Campbellsville Independent School District

(CISD)

Acceptable Use Policy(AUP),
Internet Safety Policy
&
Bring Your Own Device (BYOD) Policy

Overview --

Each person attending school or working at Campbellsville Independent School District (CISD) will be given an account in order to access the district's computer network. Once the appropriate forms are signed, and/or privileges are granted by the parent/guardian, this account will also allow the user to access the Internet, E-Mail (Electronic Mail) or both. This access is a privilege and not a right. Should a user violate any of the rules or policies outlined within this document, these privileges may be suspended or revoked.

1988 Senate Bill 230 requires that students having access to the Internet must have a parental permission form on file with the school. It is a requirement of this district in compliance with 1988 Senate Bill 230 that said permission form must be signed each school year and be on file in the office of the pertinent school before access to the internet is granted to any student. Permission may be revoked by parent and/or guardian at any time throughout the school year.

All computers are the property of the Campbellsville Independent School District and all data stored on them is the property of the school system.

Access to Inappropriate Material –

Access of materials deemed as inappropriate, including but not limited to, sexually explicit and/or obscene, is strictly prohibited. The District utilizes Internet filtering technology in order to limit access to such sites and materials. All internet traffic is logged and archived. If a faculty member suspects that a student has accessed an inappropriate website, a request can be made of the district technology staff to retrieve the logs for a particular student for a given period of time. The local administrative staff at the school will then evaluate the data and take the appropriate action. This action may include the suspension of the student's internet access up to total denial for the remainder of the school year. This policy is in accordance with ***701 KAR 5:120 Prevention of Objectionable Material Transmitted to Schools via Computer.***

Internet Safety and Security –

The safety of our students is of utmost importance to the District. Students shall be provided instruction about appropriate online behavior, including interacting with other individuals online. This instruction will include cyberbullying awareness and response. Internet safety measures shall be implemented that effectively address the following:

-Controlling access by minors to inappropriate matter on the Internet and World Wide Web;
-Safety and security of minors when they are using email, chat rooms, and other forms of direct electronic communications;
-Preventing unauthorized access, including "hacking" and other unlawful activities, by minors online;
-Unauthorized disclosure, use and dissemination of personal information regarding minors;
-Restricting minor's access to materials harmful to them.

The access of social websites from the District network by students is expressly forbidden. Electronic chat rooms, Internet Relay Chat, Skype, etc. are not permitted by students without strict faculty supervision. These types of sites are filtered by our Internet filtering system. CISD strongly advises against district faculty and staff interacting with students on social networks such as Facebook. The only E-Mail system that may be accessed via the District's network is the Kentucky Department of Education's approved system. Access to any other E-Mail system via our network is strictly prohibited. These sites are also filtered by our Internet filtering system. This is in accordance with ***701 KAR 5:120 Prevention of Objectionable Material Transmitted to Schools via Computer***. The District provided E-Mail system is for educational purposes only.

Unauthorized Access –

Access of the District network and/or a school owned computer may only be permitted with a student's personal login and password. A student may not reveal their password to anyone nor may they use another's password to access a district computer or the network. The use of any software in the attempt to gain access to a computer and/or network, obtain another user's password, or interfere with the flow of information on the network is strictly prohibited. The downloading and use of Port Scanners, hacking software, etc., is strictly prohibited unless authorized in an IT class and monitored by a faculty member. ***KRS 434.520 Unlawful access to a computer in the second degree*** states that unlawful access to a computer is a Class D felony. Any student found in violation of this statute may, at minimum, lose their network/computer privileges and at most, be brought up on criminal charges.

Misuse of Computer Information –

Any student who accesses any information, software and/or records, or assists another in doing same, is in violation of ***KRS 434.845 Misuse of Computer Information***. Examples of this type of information include, but are not limited to, Infinite Campus for student records and data and MUNIS for financial records. Gaining access to these types of information and redistributing to others, or changing information (such as student grades or attendance records) constitutes violation of this statute. ***KRS 434.845*** states that Misuse of Computer Information is a Class C felony. Any student found in violation of this statute may, at minimum, lose their network/computer privileges and at most, be brought up on criminal charges.

E-Mail and Microsoft Live @ EDU –

The Outlook Live e-mail solution is provided to users by the district as part of the Live@Edu service from Microsoft®. By signing/acknowledging this AUP, you hereby accept and agree that your right to use the Outlook Live e-mail service, and other Live@Edu services as the Kentucky Department of Education may provide over time, are subject to the terms and conditions set forth in this AUP and that the data stored in such Live@Edu services, including the Outlook Live e-mail service, are managed by the district pursuant to **policy 08.2323** and accompanying procedures. And said email is not private. You also understand that the Windows Live ID provided to users can be used to access other electronic services that provide features such as online storage and instant messaging. Use of those Microsoft® services is subject to Microsoft's® standard consumer terms of use (the Windows Live Service Agreement), and data stored in those systems are managed pursuant to the Windows Live Service Agreement and the Microsoft® Online privacy Statement. Before users can use those Microsoft services, he/she must accept the Windows Live Service Agreement and, in certain cases, obtain parent\guardian consent.

Teacher and Staff Supervision of Student Technology Use --

Teachers and others whose duties include classroom management and/or student supervision shall acknowledge responsibility for exercising reasonable supervision of student access to Internet and electronic mail by signing their Acceptable Use Agreement.

Teachers shall not direct or advise students accessing school computing and communications networks to use electronic mail systems other than the Kentucky Educations Technology System standard email system.

Teachers must be prepared to integrate the use of electronic resources into the classroom. Generally, the manner in which teachers evaluate instructional materials and content today will apply to the selection of electronic resources. On the Internet, however, information can be made available without being edited by a publisher, screened by a textbook committee, or selected by a known bookseller. Teachers must be cautioned that:

> **Quality and integrity of content on the Internet is not guaranteed. Teachers and students provided permission to do independent research must examine the source of the information. Is the source clearly identified? Is it an individual? Is it an organization? Is it an educational institution? Is it a publisher?**

In the same way that a teacher or library media specialist provides various levels of guidance to students visiting a library, the teacher/staff member supervising student use will want to structure various levels of Internet access depending upon age, grade level, or student performance. For instance:

1) Very young children should not be provided with unsupervised access to computers. At the lower grade levels, an Internet or email session may be best conducted with small groups and always supervised by a teacher or someone the teacher has designated.
2) Children in middle school, who are familiar with the Internet, and generally demonstrate good conduct, might be provided with limited independent access in a location where the session can be monitored.
3) In the upper grades, those students with good standing who have proven their ability to be responsible Network users might be provided with independent, unsupervised access for research purposes.

School Telephone Usage –

Telephone handsets in classrooms are available primarily to provide two-way communication with the school office and for contact with parents. Staff will refrain from using telephones during instructional time. Students may use the telephones only with a teachers or staff members' specific permission. Instructional time will not be interrupted to transfer calls except in emergencies. All guidelines contained within this AUP governing inappropriate language apply to telephone usage. The procedures in this AUP governing telephone usage also apply to district owned cellular phones and other wireless telecommunication systems.

Personally Owned Devices – (BYOD- bring your own device)

Personally Owned Devices (POD) include, but are not limited to; external USB storage devices, cell phones, smart phones, Android devices, iOS devices, laptop or netbook computers, and e-Readers (Kindles, or Nooks). Users are not required to bring personal devices, but if they choose to do so the following rules apply. The classroom use of personal devices is the decision of each school. Teachers and staff are the managers of each classroom and can determine if a device can or cannot be used at any given time. District staff may at any time inspect the content of any personal device.

The Campbellsville Independent School District has adopted a Bring Your Own Device (BYOD) policy for all schools in the district. This policy allows students to bring many of their own technology devices to school for use in our classrooms. Similar to other personally owned items, the district/school is not liable for the loss, damage, misuse, or theft of personally owned devices brought to school. All device configuration, maintenance and upkeep are the sole responsibility of the device owner.

Again, Students are not required to bring in outside technology to school. All students will continue to be able to utilize school equipment. No student will be left out of the instructional process.

Expectations for POD use at Campbellsville Schools: (Note that each school's SBDM can make rules more restrictive than the following, but these are a minimum)

1. Students will only use appropriate technology at teachers' discretions and will abide by procedures for use set forth by the classroom teacher.

2. Students will only use appropriate educational applications on their device as determined by the teacher (i.e. not non-school related tasks and functions).

3. Students are not to call, text message, email, post to social networks, or electronically communicate with others from their personal device, including other students, parents, guardians, friends, and family during the school day unless it is part of classroom instruction.

4. Students' devices must be registered and are permitted to access only the school's network, not private networks.

5. Teachers will not ask students to download any apps that incur a charge. They may however ask them to download free apps to use in the classroom. If a student chooses to download apps that have a charge, then they are responsible for those charges, not the CISD teachers, or administrators.

Reinforcement:

Students utilizing this opportunity to its fullest capacity within school expectations will find numerous benefits to instruction, resources, completion of assignments and personal organization.

Students not following expectations for use of personal devices will face school disciplinary measures, and/or lose access to the Districts Wireless network.

Other Policies –

Users are also not permitted to engage in the following:

- Harassing, insulting or attacking others
- Using obscene language
- Sending or displaying or accessing offensive messages or pictures
- Intentionally circumventing district proxies and filter devices
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Trespassing in another's folders, work or files
- Intentionally wasting limited resources (playing unauthorized games, unauthorized streaming video, unauthorized streaming music, accessing Facebook etc.)
- Employing the network for commercial purposes
- Intentionally loading viruses onto computers, diskettes, flash drives or networks
- Using technology resources to bully, threaten or attack a staff member or student or to access and/or set up unauthorized blogs and online journals, including, but not limited to MySpace.com, Facebook.com or Xanga.com.

Summary –

Outlined here are various activities that are prohibited by District policy. Access to the computer systems and network is a privilege for our users, not a right. Any user found in violation of these policies may result in immediate termination of computer/network privileges, other disciplinary actions as deemed by the School/District administrative staff, and/or criminal prosecution. The primary manner in which these rules will be enforced will be through teacher/faculty supervision. Automated safeguards have been put into place to filter and guard against inappropriate Internet sites and materials. The District also has appliances in place that "watch" the network for inappropriate traffic. This traffic can be traced to a single workstation and the user of that machine can be identified.

CISD Faculty/Staff Acceptable Use Policy Agreement Form

The following agreement form is to be distributed to all CISD faculty and staff. A signed agreement form must be on file at the school for each district staff member who wishes to use the network or Internet. The building Principal will retain all forms.

By signing the user agreement the staff member has agreed to abide by board policies governing access to technology resources.

____YES, I have read the CISD Acceptable Use Policy. I understand and will abide by the stated terms and conditions. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, Furthermore, if needed, appropriate legal action may be taken. I understand that I could engage in unauthorized conduct that results in liability. I will assume full responsibility for that liability and release and hold the District harmless for any consequences that result from my conduct.

Name (Please print): _____

School Assignment _____

Job Title: _____

Signature:_____ Date:_____

Staff Responsibility -Must be signed if working with students and the Network
I agree to promote the Student Acceptable Use Procedures with each of my students. I agree to instruct students on acceptable use of the Network and Internet and proper Network/Internet etiquette. During the times students are assigned to my care, I agree to direct students to acceptable Network/Internet resources and monitor their use at all times. Neglect in my responsibility as an instructor could result in disciplinary action.

Name (Please print):_____

Signature:_____Date:_____

CISD Student User Contract

Directions: Please read the attached policies governing computer use and acceptable use of the Network. The signature of a parent/guardian is required for all students wishing to use the CISD Network. Please check the appropriate box and sign below. After completing, please return **this page only** to your school.

Student Agreement (Students should sign below to indicate their agreement to the following)

_____ **Yes** I have read the CISD Acceptable Use Policy. I understand and will abide by the stated terms and conditions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action WILL be taken. Furthermore, if needed, appropriate legal action may be taken. I understand that I could engage in unauthorized conduct that results in liability. I will assume full responsibility for that liability and release and hold the district harmless for any consequences that result from my conduct.

Student Name (please print): _____

Student Signature: _____ Date: _____

Parent/Guardian Agreement (Please check one of the following and sign below)

_____ **Yes** As the parent or guardian of this student, I have read the CISD Acceptable Use Policy for Internet and Email access. I understand that this access is designed for educational purposes and the CISD technology staff have taken available precautions to eliminate access to controversial material. **However, I also recognize it is impossible for CISD to restrict access to all controversial materials and I will not hold them responsible for materials this student may acquire on the Network.** Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission for the student named above to have access to the Network, including Internet and email access. I understand that my student could engage in unauthorized conduct that results in liability. I/we will assume full responsibility for that liability and release and hold the district harmless for any consequences that result from my student's conduct.

_____ **No** I have read and understand the CISD Acceptable Use Policy for Internet and Email access, but I **do not** want my student using the Internet or Email at school.

Parent/Guardian (please print): _____

Signature: _____ Date: _____