Deweyville Independent School District
Code of Responsible Computing and Use of Technology

DISD Responsible Use Policy

Deweyville Independent School District DISD provides access to the Internet and the District's electronic communications systems for users, for educational purposes.

Access will be used to enhance learning consistent with the District's educational goals.

The District's computer systems and networks (system) are any configuration of hardware and software. The electronic communications system includes but is not limited to the following:

• Telephones, cellular telephones, and voicemail technologies;
• Email accounts;
• Servers and network equipment;
• Computer hardware (including mobile devices, tablets, i-devices) and peripherals;
• Software including operating system software and application software;
• Digitized information including stored text, data files, email, digital images, video and audio files;
• Internally or externally accessed databases, applications, or tools (Online/Internet – or District server based);
• District-provided filtered Internet access;
• District-provided filtered guest and Wi-Fi; and
• New technologies as they become available.

These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have serious consequences, harming the District, its users and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm.

For the District to be able to continue to make its network and Internet access available, all users must take responsibility for appropriate and lawful use of this access. Users must understand that one person's misuse of the District technology hardware or software, network and/or Internet access may jeopardize the ability of all to enjoy this access. While the District's management and network administrators will make reasonable efforts to administer use of the network and Internet access, they must have user cooperation in exercising and promoting responsible use of this access.

Access to the District's electronic communications systems is a privilege, not a right.

Administrators and faculty may review files and messages to maintain system integrity, to ensure that users are acting responsibly. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing the use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines.

To educate users on proper computer/network/Internet use and conduct, users are required to review these guidelines at the beginning of each school year. Employees supervising users who use the District's system must provide instruction and oversight, emphasizing its appropriate use.

Access to the District's electronic communication system, including the Internet, shall be made available to staff and users for instructional purposes. Each District computer and guest Wi-Fi has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for users, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to users as defined by CIPA.

However, while the District uses filtering technology and protection measures to restrict access to inappropriate material; it is not possible to absolutely prevent such access.

It is each user's responsibility to follow the rules of appropriate and responsible use.

Users may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and online meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. These tools should not be considered a private, personal form of communication. Their use should be restricted to school/curriculum-related activities at all times.

All users should assure that they do not share personally identifiable information online. Verbal or written language considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.

Electronic communication is an important skill for 21st Century Users. By providing this tool, the District is equipping users with the skills necessary for success in the business world or academic endeavors. Users in grades 3-12 may be given access to a District user email account. Parents wishing to deny access to District email must do so in writing to the campus principal.

A user or staff member who gains access to any inappropriate or harmful material is expected to discontinue access and to report the incident to the supervising staff member.

Any user identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Staff, users, and parents of users with access to the District's systems should be aware that use of the systems may inadvertently provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material, regardless of protections and filters in place.

Appropriate Use:

• If you are assigned an individual account for hardware and Internet access, you are responsible for not sharing the password with others.

• You are responsible for any activity that occurs under the use of your account login. If you leave your device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, you may be held responsible for that activity.

• You may not give your login information to another user.

• You will be held responsible at all times for the proper use of District technology resources, and the District may suspend or revoke your access if you violate the rules.

• Your account is to be used primarily for educational purposes.

Inappropriate Use:

• Includes, but is not limited to, those uses that violate the law, that are specifically named as violations in policy, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it.

• Transmission of any material in violation of any federal or state law is prohibited. This includes but is not limited to:

- Threatening, harassing, defamatory or obscene material;
- Copyrighted material;
- Plagiarized material;
- E-mail, social media, or discussion forum postings to the Internet or other systems, which violate federal or state law.

• Using cameras or audio/video recorders in private places where a person may reasonably expect to be safe from unauthorized surveillance, such as locker rooms or restrooms. Do not distribute, transfer, or share audio, images, or video that reveal private parts of the body that are ordinarily covered by clothing. The possession of pornographic images or video on an electronic device is prohibited.

• Using your device to record the voice or image of another in any way that disrupts the educational environment, invades the privacy of others, or is made without the prior consent of the individuals being recorded. All of the above apply to all school activities during or after regular school hours.

• Modifying or changing computer settings, electronic system resources, and/or Internal or external configurations without appropriate permission is prohibited.

Any malicious attempt to harm or destroy District equipment, materials or data, or the malicious attempt to harm or destroy data of another user on the District's system, or any of the agencies or other networks to which the District has access, is prohibited.

Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws.

Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

• Users must respect others' right to privacy.

• Users may not redistribute, forward, or share confidential information without proper authorization.

• Users must not transmit, redistribute, or forward to outside individuals not expressly authorized to receive the information.

• Users must not send messages, post documents, or participate in educational activities using a false identity, or use the accounts of others.

• Users will not access files, folders, or other electronic data of others without permission.

• Users will not use the Internet for financial gain, commercial activity, or political activity.

• Users will not use electronic resources to purchase products or services.

• Users will not redistribute copyrighted programs or data without the written permission of the copyright holder.

• Users will not engage in Cyberbullying. Cyberbullying includes but is not limited to, harassing, disrespecting, impersonating, tricking, and cyber stalking.

• Users will not reveal personal information about themselves or others such as, home addresses, phone numbers, email addresses, or birthdates.

• Users should not respond to requests for personally identifying information or contact from unknown individuals.

• Users should not meet in person with people met online. If a request for such a meeting is received, it should be reported to a teacher or administrator immediately.

• Users will use appropriate language for the educational environment and for the educational activity in which they are currently involved.

• Users will be held responsible at all times for the proper use of District technology resources, and the District may suspend or revoke your access if you violate the rules.

• Users will not access the control panel on a district computer or attempt to modify settings in any way.

• Users will not access Proxy/VPN server websites that are designed for, intended to, or by chance scan our network, or attempt in any way to circumvent our security.

• Users will not open, send, or receive obscene pictures or messages.

• Users will not upload any personal media files to any shared network folder, device, and/or the network that are not for educational purposes.

• Users will not use technology resources for any non-instructional or inappropriate purpose. (Examples include: online gaming, social media, chat, blogs, etc.)

• Users will not install any software, viruses, or games on any district computer or system connected to district networks without permission from the teacher.

• Users will not log into a computer for another user whose access has been suspended.

• Users will not waste district resources through improper use of the system. (Examples include: printing personal material, attaching personal devices without approval, etc.)

• Users will not remove equipment from the District without written permission.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the user's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

District users are bound by all portions of the Responsible Use Guidelines. A user who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved User Code of Conduct.

With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Disclaimer
The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Acknowledgement form.

Users: Please print the user's legal name (first, middle, and last) in the space provided below:

First Name: _____

Middle Name: _____

Last Name: _____

Please have the user sign in the space provided below:

User's Signature: _____

Please print user's grade level: (K-12) in the space provided: _____

Parents:
I understand the importance of the technology rules and will support the User Code of Responsible Computing and Use of Technology. Parents or guardians of users guilty of damaging property will be liable for damages in accordance with the law.

Each user authorized to access the District computers, networks, telecommunications, Internet services, or other resources is required to sign a Responsible Use Guidelines Acknowledgement form.

I understand that Computer/Network/Internet access is provided to all users unless parents or guardians request in writing to the campus principal that access be denied.

Parent's Signature: _____

Date: _____

Computer / Electronic Device - Student Responsible Use Rules

- Limit use to assigned classroom / educational purposes only.

- Do not install any software, apps, games, scripts, extensions or anything else..

- Do not access the control panel on a district computer or attempt to modify settings in any way.

- Do not access Proxy/VPN server websites that are designed for, intended to, or by chance scan our network, or attempt in any way to circumvent our security.

- Do not log into a computer for another user whose access has been suspended.

- Do not move, remove, or replace any devices or equipment.

- Do not abuse or destroy any devices or equipment. Handle all technology with care.

Students will be held responsible at all times for the proper use of technology resources, and the district may suspend or revoke your access if you violate any of these rules.