

DEVICE USER AGREEMENT

STUDENT ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE DEVICE NETWORK OF

Four County Career Center

Four County Career Center is pleased to make available to students access to network systems within the District and to the Internet, the world-wide network that provides various means of accessing significant educational materials and opportunities. For specific information regarding Bring Your Own Device (BYOD) or 1:1 information, please refer to the student 1:1/BYOD Handbook.

In order for the School District to be able to continue to make its network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the School's teachers and other Staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("Policy") of the School District and the Data Acquisition Site that provides Internet access to the School District. Upon reviewing, signing, and returning this Policy as the students have been directed, each student will be given the opportunity to enjoy Internet access at School and is agreeing to follow the Policy. If a student is under 18 years of age, he or she must have his or her parents or guardians read and sign the Policy. The School District cannot provide access to any student who, if 18 or older, fails to sign and submit the Policy to the School as directed or, if under 18, does not return the Policy as directed with the signatures of the student and his/her parents or guardians.

Listed below are the provisions of your agreement regarding the network and Internet usage. If you have any questions about these provisions, you should contact the person that your School has designated as the one to whom you can direct your questions. If any user violates this Policy, the student's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing this Policy, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the person designated by the School for such reporting. Misuse means any violations of this Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

II. TERM OF THE PERMITTED USE

A student who submits to the School, as directed, a properly signed Policy and follows the Policy to which she or he has agreed will have network and Internet access during the course of the school year only. Students will be asked to sign a new Policy each year during which they are students in the School District before they are given an access account.

III. ACCEPTABLE USES

- A. **Educational Purposes Only.** The School District is providing access to its network and the Internet for *only* educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the School to help you decide if a use is appropriate.
- B. **Unacceptable Uses of Network.** Among the uses that are considered unacceptable and which constitute a violation of this Policy are the following:
1. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the School District's Student Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or devices of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
 2. Uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participate in

- “hacking” activities or any form of unauthorized access to other devices, networks, or information systems.
3. Uses that jeopardize the security of student access and of the network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user; don't connect wireless devices to the network or attempt to intercept wireless communications.
 4. Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

C. Netiquette. All users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
2. Avoid language and uses which may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
3. Don't assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
4. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

IV. INTERNET SAFETY

A. General Warning; Individual Responsibility of Parents and Users. All users and their parents/guardians are advised that access to the network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the network and Internet and stay away from these sites. Parents of minors are the best guide to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.

- B. **Personal Safety.** Be safe. In using the network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the network or Internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.
- C. **“Hacking” and Other Illegal Activities.** It is a violation of this Policy to use the School’s network or the Internet to gain unauthorized access to other devices or device systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
- D. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
- E. **Active Restriction Measures.** The School, either by itself or in combination with the Information Technology Center (ITC) providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that

- taken as a whole and with respect to minors, appeals to a prurient interest in

- nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
 - taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

V. PRIVACY

Network and Internet access is provided as a tool for your education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

VI. FAILURE TO FOLLOW POLICY

The user's use of the network and Internet is a privilege, not a right. A user who violates this Policy, shall at a minimum, have his or her access to the network and Internet terminated, which the School District may refuse to reinstate for the remainder of the student's enrollment in the School District. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the network and Internet, including any user whose access has been denied or terminated. The School District may also take other disciplinary action in such circumstances.

VII. WARRANTIES/INDEMNIFICATION

The School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its network and the Internet provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its network or the Internet under this Policy. By signing this Policy, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the School, the School District, the Data Acquisition Site that provides the Internet access opportunity to the School District and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its network and the Internet, including but

not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the School in the event of the School's initiating an investigation of a user's use of his or her access to its network and the Internet, whether that use is on a School device or on another device outside the School District's network.

VIII. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new Policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardian) or such new Policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the School to receive such information.

Use of Device Technology:

- (1) A student shall not use or modify any device technology (hardware, software, or peripherals, connections etc.) provided by the school without authorization from school authorities - including, but not limited to Facebook, Twitter, SnapChat, Instagram, Facetime, etc. This is to include devices issued to students to assist in the delivery of the curriculum.
- (2) No student shall install, copy, delete, transmit, upload/download or modify in any way files or violate copyright laws or use any software outside the rights granted to him/her (examples: LimeWire, BearShare, BitTorrent, etc.). No student shall have in possession or use destructive/invasive programs e.g. games, pictures, music, and videos. This is to include but not limited to the Internet, software used for class, or software used in the media centers.
- (3) No student shall use device technology in ways which violate the law or violate the rights of others: e.g. viewing, copying files, transmitting, deleting, harassing, threatening, degrading, pornographic, or racist or using others login/password. Any student with knowledge that such material exists on their devices may take their device to the Help Desk and must specifically ask that it be removed. This must be done prior to being discovered by staff in order for students to avoid consequences. Students are not to send mass emails to groups and/or students.
- (4) No student shall attempt to access internal/external networks outside the regular connections, e.g. via filter bypass, stolen passwords, proxy's, use of IP addresses, TELNET, FTP, or any unauthorized means.

- (5) Students shall not use devices and/or other owned equipment to create websites or post pictures/information on any website(s) without school authorization.
- (6) Four County Career Center shall provide appropriate technology for student use and to deliver the curriculum of the school. Network use will be monitored - no student shall have the expectation of privacy for files, hardware, software, peripherals, etc. All 1:1 Chromebook repairs and service (erasing, hardware repair/replacement, damaged equipment evaluation, etc.) are to be performed by only the Help Desk Center.
- (7) It is the student's responsibility to follow directions necessary to establish a confidential password for all technology. Students are not to leave devices unattended while logged onto the Four County Career Center network. Students shall not give their password to anyone else or allow anyone else to log onto their account. No student shall log onto another student's account or device. Students shall not loan or allow others to use their devices.
- (8) No student shall mark, scratch, deface or damage any device. Students shall not put stickers and decals on 1:1 devices.

Damage or Misuse of Property: Consequences may include suspension/expulsion. A legal guardian or student (if emancipated) may be charged for damages to school property to include devices, PC's, equipment, other instructional supplies, facilities, etc.