



## RESPONSIBLE USE AND INTERNET SAFETY POLICY

### FOR USE OF THE COMPUTER AND NETWORK SYSTEMS OF THE BUTLER TECHNOLOGY AND CAREER DEVELOPMENT SCHOOLS

Butler Technology and Career Development District uses technology and the Internet to teach the skills, and behaviors that students will need to engage in this rapidly changing world to be successful and responsible members of the community, and life-long learners.

#### **I. THE POLICY**

This document serves as the Responsible Use and Internet Safety Policy (“Policy”) of the District. Technology and the Internet are rapidly evolving, and this policy cannot lay down rules to cover every possible situation. Therefore, we begin with the three basic principals below, and the expectation that all students, employees and guests who use this technology will do so in a way that is consistent with the District’s educational mission.

#### **II. BASIC PRINCIPALS**

As a member of the Butler Tech community, I agree to the following principles:

**1. To Respect and Protect Myself**

I will make school-appropriate judgments about the information and images that I view and share online. I will be careful with the personal information and images I share about myself. I will protect passwords, accounts, and resources. I will not use District resources for inappropriate and/or unlawful activities. If I am unsure of the lawful nature of an activity, I will consult with the person(s) designated by the District to help me decide if a use is appropriate. I will report any attacks or inappropriate behavior directed at me.

**2. To Respect and Protect Others**

Everything in #1 also applies to my treatment of others. I will not use any medium to bully, harass, or stalk other people. I will not share information and images about others without permission. I will show respect for others by not using/altering their passwords/accounts. I will report any attacks or inappropriate behavior directed at others.

**3. To Respect and Protect Intellectual and Physical Property**

I will not plagiarize the work of others and I will respect copyright laws. I will only use the District’s technology, network, and resources for school-appropriate activities and encourage others to do the same. I will treat the District’s technology equipment with care.

In addition to the aforementioned principals, listed below are specific provisions of your agreement regarding computer network and Internet use. Contact a building administrator if you have any questions about these provisions. If any user violates this Policy, the user’s access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

Upon signing this Policy, each user will be given the opportunity to enjoy Internet access at school and agrees to follow the Policy. If a user is under 18 years of age, he or she must have his or her parents or guardians read and sign the Policy. The District cannot provide access to any user who, if 18 or older, fails to sign and submit the Policy to the District as directed or, if under 18, does not return the Policy as directed with the signatures of the student and his/her parent or guardian.

## RESPONSIBLE USE AND INTERNET SAFETY POLICY

### III. UNACCEPTABLE USES

#### A. 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 District's Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers 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 computers, networks, or information systems.
3. Uses that jeopardize the security of user access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user.
4. Uses that are commercial transactions. 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. You may not use the computer network or devices for online gaming or gambling.
5. Uses which violate District fraternization policies or uses which promote undue familiarity between those in a faculty/student or superior/subordinate relationship. For example, students becoming online 'friends' with faculty on a social networking site.
6. Use of any personal devices on campus which violate any policy (for example, sexting using a personal cell phone).
7. Social Media. Use of social media during school hours or using District computer networks, internet, or devices must be authorized by a teacher for an approved educational purpose. Any social media activity of a student while using District computer networks, internet, or devices are subject to the Responsible Use Policy. Any social media activity that is directed at the Butler Tech community and/or is disruptive shall result in discipline.

#### B. **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. 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.

## RESPONSIBLE USE AND INTERNET SAFETY POLICY

2. Don't assume that the sender of a message is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her information to third parties. This should only be done with permission or when you know that the individual would have no objection.
3. Be considerate when sending attachments (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 that the recipient can open.

### V. INTERNET SAFETY

- A. General Warning; Individual Responsibility Users.** All users and their parents/guardians are advised that access to the electronic 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 computer network and Internet and stay away from these sites. Parents of minors are the best guides 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 District's Technology Helpdesk.
- B. Personal Safety.** Be safe. In using the computer 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 computer 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. Illegal Activities.** It is a violation of this Policy to use the District's computer network or the Internet to gain unauthorized access to other computers or computer 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 User Information.** Personally identifiable information concerning users 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 District, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering technologies designed to prevent users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The District 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 that 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 when appropriate.

## RESPONSIBLE USE AND INTERNET SAFETY POLICY

The term “harmful to minors” as used above means 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;
- and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

### **VI. DISTRICT-PROVIDED DEVICES**

When using District-provided technology devices, users are accountable for the responsible use of the devices. Use of District-provided devices is a privilege which may be revoked at any time.

Violation of these policies will be subject to normal disciplinary action. Butler Tech has adopted a separate handbook for its 1:1 Mobile Learning Device (MLD) Program. Both this Responsible Use Policy and the MLD Handbook apply to District-provided devices. In the event of any conflict between this Responsible Use Policy and the MLD Handbook, the MLD Handbook shall control.

- A. Content and Software** – District equipment is to be used for educational purposes only. Music, videos, games and software must be District approved and installed.
- B. Configuration** – users may not alter the configuration of the device or install passwords on screensavers, BIOS settings menus, or deletion of files or folders. Deletion of some files may also result in a computer failure and may interfere in the ability to complete classwork, directly impacting grades.
- C. Equipment Repairs** – if the computer fails while in use, a determination will be made to determine if the failure was due to the equipment, or due to improper use. If the failure is due to improper use, the student or parent may be held liable for repairs.
- D. Loss or Damage** – if equipment is issued to the user, and the property is damaged, lost or stolen, the user is responsible for the cost or repair or replacement based upon the fair market value at the date of loss. Loss or theft of property must be reported to the District within one business day, and a police report must be filed within 48 hours of the occurrence if applicable.
  - a. If the equipment is stolen:**
    - i. File a police report within 48 hours of the occurrence
    - ii. Notify the Principal or Supervisor immediately, or within one business day
  - b. If the equipment is lost:**
    - i. The user will be responsible to pay the District the total costs associated with replacing the equipment.
  - c. Users will be charged for the replacement or repair of the equipment if it has been deliberately damaged or vandalized.**

### **VI. PERSONAL DEVICES**

If personal electronic devices are used on the District network or on District property, use of the personal device must be consistent with the District AUP. Internet access on the District network is recorded, and misuse of personal devices, on or off the District network while on District property, will be subject to normal disciplinary action.

## **RESPONSIBLE USE AND INTERNET SAFETY POLICY**

- A. Cell phone Use.** Personal cell phones on campus will be set to 'silent' or powered off during class unless they are being used for educational purposes as defined by the instructor. During non-class time the regulations of the student handbook define how they may be used, so long as they are not a disruption and such uses comply with District AUP standards. Any misuse will be subject to normal disciplinary action.
- B. Other devices.** Use of other personal devices (such as laptops, tablets, iPods, mp3 players and other personal devices) on the District campus or network must be in compliance with the District AUP; misuse will be subject to disciplinary action.

### **VII. PRIVACY**

Network and Internet access is provided as a tool for your education.

**The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of computers, networks 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 District and no user shall have any expectation of privacy regarding such materials or devices.**

Users shall have no expectation of privacy in any emails, instant messages, documents, text messages, or any other electronic communication sent, received, or stored by or through Butler Tech's computers, computer network, electronic messaging systems, or other devices.

Users must not consider these communications to be private or confidential: All emails, instant messages, documents, text messages, and other information that is accessed, stored, created, received, or sent by or through any of Butler Tech's computers, computer network, electronic messaging systems, and other devices may be the property of the District. **Authorized District personnel may view files, communications, data, or any other electronic communication at any time for any reason.**

### **VIII. FAILURE TO FOLLOW POLICY**

Use of the computer network and Internet is a privilege, not a right. Any user who violates this Policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the District may refuse to reinstate for the remainder of the user's enrollment in the 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 computer network and Internet, including any user whose access has been denied or terminated. The District may also take other disciplinary action in such circumstances.

### **IX. WARRANTIES/INDEMNIFICATION**

The District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks 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 use of its computer networks 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, the Board of Education, the Data Acquisition Site that provides the computer and Internet access opportunity to the 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 computer network and the Internet, including

## **RESPONSIBLE USE AND INTERNET SAFETY POLICY**

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 District in the event of the District's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a District computer or on another computer outside the District's network.

### **X. 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 District to receive such information.

### **XI. EDUCATION, SUPERVISION AND MONITORING**

It shall be the responsibility of all members of the Butler Tech staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Information Technology or designated representatives.

The Director of Information Technology or designated representatives will provide age-appropriate training for students who use Butler Tech's Internet facilities. The training provided will be designed to promote Butler Tech's commitment to:

- The standards and acceptable use of Internet services as set forth in Butler Tech's Internet Safety Policy.
- User safety with regard to: (1) safety on the Internet; (2) appropriate behavior while on online, on social networking Web sites, and in chat rooms; and (3) cyberbullying awareness and response.
- Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the user will acknowledge that he/she received the training, understood it, and will follow the provisions of Butler Tech's responsible use policies.



