

LPPS Acceptable Use Guidelines for Digital Resources

In compliance with the Children's Internet Protection Act (CIPA) and our commitment to safe, responsible, and productive technology use, our district has adopted policies to protect students and promote a positive digital environment. These policies, including IFBGA Computer Access and Use, JCDAF Bullying, Cyberbullying, and Intimidation, along with others, are available for review at each school and district administrative office.

Guidelines for Acceptable Use of Internet and Digital Resources

Our district strives to foster digital citizenship and support a safe, productive environment in today's digital landscape. Responsible use of technology includes the following guidelines:

1. Protection from Inappropriate Content

Access to inappropriate material is restricted to protect all users.

2. Restricted Communication Platforms

Unauthorized use of personal email, direct messaging, external chat services, or social media by students is prohibited to maintain safety and focus on learning.

3. Positive Digital Behavior

Any form of cyberbullying, harassment, or intimidation is strictly prohibited.

4. Personal Privacy

Students and staff should not share personal or sensitive information online.

5. Responsible Use of Artificial Intelligence (AI)

AI tools can enhance learning and productivity but must be used ethically. Misuse, including using AI to cheat, plagiarize, or access unauthorized resources, is prohibited. All work must reflect the student's understanding and effort, and AI tools should support—not replace—learning.

6. Digital Literacy and Productivity

Users are encouraged to utilize digital tools for productivity, organization, and collaboration in ways that enhance learning and creativity. All tools should be used with respect for copyright and intellectual property rights.

7. Prohibited Activities

The following activities are considered inappropriate and are not allowed:

- Hacking & Unauthorized Access: Tampering with systems, attempting unauthorized access, or any form of unauthorized system penetration is strictly prohibited.
- Password Security: Users must not share passwords or attempt to bypass security measures.
- Respectful Communication: In all forms of digital communication, language should remain respectful and appropriate.
- Privacy of Files: Accessing or modifying others' files, folders, cloud storage, email addresses or data without permission is forbidden.
- Respecting Digital Tools and Equipment: Users must not damage or tamper with district hardware, software, or network resources.
- Bypassing Security Measures: Use of tools such as Virtual Private Networks (VPNs) or other circumvention software to bypass district security settings, firewalls, or content filters is strictly prohibited.
- Copyright and Legal Compliance: All users must respect copyright laws, avoiding unauthorized distribution of content.
- Restricted Social Networking and Chat Room Interactions: Use of personal social media, online forums, or chat rooms is prohibited without district permission.
- Virus and Malware Protection: Users must not knowingly spread viruses or malicious software.
- Restricted Use for Personal, Commercial, or Violent Purposes: District resources, network, and district accounts must not be used for personal financial gain, commercial purposes, or any form of violent or illegal activity.

- **Mobile Devices:** Louisiana State Law, Senate Bill 207 (2024) prohibits the use of cellphones. “no students shall possess, on his person, an electronic telecommunication device throughout the instructional day. If a student brings an electronic telecommunication device in any public elementary or secondary school building or on the grounds thereof during an instructional day, the electronic device shall either be turned off and properly stowed away for the duration of the instructional day or prohibited from being turned on and used during the instructional day.”
- **Student Use of Devices:** Users must not use devices to record, transmit, or post images, sound, or video of people unless authorized by teachers or administrators. Student devices with cameras and video capability shall not be used to infringe upon the privacy of others.

Consequences for Policy Violations

Any violations of these guidelines, applicable state and federal laws, or district policies may result in loss of network privileges, disciplinary action, and legal action/criminal prosecution.

Implementation and Enforcement

To ensure compliance and protect our students, the following procedures are in place:

1. Staff Training

LPPS will review CIPA and Acceptable Use policies with staff. Staff members will sign an acknowledgment form to confirm their understanding and acceptance of these responsibilities.

2. Student Education

Teachers will review Acceptable Use guidelines with students. Students in grade 3 and above are required to sign a statement acknowledging their understanding and commitment to responsible digital use.

3. Content Filtering and Monitoring

The district employs advanced filtering software to block inappropriate content. Monitoring systems help ensure safe use, and district staff review reports regularly to maintain compliance.

4. Digital Privacy and Parental Consent

Parents give permission for the use of approved digital tools and curriculum unless specific request to deny through the school is made. All student photos on school websites will be unidentified unless parental permission is granted. Parents may also opt to:

- Deny their child internet access.
- Deny permission for their child's work to be published on school websites.
- Deny permission for their child's unidentified photos to appear on school websites.

These guidelines uphold our commitment to a safe, productive, and ethical digital environment where students learn to navigate technology responsibly.

For access to the full version of LPPS Policy IFBGA: Student Computer Access and Use, visit bit.ly/IFBGA
LPPS Internet Safety, Digital Citizenship, and Cybersecurity information can be found at bit.ly/LPPSsafety

Directrices de uso aceptable de LPPS para recursos digitales

En cumplimiento con la Ley de Protección de Internet para Niños (CIPA) y nuestro compromiso con el uso seguro, responsable y productivo de la tecnología, nuestro distrito ha adoptado políticas para proteger a los estudiantes y promover un entorno digital positivo. Estas políticas, incluyendo Acceso y Uso de Ordenadores de la IFBGA, Acoso Escolar, Ciberacoso y Intimidación de JCDAF, entre otras, están disponibles para su revisión en cada oficina administrativa escolar y distrital.

Directrices para el uso aceptable de Internet y recursos digitales

Nuestro distrito se esfuerza por fomentar la ciudadanía digital y apoyar un entorno seguro y productivo en el entorno digital actual. El uso responsable de la tecnología incluye las siguientes directrices:

1. Protección frente a contenido inapropiado

El acceso a material inapropiado está restringido para proteger a todos los usuarios.

2. Plataformas de comunicación restringida

El uso no autorizado de correo electrónico personal, mensajería directa, servicios de chat externos o redes sociales por parte de los estudiantes está prohibido para mantener la seguridad y centrarse en el aprendizaje.

3. Comportamiento digital positivo

Cualquier forma de ciberacoso, acoso o intimidación está estrictamente prohibida.

4. Privacidad personal

Los estudiantes y el personal no deben compartir información personal o sensible en línea.

5. Uso responsable de la inteligencia artificial (IA)

Las herramientas de IA pueden mejorar el aprendizaje y la productividad, pero deben usarse éticamente. El uso indebido, incluido el uso de IA para engañar, plagiar o acceder a recursos no autorizados, está prohibido. Todo el trabajo debe reflejar la comprensión y el esfuerzo del estudiante, y las herramientas de IA deben apoyar, no reemplazar, el aprendizaje.

6. Alfabetización digital y productividad

Se anima a los usuarios a utilizar herramientas digitales para la productividad, la organización y la colaboración de formas que mejoren el aprendizaje y la creatividad. Todas las herramientas deben utilizarse respetando los derechos de autor y propiedad intelectual.

7. Actividades prohibidas

Las siguientes actividades se consideran inapropiadas y no están permitidas:

- Hackeo y acceso no autorizado: Está estrictamente prohibido manipular sistemas, intentar acceder sin autorización o cualquier forma de penetración no autorizada.
- Seguridad de contraseñas: Los usuarios no deben compartir contraseñas ni intentar eludir las medidas de seguridad.
- Comunicación respetuosa: En todas las formas de comunicación digital, el lenguaje debe seguir siendo respetuoso y apropiado.
- Privacidad de los archivos: Está prohibido acceder o modificar archivos, carpetas, almacenamiento en la nube, direcciones de correo electrónico o datos de terceros sin permiso.
- Respeto a las herramientas y equipos digitales: Los usuarios no deben dañar ni manipular el hardware, software o recursos de red del distrito.
- Eludir medidas de seguridad: Está estrictamente prohibido el uso de herramientas como Redes Privadas Virtuales (VPN) u otros programas de elusión para eludir configuraciones de seguridad de distritos, cortafuegos o filtros de contenido.
- Derechos de autor y cumplimiento legal: Todos los usuarios deben respetar las leyes de derechos de autor, evitando la distribución no autorizada de contenido.
- Interacciones restringidas en redes sociales y salas de chat: Está prohibido el uso de redes sociales personales, foros en línea o salas de chat sin permiso del distrito.
- Protección contra virus y malware: Los usuarios no deben propagar virus ni software malicioso a sabiendas.

- **Uso restringido con fines personales, comerciales o violentos:** Los recursos, redes y cuentas del distrito no deben utilizarse para beneficio financiero personal, fines comerciales ni ninguna forma de actividad violenta o ilegal.
- **Dispositivos móviles:** La ley estatal de Luisiana, el Proyecto de Ley del Senado 207 (2024) prohíbe el uso de teléfonos móviles. "Ningún alumno deberá poseer, consigo, un dispositivo electrónico de telecomunicaciones durante toda la jornada de instrucción. Si un estudiante lleva un dispositivo electrónico de telecomunicaciones a cualquier edificio público de primaria o secundaria o en sus terrenos durante una jornada de instrucción, el dispositivo electrónico deberá ser apagado y guardado adecuadamente durante la jornada de instrucción o prohibido de ser encendido y utilizado durante la jornada de instrucción."
- **Uso de dispositivos por parte de los estudiantes:** Los usuarios no deben utilizar dispositivos para grabar, transmitir o publicar imágenes, sonido o vídeo de personas a menos que estén autorizados por profesores o administradores. Los dispositivos de los estudiantes con cámaras y capacidad de vídeo no deben ser utilizados para vulnerar la privacidad de otros.

Consecuencias por infracciones de políticas

Cualquier infracción de estas directrices, de las leyes estatales y federales aplicables o de las políticas del distrito puede suponer la pérdida de privilegios de red, medidas disciplinarias y acciones legales o procesos penales.

Implementación y aplicación

Para garantizar el cumplimiento y proteger a nuestros estudiantes, existen los siguientes procedimientos:

1. Formación del personal

LPPS revisará las políticas de CIPA y Uso Aceptable con el personal. Los miembros del personal firmarán un formulario de reconocimiento para confirmar su comprensión y aceptación de estas responsabilidades.

2. Educación del alumnado

Los profesores revisarán las directrices de Uso Aceptable con los alumnos. Los estudiantes de 3º curso en adelante deben firmar una declaración reconociendo su comprensión y compromiso con un uso digital responsable.

3. Filtrado y monitorización de contenidos

El distrito emplea software avanzado de filtrado para bloquear contenido inapropiado. Los sistemas de monitorización ayudan a garantizar un uso seguro, y el personal del distrito revisa los informes regularmente para mantener el cumplimiento.

4. Privacidad digital y consentimiento parental

Los padres dan permiso para el uso de herramientas digitales y currículos aprobados, salvo que se solicite específicamente la denegación a través del colegio. Todas las fotos de los estudiantes en las páginas web del colegio permanecerán sin identificar a menos que se conceda el permiso de los padres. Los padres también pueden optar por:

- Negar el acceso a internet a su hijo.
- Negar el permiso para que el trabajo de su hijo se publique en las páginas web de las escuelas.
- Negar el permiso para que las fotos no identificadas de su hijo aparezcan en las páginas web de los colegios.

Estas directrices respaldan nuestro compromiso con un entorno digital seguro, productivo y ético donde los estudiantes aprendan a navegar la tecnología de forma responsable.

Para acceder a la versión completa de la Política LPPS IFBGA: Acceso y Uso de Ordenadores para Estudiantes, visite bit.ly/IFBGA
La información sobre seguridad en Internet, Ciudadanía Digital y Ciberseguridad de LPPS puede encontrarse en bit.ly/LPPSsafety