un estudiante tiene preguntas sobre cualquier política, norma, regulación o directiva vinculada con los recursos tecnológicos, o si un estudiante se encuentra en una situación donde no está seguro sobre las expectativas en cuanto al uso apropiado o cómo proceder, debe contactar con un maestro o administrador para recibir la orientación indicada.

3. Dado que los recursos tecnológicos del distrito son propiedad del distrito, los usuarios no tienen derecho a expectativas de privacidad respecto al contenido de sus archivos personales, incluyendo pero no limitado al correo electrónico y otras comunicaciones electrónicas dentro de los recursos tecnológicos del distrito. Los usuarios tampoco tienen derecho a expectativas de privacidad en ninguna página web que visiten utilizando los recursos tecnológicos del distrito. El uso de los recursos tecnológicos del distrito puede ser monitorizado por el distrito sin aviso para determinar el cumplimiento de la política y las normas de seguridad en internet y uso apropiado. A través de dicho proceso de monitorización, el distrito puede involuntariamente obtener información de acceso a la cuenta personal de internet de un estudiante mediante el uso de un dispositivo electrónico o programa que monitoriza la red del distrito, o mediante un dispositivo de comunicaciones electrónicas provisto o pagado parcial o íntegramente por el distrito. Si el distrito consigue dicha información personal de acceso al internet, el distrito no utilizará esa información de acceso para acceder a la cuenta personal de internet de un estudiante, salvo en caso permitido por la ley. El mantenimiento y la monitorización rutinaria de los recursos tecnológicos del distrito también puede llevar al descubrimiento

de la violación de la política, normas o leyes del distrito por el usuario. Se llevará a cabo una investigación personal si existe una sospecha razonable de que un usuario ha violado la ley o la política/normas del distrito de seguridad en internet y uso apropiado. Se llevará a cabo una investigación en conformidad con los requisitos legales.

4. El distrito no garantiza de ninguna manera, expresa o implícita, que el funcionamiento de los servicios provistos por o a través de los recursos tecnológicos del distrito sean sin errores ni defectos. El distrito no será responsable por los daños que puedan sufrir los usuarios, incluyendo pero no limitado a la pérdida de datos o interrupciones al servicio. El distrito no es responsable por la precisión ni la calidad de la información adquirida a través del sistema o guardada en ella. El distrito no será responsable por las responsabilidades económicas que puedan surgir por el uso no autorizado de los recursos tecnológicos del distrito.

5. El uso de la tecnología AI en el Distrito Escolar del Área de Verona debe cumplir con la Política de Uso Aceptable (AUP por sus siglas en inglés). La tecnología AI puede ser un recurso para mejorar las experiencias de aprendizaje y enseñanza, pero ha de usarse de manera responsable y ética. Los estudiantes, los maestros y los miembros del personal docente deben garantizar que cualquier sistema de AI que utilicen sea apropiado para las edades de los participantes y que no vulnere la privacidad de otras personas. El uso de AI con fines académicos debe alinearse con el currículo y los objetivos de instrucción del distrito. Además, los estudiantes, maestros y miembros del personal docente deben utilizar las herramientas AI de manera responsable, evitando cualquier forma de plagio o deshonestidad. El incumplimiento de estas directrices puede resultar en acción disciplinaria. Al seguir estas directrices, podemos garantizar que la tecnología AI se utiliza de manera apropiada y segura dentro del Distrito Escolar del Área de Verona.

B. Rol y responsabilidades de los progenitores

1. Después de consultar con el administrador del sitio, y en cumplimiento de las normas que gobiernan la confidencialidad de los registros estudiantiles, los progenitores/tutores pueden solicitar e investigar el contenido de los archivos de uso tecnológico de sus hijos(as).

2. Existe un amplio abanico de materiales disponibles en internet, y quizá no todos encajan con los valores específicos de cada familia. Aunque el distrito utiliza un filtro de internet, no es posible garantizar la protección íntegra del acceso a materiales inapropiados. No es posible que el distrito monitorice ni imponga una amplia gama de valores sociales en el uso estudiantil del internet. Además, el distrito reconoce que los progenitores/tutores son quienes tienen la responsabilidad principal de transmitir sus valores familiares específicos a sus hijos(as). El distrito anima a los progenitores/tutores a que especifiquen a sus hijos(as) qué materiales son y no son aceptables para su acceso mediante los recursos tecnológicos del distrito.

3. De acuerdo a la Política de Uso Aceptable para los estudiantes de VAHS, los progenitores/tutores son responsables por garantizar que monitorizan el uso de su hijo(a) del internet y los recursos tecnológicos durante las horas no lectivas. Esto incluye pero no se limita a los dispositivos estudiantiles, las cuentas de correo electrónico provistas por el

distrito, los espacios de aprendizaje en línea, las herramientas y aplicaciones de colaboración, y los recursos educativos. Los progenitores/tutores deben establecer unas expectativas claras respecto al uso apropiado de los dispositivos electrónicos durante las horas no lectivas. Si su hijo(a) no está cumpliendo esas normas, ustedes tienen derecho a limitar su acceso al dispositivo mientras esté en casa.

C. Normas de uso apropiado

1. Seguridad personal
    a. Los estudiantes no publicarán información de contacto personal sobre sí mismos ni sobre otras personas en internet. La información de contacto personal incluye pero no se limita a su dirección de domicilio y su número de teléfono. Se podrán contemplar excepciones por motivos de investigación de carreras o educación post-preparatoria, o con la aprobación de un instructor.

    b. Los estudiantes no se pondrán de acuerdo para encontrarse con alguien que conocieron en línea sin la aprobación y la participación de sus progenitores/tutores.

    c. Los estudiantes harán saber inmediatamente a su maestro u otro miembro del personal docente presente cualquier comunicación electrónica (por ejemplo, mensajes) que reciban que sean inapropiadas o que les haga sentirse incómodos.

2. Redes sociales
    a. Los recursos de web que enfatizan la colaboración y la participación, como las salas de chat en línea, los wikis, los blogs, los foros y otras herramientas de Web 2.0 se podrán utilizar para propósitos educativos o relacionados con la escuela según lo determine el personal docente o administrativo del distrito. Cualquier otro uso de las redes o recursos sociales por los estudiantes está prohibido.

3. Actividades no autorizadas
    a. Los estudiantes no podrán utilizar los recursos tecnológicos del distrito con fines comerciales, incluyendo pero no limitado a la compra, venta o publicidad de bienes o servicios.

    b. Los estudiantes no intentarán conseguir acceso no autorizado a los recursos tecnológicos del distrito, ni a ningún sistema operativo a través de los recursos tecnológicos del distrito, ni traspasarán su propio acceso autorizado. Esto incluye el intentar iniciar sesión en la cuenta de otra persona o acceder a los archivos de otra persona.

    c. No está permitida la descarga ni la instalación de programas o aplicaciones a los recursos tecnológicos del distrito, incluyendo a los dispositivos móviles pertenecientes al distrito, sin el permiso de un maestro. No está

permitido que los estudiantes suban software personal a los recursos tecnológicos del distrito, incluyendo a los dispositivos móviles pertenecientes al distrito, en ningún caso.

d. Los estudiantes no harán intentos deliberados de interrumpir la operación de los recursos tecnológicos del distrito, ni de destruir datos mediante la difusión deliberada de virus informáticos, ni por ningún otro medio.

e. Los estudiantes no utilizarán los recursos tecnológicos del distrito para involucrarse en ningún acto ilegal ni ningún acto que viole otra política o norma del distrito.

f. Los dispositivos móviles vienen con una imagen estandarizada ya incorporada. Cualquier otra imagen utilizada como fondo de escritorio o de pantalla debe ajustarse a las políticas y normas del distrito. No está permitida la utilización de ninguna imagen inapropiada, incluyendo la presencia de fusiles, armas, material pornográfico, lenguaje inapropiado, alcohol, drogas o símbolos relacionados con las pandillas.

g. Los dispositivos móviles vienen equipados con funciones especiales como la webcam. Las webcam se deben utilizar solamente con fines educativos y bajo la supervisión del maestro. No se permite escuchar música ni ver películas en el dispositivo durante las horas lectivas sin permiso del maestro. Solo se dará permiso para el uso de multimedia para completar proyectos o tareas escolares. Los estudiantes podrán escuchar música o ver películas en los dispositivos móviles pertenecientes al distrito durante las horas no lectivas y fuera del recinto escolar.

h. Los juegos en línea, las descargas y streaming de música, así como las descargas y streaming de videos, no están permitidos en ningún equipamiento del distrito, incluidos los dispositivos móviles pertenecientes al distrito, salvo con permiso del maestro y solamente si la actividad apoya la educación, según determine el personal docente. Los juegos de azar están terminantemente prohibidos.

4. <u>Seguridad del sistema y gestión de datos</u>
   a. Los estudiantes son responsables por el uso de sus cuentas individuales y deben tomar toda precaución razonable para evitar que otras personas puedan utilizar su cuenta personal. Los estudiantes solamente podrán iniciar sesión a su dispositivo móvil asignado o red del distrito con su nombre de usuario asignado. Los estudiantes no podrán compartir su información de acceso ni su contraseña con otros estudiantes o personas. Los estudiantes podrán compartir su información de acceso y contraseña con sus progenitores/tutores.

   b. Los estudiantes notificarán inmediatamente al Coordinador de Tecnología Educativa de su edificio si identifican un posible problema de seguridad.

Los estudiantes no buscarán posibles problemas de seguridad porque esto puede ser interpretado como un intento no autorizado de conseguir acceso, por ejemplo, piratería informática.

c. Todos los estudiantes tendrán acceso a un drive en la red y un drive de Google en la nube donde podrán guardar datos. Es la responsabilidad del estudiante gestionar sus archivos, guardándolos según sea necesario al drive de la red o la nube de Google.

5. <u>El acoso cibernético/Respeto por la privacidad</u>
   a. Los estudiantes no utilizarán lenguaje obsceno, profano, indecente, vulgar, grosero, inflamatorio, amenazante ni irrespetuoso. Las restricciones en cuanto al lenguaje inapropiado se aplican a los mensajes públicos y privados, y los materiales publicados en sitios web.

   b. Los estudiantes no publicarán información que, de utilizarse, ponga en peligro la salud, la seguridad o el bienestar de otras personas.

   c. Los estudiantes no participarán en ataques personales, incluidos pero no limitados a ataques perjudiciales o discriminatorios.

   d. Los estudiantes no acosarán ni harán bullying a otras personas. El “acoso” hace referencia a conducta física o verbal, o abuso psicológico, por cualquier persona que interrumpe o interfiere con el desempeño escolar de un estudiante, o que crea un ambiente de aprendizaje intimidante, hostil u ofensivo. Si un usuario le dice a una persona que deje de enviarle mensajes, debe dejar de hacerlo.

   e. Los estudiantes no participarán del acoso cibernético. El “acoso cibernético” incluye, pero no está limitado a los siguientes mal usos de la tecnología: el acoso, las burlas, la intimidación, las amenazas, o el aterrorizar a otra persona mediante mensajes o publicaciones de mensajes inapropiados y dañinos de correo electrónico, de mensajería instantánea, o de texto, imágenes o fotos digitales, o publicaciones en sitios web que son materialmente o sustancialmente perjudiciales o que violan la política del distrito. En situaciones donde el acoso cibernético originó en una computadora u otro dispositivo de comunicación, como un celular, que no pertenece a la escuela, y que se pone en conocimiento de los oficiales escolares, cualquier acción disciplinaria tomada se basará sobre si la conducta se determina como sustancialmente perjudicial al proceso educativo de manera que interrumpe notablemente o impide de manera substancial las actividades del día a día de la escuela. Además, dicha conducta deberá también constituir una infracción de la política publicada de la escuela. Dicha conducta incluye, pero no se limita al acoso o la formulación de una amenaza fuera del recinto escolar que pretende poner en peligro la salud, la seguridad o la propiedad de otros en la escuela o una actividad escolar dondequiera que se celebre, o hacia un(a) empleado(a) del distrito o un miembro de la Junta Escolar.

f. Los estudiantes no publicarán intencionalmente ni imprudentemente información falsa o difamatoria sobre una persona u organización.

6. El plagio y la violación de los derechos de autor
   a. Los estudiantes no plagiarán. El plagio es tomar de las obras ajenas y presentarlas como propias. Las políticas del distrito respecto al plagió gobernarán el uso del material accedido a través de los recursos tecnológicos del distrito.

   b. Los estudiantes respetarán los derechos de autor. La violación de los derechos de autor sucede cuando una persona reproduce de manera inapropiada una obra protegida por copyright. Si una obra contiene lenguaje que especifica un uso aceptable de dicha obra, el usuario debe obedecer las estipulaciones expresadas. Si el usuario no está seguro si puede utilizar una obra, deberá pedir permiso del dueño del copyright y citarla apropiadamente. Las políticas del distrito respecto a los derechos de autor gobiernan el uso del material accedido a través de los recursos tecnológicos del distrito.

7. Acceso inapropiado a materiales
   a. Los estudiantes no utilizarán los recursos tecnológicos del distrito para acceder a o visualizar material profano u obsceno (por ejemplo, la pornografía), que defiende actos ilegales o que defiende la violencia o discriminación hacia otras personas (literatura del odio).

   b. Si un estudiante involuntariamente accede o visualiza tal información, debe inmediatamente avisar de ello de la manera indicada por su maestro. Esto protege a los usuarios ante una acusación de haber violado intencionalmente la política y las normas del distrito.

   c. Si un estudiante recibe material inapropiado mediante comunicación electrónica (por ejemplo, correo electrónico), debe notificar al remitente de que dicho material está prohibido, y borrar el material. Si el remitente continúa enviando dicho material, el estudiante debe notificar a su maestro o el administrador del sitio.

D. Las computadoras portátiles de propiedad personal y otros dispositivos informáticos o de comunicación

1. Una computadora portátil o de mano de propiedad personal, o cualquier otro dispositivo informático o de comunicación se puede conectar al internet en la escuela solamente mediante la red inalámbrica pública del distrito, que permite acceso filtrado solo a la web en internet. Conectar una computadora portátil u otro dispositivo a un dispositivo fuera de la red se permitirá con fines instructivos.

2. La computadora portátil/de mano o cualquier otro dispositivo informático o de

comunicación se debe utilizar de acuerdo a las políticas y normas del distrito, incluyendo pero no limitado a aquellas aplicables a la seguridad en internet y el uso apropiado de los recursos tecnológicos del distrito. Cualquier infracción de dichas políticas o normas puede resultar en la exclusión del dispositivo de la escuela y/o medidas disciplinarias impuestas a la persona que cometió la infracción.

3. Cualquier estudiante que traiga una computadora portátil/de mano o cualquier otro dispositivo informático a la escuela deberá utilizarlo como herramienta de aprendizaje y solo para el currículo escolar. No puede ser utilizado como sistema de entretenimiento. Los estudiantes deberán apagar y guardar una computadora portátil/de mano o cualquier otro dispositivo informático de propiedad personal cuando así se lo indique un miembro del personal docente.

4. Los dispositivos de propiedad personal no podrán acceder a las impresoras ni copiadoras del distrito.

5. Si se encuentra o se confisca un dispositivo tecnológico de propiedad personal (por ejemplo, un celular), la persona que recupera el dispositivo no está autorizada para ver el contenido de dicho dispositivo. El protocolo del distrito requiere que el personal docente coloque el dispositivo en un lugar seguro, lo etiquete con la hora/fecha y lo entregue en la oficina. El personal administrativo del distrito o agente y/o representante del orden público son los únicos autorizados para ver el contenido, y cualquier investigación o repaso del contenido del dispositivo deberá ser consistente con los requisitos legales.

6. El distrito podrá examinar las computadoras de propiedad personal y otros dispositivos de comunicación, e investigar su contenido, si existe una razón para creer que han sido violadas las políticas, normas, regulaciones o leyes escolares. El alcance de la investigación estará limitado a la violación de la que se acusa al estudiante, y la investigación se llevará a cabo en conformidad con los requisitos legales. Las personas no tienen derecho a expectativas de privacidad en el uso de la red inalámbrica o los sistemas tecnológicos del distrito, y dicho uso está sujeto a la monitorización.

7. No se requiere que los estudiantes traigan computadoras portátiles ni ningún otro dispositivo de comunicación de propiedad personal a la escuela. El distrito rechaza cualquier responsabilidad por la pérdida, robo o daño de la propiedad personal traída a la escuela por los estudiantes. Cualquier computadora portátil/de mano, o cualquier dispositivo de comunicación es responsabilidad del estudiante que lo trajo a la escuela.

E. Infracciones de política y normas

1. El distrito cooperará plenamente con los oficiales locales, estatales o federales en cualquier investigación que concierne o esté relacionada con cualquier actividad ilegal llevada a cabo mediante los recursos tecnológicas del distrito.

2. En el caso de existir una alegación de infracción por un estudiante de la política y/o normas del distrito de seguridad en internet y uso apropiado, el personal investigará y se reunirá con las personas indicadas. El estudiante recibirá la oportunidad de ser escuchado

de la manera estipulada por los códigos disciplinarios del edificio. Las medidas disciplinarias están diseñadas para abordar temas específicos relacionados con la infracción y asistir al estudiante en alcanzar la disciplina propia necesaria para conducirse apropiadamente en una red electrónica. Las consecuencias de las infracciones de la política y las normas de seguridad en internet y uso aceptable incluyen pero no se limitan a las siguientes:

- Suspensión de privilegios del uso de la red
- Revocación de privilegios del uso de la red
- Suspensión de privilegios del uso de internet
- Revocación de privilegios del uso de internet
- Suspensión y/o expulsión escolar
- Acción legal y enjuiciamiento por las autoridades
- Otras acciones disciplinarias