

Technology and Internet Acceptable Use Policy for Students**General Information**

District #145 recognizes that telecommunications and other new technologies change the way information may be accessed, communicated and transferred by members of society, and that these changes may alter instruction and student learning. The school supports access to information resources, including the development of appropriate skills to analyze, properly use, and evaluate such resources.

Because telecommunications have the potential to lead to any public file server in the world it can open classrooms to electronic information, which may not have been screened by District #145 staff. The staff is expected to follow guidelines for the selection of materials that are to be presented to students. Regardless, a plethora of material is available and it would be impossible to constantly screen all District traffic in its entirety. Thus, on a global network, it is impossible to control all materials, and an industrious user may discover controversial information.

District #145 firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may acquire material not consistent with the educational goals of the District. However, District #145 also believes that students and staff have a personal responsibility to abide by the following terms and conditions, which are consistent with District goals.

While computers are in the District, networks are provided for students to conduct research and access valuable educational information, such access will be provided to students who act in a considerate and responsible manner. General school policies for behavior and communications apply to all computer use and users. Students are responsible for all communications that take place when they are using school equipment whether individually, in a group, or if the equipment is off school grounds. Students are also responsible for the equipment they use whether on or off school grounds.

Acceptable Use Policy Violations

A complex association of government agencies and regional and state networks provide Internet access in public schools. The operation of this network is dependent upon proper conduct of end users and strict guidelines. By logging onto the District #145 network, the end user accepts these guidelines and responsibilities listed in the Terms and Conditions of School District #145 policies. Improper use of the District technology system could result in termination of a users account, network access, and disciplinary action from Administration such as expulsion from school or suspension. In certain cases, the proper civil authorities might also be required to resolve issues of misuse. In these cases, District Administrators and the intervening authority office will handle the proper actions of authority.

Terms and Conditions**Please read carefully through the following terms and conditions:**

Privileges – The use of the Internet, e-mail and any District computer is a privilege, not a right. Inappropriate use will result in a cancellation of said privileges. Student e-mail can be accessed at any time by administrators or the technology director has a concern. Computers that are property of School District #145 may be searched at any time. Additionally, Administrators and the District Technical Director reserve the right to search any technological devices on District property. District technology should be used for educational purposes only.

Security – Users should not expect that files stored on District servers, or any type of District storage equipment will be private. Network storage is school property and school administrators and the Technology Director reserve the right to search any data stored on school property. These authorized school personnel may review files, communications, and any e-mail to maintain system integrity, insure school security, and insure that users are utilizing the system responsibly and accordingly to policies.

Security is an essential part of technology and the District technology staff takes measures of security seriously. If a user believes they can identify a security problem on the network, they must notify a District technology staff member or the Technology Director. Do not demonstrate the problem to other users.

User Accounts – Each user in the District is allotted a specific amount of storage space on the District servers. The space size is subject to change without notice. There are many factors that determine the correct amount of space for each user. Users exceeding this limit without any educational reason may have files that are causing issues removed without notice. This discretion is up to District technology staff members and actions can vary upon select cases. The District technology staff follows all District policies and does not discriminate against staff or students.

Users are not to share individual account information, passwords, or privileges with anyone other than District technology staff or Administrators. Users are also prohibited from gaining access to an account that is not in their name, this includes but is not limited to: revealing, or attempting to learn or use other user's passwords, spreading viruses, attempting to "hack" in to restricted systems or attempting to use administrative commands or programs. Each user's actions are tracked and sharing account information could compromise an individual's innocence in certain situations. Sharing accounts could result in loss of privileges for both parties. Any problems that arise from the use of an account are the liability or responsibility of the account holder. All account holders hereby release School District #145 and ESU 6 from any and all claims or damage of any nature arising from their use, access, or inability to access or use computers or the network. School District #145 makes no warranties of any kind for the information or services it provides. All financial responsibilities incurred by a user are not the responsibility of School District #145.

The following actions are prohibited:

- Transmitting or knowingly receive any materials in violation of any United States, Nebraska, or District #145 regulations or laws. This includes, but is not limited to: copyrighted material, threatening, harassing, pornographic, obscene, profane, or hate related material, materials related to the illegal use or manufacture of restricted substances, defamatory or discriminatory material, or material protected by trade secret.
- Commercial activities, product advertising, political lobbying and extensive personal use.
- Conducting personal/business transactions through the network.
- Developing, downloading or activating programs that are not required for educational use or intentionally using these programs to harass other users, infiltrate/gain unauthorized access to any computer system, or alter the software provided on District computers.
- Using inappropriate language or profanity.
- Revealing personal addresses or phone numbers, or those of students or staff without consent. Parental consent is required for minors under the age of 19.
- Sharing account passwords – see “User Accounts”. (If you believe that someone has obtained unauthorized access to your account or any account on the system, please notify the building system Administrator immediately).
- Sending, receiving, or displaying offensive messages or pictures.
- Harassment or insults of any type.
- Engaging in racial, gender, or other slurs.
- Trespassing in other work, folders, or files.
- The use of list serves without teacher or administrative approval.
- Chain letters or using District equipment to plan events that are banned by school policy.
- Using computers and technology for game-playing or trivial applications.
- Inappropriate use of Internet accounts.
- Bypassing or accessing and changing school security features including, but not limited to, content filters, firewalls, user restriction applications, and data access control enforcements.
- Violating U.S. Copyright laws.

Please read and understand the following:

Participating or creating an instance defined below may result in cancellation of privileges and other disciplinary actions according to school policies. School officials will handle violations in accordance with due process proceedings.

Vandalism – Vandalism is defined as any willful or malicious act of destruction or an attempt to harm or destroy any hardware, software, or data belonging to the school or another user. This includes the uploading or creation of computer viruses. Vandalism will result in user paying for repair and/or technician time to restore network/equipment to previous condition, loss of Internet privileges and may be subject to criminal prosecution. Parents and/or guardians are financially responsible for acts of vandalism committed by their children.

Hacking – Hacking is defined as attempting to gain unauthorized access to computer systems. Hackers are dealt with according to school policy, in certain cases the proper authorities will also be contacted if a user has participated in any type of illegal action, including but not limited to items such as identity theft.

Indirect Access – This includes using a non-District computer in a manner that results in the user gaining access to a District computer, and using a District computer to gain access to other systems.

The consequences of unacceptable use are:

- Suspension and/or termination of electronic resource use privileges.
- And/or additional disciplinary action as determined at the building level in line with existing practice regarding unacceptable language and/or behavior.
- And/or financial remuneration for lost time and for damaged equipment.
- And/or referral to law enforcement authorities for criminal or civil prosecution.

Internet Protection Measures

School District #145 uses content filtering and protection measures, which blocks and/or filters Internet access to prevent access to certain Internet sites that are not in accordance with the policies of the District.

- The filtering measures that blocks or filters Internet access may be disabled by an authorized staff member for bona fide research purposes or for specific sites if recommended by District Administration or approved by a District technology staff member.
- An authorized District technology staff member may override these protection measures to provide access to a site for research or other lawful purposes, during which time the minor will be monitored directly by the authorized staff member or his/her designee.

These measures have been put in place and required by federal law. Any issues with the content filtering systems of School District #145 need to be brought up with the District Technology Coordinator or Superintendent. These filtering systems are not guaranteed to filter all content that is not in line with the policies and educational goals of School District #145, therefore all Internet use is at the liability of the user.

The following categories of sites are filtered or blocked by School District #145 in accordance to the CIPA (Children's Internet Protection Act) enacted in December 2000.

- **Crime:** Sites providing instructions on performing criminal activities or acquiring illegal items, including defeating security, disabling, or otherwise interfering with computer systems (hacking or cracking); unauthorized use of telephone or communications equipment to place free calls or charge another's account for calls; deactivating copy protection or registration schemes of software or hardware systems (pirating and warez); construction and usage of munitions such as pipe bombs, letter bombs, and land mines; and lock picking, spying, or general subterfuge and defeating of security measures.
- **Drugs/Advocacy:** Sites advocating the legal use of illegal drugs for medical and personal use.
- **Drugs/Non-Medical:** Sites providing information on growth, distribution, and advocacy of drugs for non-medical use (typically mood altering), including alcohol and tobacco products.
- **Entertainment/Games:** Sites dedicated to games, gaming, game tips, game downloads, interactive games, and multi-player games.
- **Entertainment/Sports:** Sites dedicated to professional and amateur sports and sporting events.
- **Finance:** Sites dedicated to personal finance, banking, stock trading, and wealth accumulation.
- **Gambling:** Sites dedicated to promotion of or participation in wagering, gambling, casinos, or lotteries.
- **Interactive/Chat:** Sites providing interactive communication services, such as Web chat, bulletin boards, and IRC.
- **Interactive/Mail:** Sites providing interactive electronic-mail services.
- **Intolerance:** Sites advocating intolerance or hatred of a person or group of people.
- **Any websites that are sexually explicit in nature that includes but are not limited to the topics of:** Acts, Attire, Nudity, Personals, Sex Ed/Basic, Sex Ed/Advanced, or Sex Ed/Sexuality.
- **Violence:** Sites depicting or advocating violence, including sites promoting violent terrorist acts against others that do not fall under the Intolerance category.

- Weapons: Sites that display, sell, or advocate the use of weapons, including guns, knives, and martial arts weaponry.

Objections to Internet Protection Policies

An individual who has been granted access to the Internet by School District #145 and desires to access an Internet site that is not compliant with this policy may challenge the enforcement of the policy according to the following procedures.

- Internet site review requests should be directed to a member of the District technology staff in writing or e-mail for consideration. If that member determines that the site has educational purpose, they shall have the authority to unblock or change the filter of that site. If the staff member is unsure as to the educational validity of the site, then it shall be referred to the Technology Coordinator.
- The Technology Coordinator will review the site within seven working days of submission of the request and, if deemed appropriate for educational or work-related purposes, will unblock the site.
- Challenges to the application or enforcement of School District #145 Internet Safety Policy that cannot be resolved at the levels outlined in the preceding steps will be handled in accordance through the authority of School District #145 Administrator and/or at the board level for challenges presented in writing.

Policy Adopted: 04/07/97
Policy Revised: 08/04/03
Policy Revised: 03/04/09

SCHOOL DISTRICT 145
WAVERLY, NEBRASKA