

Evergreen School District
Technology Code of Conduct

Use of the network, which includes the local Evergreen School District computer network as well as the Internet, shall be in support of education and research that is consistent with the mission of the District.

Internet use is limited to those staff members who have completed the appropriate agreement form, and students whose parent or guardian has not submitted a "Refusal of Student Internet Access" on behalf of their student.

1. Use of the network in such a way that it does not disrupt its use by others.
2. Maintain the integrity of files and data. Modifying or copying files/data of other users without their consent is not permitted.
3. Be ethical and courteous. Defamatory, harassing, or obscene mail or discriminatory remarks are not allowed on the network.
4. Treat information created by others as the private property of the creator. Respect copyrights.
5. Personal information, such as complete names, addresses, telephone numbers, and identifiable photos, should remain confidential when communicating on the District network.
6. No user, staff or student, may disclose, use, or disseminate personal identification information regarding minors without authorization.
7. Use the technology to access only appropriate material.
8. Students will notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant Message services).
9. Students should never make appointments to meet people in person whom they have contacted on the system without District and parent permission.
10. Protect your passwords from others.
11. Computer hardware or software should not be destroyed, modified, or abused in any way.
12. "Hacking" the system is not permitted.
13. The network is not to be used for commercial purposes.
14. Respect the privacy of others. Use only your password.

The District reserves the right to remove a user's account if it is determined that the user is engaged in unauthorized activity or is violating this code of conduct.

Technology, Network, and Internet Acceptable Use Guidelines

(Adopted from the K-20 Network Acceptable Use Agreement)

COMPUTER and/or THIN CLIENT

1. The use of District computers and/or Thin Clients is for District work only. Users will not download any software for personal use. Software for Department/School/District use or testing will be loaded on computers only by District CIR (Communications & Information Resources) or ET (Educational Technology) staff, or their designated vendor(s).
2. Only CIR or ET staff, or their designated vendor(s), are authorized to evaluate or perform maintenance/work on District computing/technology equipment.

NETWORK

1. All use of the system must be in support of education and research and be consistent with the mission of the District. The District reserves the right to prioritize use and access to the system.
2. Any use of the system must be in conformity to state and federal law, network provider policies and licenses and District policy. Use of the system for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designee.
3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.
5. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
6. Users are responsible for the appropriateness and content of material they store, transmit, or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.

SECURITY

1. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Individual account owners are ultimately responsible for all activity under their account.
2. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to any systems on the Evergreen network or outside the Evergreen network.
3. Communications may not be encrypted so as to avoid security review.
4. Users should change passwords regularly and avoid easily guessed passwords.

STUDENT SECURITY RESPONSIBILITIES

Note: This information is being provided on the Staff Technology, Network, and Internet Acceptable Use Guidelines for awareness of student responsibilities.

1. Personal information such as complete names, addresses, telephone numbers, and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher

Technology, Network, and Internet Acceptable Use Guidelines

(Adopted from the K-20 Network Acceptable Use Agreement)

and parent or guardian. No user may disclose, use, or disseminate personal identification information regarding minors without authorization.

2. Students should never make appointments to meet people in person whom they have contacted on the system without District and parent permission.
3. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant Message services).

STUDENT AND/OR FISCAL/HR SYSTEMS/TESTING INFORMATION AND/OR MATERIALS/ANY OTHER CONFIDENTIAL INFORMATION

1. Users with access to the WESPaC Student System and/or Fiscal/HR System, or anyone with network/computer access, shall not download any confidential information, including but not limited to fiscal, student, or testing information, to any medium for use outside the District, or for unauthorized use within the District. Vendors needing information must work through CIR in order to obtain any Evergreen staff, student, or other information.
2. All District staff will refer to FERPA guidelines before releasing any student information.

COPYRIGHT

1. The unauthorized installation, use, storage, or distribution of copyrighted software or materials on District computers is prohibited. All users of the District network shall comply with current copyright laws.

GENERAL USE

1. Diligent effort must be made to conserve system resources. For example, users should frequently delete e-mail and unused files, and users should promptly disconnect video conferences upon completion.
2. An Individual *User Informed Consent Form* signed by each staff member, and anyone with District network access, must be on file with the District.
3. A parent or guardian who does not want their student to use the internet at school needs to complete and submit to their student's school a *Refusal of Student Internet Access* form.

Nothing in these regulations is intended to preclude the use of the system in conformity with District policy and procedure.

From time to time, the District will make a determination on whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the District. For security and administrative purposes the District reserves the right for authorized personnel to review system use and file content. The District reserves the right to remove a user account on the system to prevent further unauthorized activity. The District's wide-area network provider (Washington K-20 network) reserves the right to disconnect the District to prevent unauthorized activity.

Violation of any of the conditions of use may be cause for disciplinary action.