



## Electronic Access/User Agreement Form

STUDENT NAME: \_\_\_\_\_

PARENT NAME: \_\_\_\_\_ SCHOOL: \_\_\_\_\_

I have read the District's Acceptable Use Policy, understand the policy, and agree to comply with the policy as stated. Should I violate the policy, I understand that I may lose network privileges.

\_\_\_\_\_  
*Student Signature Date*

As the parent or legal guardian of the student signed above, I grant permission for the student to access networked services such as e-mail and the Internet. The District uses software to control access to objectionable material on the Internet and provides supervision of student computer use. However, I understand that some material accessed on the Internet may be objectionable. I accept responsibility for providing the student guidance on Internet access.

\_\_\_\_\_  
*Parent/Guardian Signature Date*

### Parent Permission for World Wide Web Publishing of Student Work

We understand that our daughter's/son's work (art, writing, etc.) may be considered for publication on the World Wide Web, a part of the Internet. No home address or telephone number will appear with such work.

We grant permission for publishing on the World Wide Web as described above. A copy of all work published on the World Wide Web will be printed out and sent home with the student.

\_\_\_\_\_  
*Parent/Guardian Signature Date*

I, the student, give permission for publishing my work on the World Wide Web.

\_\_\_\_\_  
*Student Signature Date*

NOTE: Federal law requires the District to monitor online activities of minors.

### Staff Agreement and Responsibility – (Must be signed if working with students and the network)

I understand and will abide by the Fleming County School District's Acceptable Use Procedures for Network Access and Telephone Usage. I further understand that any violation of the regulations stated in this policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action up to and including termination may be taken, and/or appropriate legal action may be pursued.

I agree to promote the Acceptable Use Procedures with each of my students. I agree to instruct students on acceptable use of the network and proper network/telephone etiquette. During the times students are assigned to my care, I agree to direct students to acceptable network/telephone resources and monitor their use at all times. Neglect in my responsibility as an instructor could result in disciplinary action.

Personnel Name (Please print): \_\_\_\_\_ School Assignment: \_\_\_\_\_

Job Title: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

# Fleming County Schools

### Fleming County School District Acceptable Use Policy

The Fleming County School District provides students and staff with a service called the Network. The Network is a computer service, which includes the use of computers, servers, software, Internet and E-mail. This Policy addresses the acceptable use of the Network. It also addresses the use of stand-alone computers, peripherals, telephone usage and other instructional technology equipment. All employees, students, parents/guardians or any other persons accessing the Network must sign the Acceptable Use Policy before direct access is provided.

In addition to providing students with the understanding and skills needed to use the Network and telephone services in an appropriate manner, the Fleming County School District:

- Reserves the right to monitor all activity on the Network.
- Reserves the right to monitor computer use or lack of use.
- Reserves the right to deny access of the Network to any individual.
- Shall establish procedures that will maximize the Network system security.
- Shall supervise student use of the Network and Telephones.

#### **The following standards for student and staff access to the Network will be as follows:**

- Network access throughout the district is to be used only for instruction, research, school administration, and work related communications. District access is not to be used for private business.
- Instructional staff will select and guide students on the appropriate use of Internet and instructional software on the Network.
- The district will be responsible for supervising network use. Auditing procedures are in place to monitor access to the network. School and district proxy servers will be continually monitored and updated in accordance with the federal legislation, [Children's Internet Protection Act](#) (CIPA: 47 U.S.C. 254), KY Senate Bill 230, and KY KAR 5:120.
- However, the district cannot continually monitor every communication and network session for every student and staff member beyond the scope of supervision defined in the user agreement.
- Internet access and supervision from outside the district premises is the responsibility of the parents or guardians.
- Users should not reveal their full name and personal information (address, phone number, financial information, social security number, etc.) or establish relationships with "strangers" on the network, unless the communication has been coordinated by instructional staff.
- Staff will not reveal a student's full name or post a picture of the student or the student's work on the Network with personally identifiable information unless the parent has given written consent.
- The content of any district web page is the responsibility of the sponsoring staff member who hosts the page.
- School-related clubs and organizations that wish to establish a web site must be a part of the school's web account.
- Non-instructional chat rooms may not be included on any school web account.
- Be polite. The use of appropriate language shall not include vulgar or abusive messages.
- Attempting to disrupt communication on the network by creating or downloading computer viruses or destroying data of other users is a form of vandalism.
- Passwords are private. You are responsible for your password. Do not allow others to use your password. Do not use another user's password or trespass in folders, work or files of others.
- Use of the Network that offends or tends to degrade others will not be allowed.
- Do not attempt to gain unauthorized access to resources and entities.
- Do not install or use any unauthorized software or hardware to any district computer system or Network. This includes down loading games, music, videos, etc. Copyrights must be respected. • Do not use the Network for any illegal activity, including violation of copyright or other contracts.
- Do not attempt to modify or remove computer equipment, software, or peripherals without proper authorization.
- Do not take actions, without authorization, which interfere with the access of others to information systems.
- Do not circumvent logon or other security measures. (McAfee, etc.)
- Do not use proxy anonymizer (proxy bypass) sites to circumvent network restrictions.

- Streaming or downloading video or audio for non-educational purposes is strictly prohibited.
- Do not use MUD (multi-user games) via the network.
- Do not purposefully annoy other Internet users, on or off the Fleming County Network. This includes such things as continuous talk, requests, chat lines, etc.
- Do not establish or access e-mail accounts through third party providers. Only Kentucky Education Technology Systems can be used.
- Use of pen drives (USB flash drives) is limited to educational purposes. Pen drives may not be used to transfer software, inappropriate material, or downloaded music, games, or videos to the district network. Pen drives must be scanned for viruses upon connecting to a network workstation.

### Telephone Usage

- Telephone calls are available primarily to provide two-way communications with the school office and for contact with parents.
  - Staff will refrain from using telephones during instructional time.
  - Students may use the telephones under staff supervision when there is a legitimate need such as: calling parents to arrange transportation, delivery of medicine or clothes, or similar rare circumstances.
  - Instruction time will not be interrupted to transfer calls except in emergencies.
  - The use of cellular devices by students and staff during the school day is prohibited except in emergency situations.

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 cellular phones and other wireless telecommunication systems.

### Staff and Student Owned Computing Devices

The Fleming County School District continues to improve Network services. Where wireless network access is available, students and staff may be permitted use personally owned devices, when appropriate. The following conditions must be addressed prior to the district allowing access to any student or staff member.

- Security, including virus protection
  - Network stability
  - Liability for personal property
  - Repairs and upgrades

Any student or staff member who brings a personally owned computer or other technology device to school shall be personally responsible for the safety and security of the equipment, and shall therefore be responsible for any damages to those devices. No privately owned device shall be granted access to the Network without authorization of the district technology staff. Any device that connects to the Internet via wireless connection (802.11 a/b/g/n) is considered a technology device. Any device that operates via the following operating systems is considered a computing device: Palm OS, Windows, Pocket PC, Mac, or other like system. Student-owned devices connecting to the Fleming County Schools network wirelessly may be granted Internet access only. All Internet traffic shall be logged and filtered through the district proxy (Senate Bill 230; 701 KAR 5:120)

Any software residing on privately owned computing or technology devices is the sole responsibility of the owner and must be personally owned and legally obtained. The District shall not be responsible for determining whether software residing on privately owned devices is legal. Anti-virus software is the responsibility of the owner and must be updated to meet the minimum requirements of the district. Any device failing to meet anti-virus standards will be denied access to the District Network. Any personal software residing on student or staff owned devices that interfere with the Fleming County Schools Network may be removed by District technology staff; alternately, the technology staff may remove the device from the network until such software is removed.

Repair and maintenance of student and staff owned devices is the sole responsibility of the owner. District owned internal components may not be added to personally owned devices. Any damages incurred to personally owned devices as a result of use on the Fleming County Schools Network are the responsibility of the owner. The privacy and security of any item stored on or transmitted by personally owned devices is the responsibility of the owner.

### **For all privately owned computing or technology devices in Fleming County Schools, the District reserves the right to:**

- Monitor and log all activity.
  - Determine when and where the use of such devices is permissible.
  - Determine whether specific uses of these devices are consistent with the Acceptable Use Policy and Discipline Handbook.
  - Determine whether use of these devices or network resources is appropriate.
  - Install additional management software and/or apply permission or security policies to such devices.
  - Remove the user's access to the network and/or terminate the right to use personally owned equipment in district facilities if it is determined that the user has engaged in unauthorized activity or has violated the Acceptable Use Policy.

Please complete the information below and return a copy to the District Technology Coordinator to request permission to use a privately owned computing or technology device on the Fleming County Schools Network.

Brand Name: \_\_\_\_\_ Model #: \_\_\_\_\_ Serial #: \_\_\_\_\_

Description: \_\_\_\_\_ Equipment Location: \_\_\_\_\_

Student Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Parent Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Disciplinary Action**

- Student discipline for violation of any part of these procedures shall be based on the severity of the infraction.
  - Student disciplinary action includes, but is not limited to, the loss of any or all computer privileges, termination of the user's account, removal from the class with a failing grade and/or suspension/expulsion. Privileges will be reinstated at the discretion of the district administrators.
  - Discipline of staff may involve actions up to and including termination of employment.
  - Parents, guardians and/or perpetrators may be billed for damages to technology resources.
  - Illegal/criminal activities will be referred to the appropriate law enforcement agency.
  - Students or staff members who deface a District web site or otherwise make unauthorized changes to a web site shall be subject to disciplinary action, up to and including expulsion and termination, as appropriate.

**Outlook Live**

The Outlook Live e-mail solution is provided to your child by the District as part of the Live@edu service from Microsoft. By signing this form, you hereby accept and agree that your child's rights 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 District policy/procedure as provided, and that the data stored in such Live@edu services, including the Outlook Live e-mail service, is managed by the district pursuant to policy 08.2323 and accompanying procedures. You also understand that the Windows Live ID provided to your child can also 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 is managed pursuant to the Windows Live Service Agreement and the Microsoft Online Privacy Statement. Before you child can use those Microsoft services, he/she must accept the Windows Live Service Agreement and, in certain cases, obtain your consent.