



FLOYD COUNTY BOARD OF EDUCATION

Tonya Horne-Williams, Superintendent

442 KY RT 550

Eastern, KY 41622

Telephone (606) 886-2354 Fax (606) 886-4550

www.floyd.kyschools.us

William Newsome, Jr., Board Chair - District 3

Linda C. Gearheart, Vice-Chair - District 1

Dr. Chandra Varia, Member- District 2

Keith Smallwood, Member - District 4

Steve Slone, Member - District 5

Consent Agenda Item (Action Item):

Receive information about House Bill 208 and how Floyd County Schools is already in full compliance with the requirements outlined.

Applicable State or Regulations:

Board Policy 01.11 General Powers and Duties of the Board of Education.

Fiscal/Budgetary Impact:

There is no new budgetary impact to the district.

History/Background:

HB 208 requires district policy at a minimum to prohibit a students use of a personal telecommunications device during instructional time, except during an emergency, if directed to do so by a teacher for an instructional purpose, or if authorized by a teacher. This is outlined in our Acceptable Use Policy (attached) given to parents and students each year. HB 208 also requires districts to prevent access to social media and sexually explicit material through filtering technology, which Floyd County has a web filter already in place blocking such sites.

Recommended Action:

Receive information as presented.

Contact Person(s):

Wes Turner (606) 886-2354

Director

Superintendent

Date:

May 13, 2025

CHAPTER 90

(HB 208)

AN ACT relating to technology in public schools.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔Section 1. KRS 158.165 is amended to read as follows:

- (1) (a) The board of education of each school district shall ~~adopt~~^{develop} a policy regarding the possession and use of a personal telecommunications device by a student while on school property ~~or while attending a school-sponsored or school-related activity on or off school property~~, and shall include the policy in the district's written standards of student conduct.
- (b) *The policy shall, at a minimum, prohibit a student's use of a personal telecommunications device during instructional time, except during an emergency, if directed to do so by a teacher for an instructional purpose, or if authorized by a teacher.*
- (c) A student who violates the policy shall be subject to discipline as provided by board policy.
- (2) *As used* in this section, "personal telecommunications device":
 - (a) Means a device that emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor, including~~[-]~~ but not limited to~~[-]~~ a paging device and a cellular telephone; *and*
 - (b) *Does not include any device a student is authorized to use pursuant to the Individuals with Disabilities Education Act, 20 U.S.C. sec. 1400 et seq., the Americans with Disabilities Act, 42 U.S.C. sec. 12101 et seq., or the Rehabilitation Act of 1973, 29 U.S.C. sec. 701 et seq., or successor acts.*

➔Section 2. KRS 156.675 is amended to read as follows:

- (1) The Kentucky Board of Education shall promulgate administrative regulations to prevent *social media and* sexually explicit material from being transmitted via any video or computer system, software or hardware product, or Internet service managed or provided to local schools or school districts.
- (2) Each local school district and school shall utilize the latest available filtering technology to ensure that *social media and* sexually explicit material is not made available to students.
- (3) The Kentucky Department of Education shall make available to school districts and schools upon request and without cost, state-of-the-art software products that enable local districts and schools to prevent access to *social media and* sexually explicit material. The department shall also notify all school districts and schools of the availability of the software. Any product provided or obtained by a district or school shall meet the requirements of subsection (2) of this section.
- (4) Each local school district shall establish a policy regarding student internet access that shall include~~[-]~~ but not be limited to~~[-]~~ parental consent for student internet use, teacher supervision of student computer use, and auditing procedures to determine whether education technology is being used for the purpose of accessing *social media or* sexually explicit or other objectionable material.
- (5) *The provisions of subsections (1) to (4) of this section shall only apply to social media that a student is not authorized by a teacher to access for an instructional purpose.*

Signed by Governor March 26, 2025.



FLOYD COUNTY SCHOOLS ACCEPTABLE USE POLICY



CURRICULUM AND INSTRUCTION POLICY # 08.2323

Floyd County School District in compliance with the KETS Master Plan for Kentucky provides students and staff with electronic information and communication to enhance learning through electronic resources via means of Internet and E-mail. We believe it is incumbent upon users to utilize this privilege in an appropriate and responsible manner as required by this policy and related procedures, which apply to all parties who use District technology.

PARENTAL CONSENT REQUIREMENT

Regardless of the level, the student must sign a user's agreement and parental permission must be secured before Internet access can be provided. This policy acknowledges the fact that standards of behavior relating to morals and personal values are within the realm of the family. To the degree that a parent guides a child's exposure to television, videos, and music the parent should guide the child's exposure to the computer networks when giving permission for independent access or individualized study. The school cannot be held responsible if a student given parental permission for independent access intentionally accesses material, which his/her family considers objectionable. District and school acceptable use policies are intended to address "ethics," leaving issues relating to "morals" between the parent or guardian and child. Parents shall be notified in writing (via Code of Conduct) that the Internet and electronic mail may be used with students as part of the instructional process.

Parents shall be notified (via Code of Conduct) that students must sign a student Acceptable Use Policy agreement before direct access to Internet and electronic mail will be provided. Written parental consent shall be required (AUP user agreement) before any student is given direct, hands on access to the Internet or to electronic mail.

This AUP, once signed by the Student/Staff/Admin/Parent, shall be kept on file as a legal, binding document, for the duration of their career at Floyd County Schools unless otherwise dictated by policy change.

"Parental Consent to Child's Use of Microsoft Online Service. When your child provides information to Microsoft, the information is used to enable and customize Microsoft services and for the purposes described in the Microsoft Online Privacy Statement (available online at <https://privacy.microsoft.com/en-us/privacystatement>). Some Microsoft online services within Office 365 allow people of all ages to share personal information with others and that the permission granted hereunder allows your child access to sign in and use these services. Giving or denying permission for your child to sign in and use Microsoft services will not affect his or her ability to use other websites."

Parents shall be notified in writing (via Code of Conduct) that students will be held accountable for violations of the student Acceptable Use Policy agreement and that disciplinary action may be taken.

PERSONALLY OWNED DEVICES

Any school personnel or student who brings a privately or personally owned computer/software/peripheral into the Floyd County School District, may be allowed to connect their personally owned device to the district network, and must adhere to all Floyd County Board of Education Policies and Procedures. This includes all aspects of this Acceptable Use Policy and they must maintain equipment to a Kentucky Education Technology System Standard for Internet and email access. Such access will be monitored and will require students to login using their district credentials. However, families are responsible for all service and support of personal devices. The district is not responsible for any damage or loss incurred with the use of a personal device in the school setting. Students are expected to use devices for educational purposes and only with the consent of school staff.

TEACHER AND STAFF SUPERVISION OF STUDENT COMPUTER USE

1. Teachers/Staff and others whose duties include classroom management and /or student supervision shall sign an Acceptable Use Agreement acknowledging responsibility for exercising reasonable supervision of student access to Internet and Electronic Mail.
2. Teachers/Staff shall not direct or advise students accessing school computing and communications networks to use electronic mail systems other than the Kentucky Education Technology System standard email system.
3. Teachers/Staff shall supervise all student computer use to ensure it is used for educational purposes and non-approved software, programs and resources are not utilized. This includes the restricted use of Virtual Private Networks (VPNs) or Anonymizers that permit access to the Internet via means of bypassing the District's Web Filtering service.
4. Teachers/Staff will maintain daily log files that will provide student name, date, time-in and time out for all student use of computers.
5. Teachers/Staff shall supervise and proof all school-related material placed, posted, or published on school sites.
6. Teachers/Staff shall not publish/post or direct/advise students to post or publish school-related information outside the school district except in cases where students name and or work needs to be published to any online entity or other KDE supported events and where written parental permission has been given.

EMPLOYEE USE

Employees are encouraged to use e-mail and other District technology resources to promote student learning and communication. If those resources are used, they shall be used for purposes directly related to work-related activities.

Employees are required to set up and utilize Multi-factor Authentication (MFA) in order to access district provided accounts and any application that uses district credentials for access. MFA not only protects the employees account but also will aid in protecting the data an employee's account has access to.

Technology-based materials, activities and communication tools shall be appropriate for and within the range of the knowledge, understanding, age and maturity of students with whom they are used.

District employees and activity sponsors may set up websites, messaging apps or social networking accounts using district resources and following district guidelines to promote communications with students, parents, and

the community concerning school-related activities and for the purpose of supplementing classroom instruction with school and/or district level administrator approval.

Networking, communication and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

In order for district employees or district activity sponsors to set up websites, messaging apps or social networking accounts for instructional, administrative or other work-related communication purposes, they shall comply with the following:

- They shall request prior permission from the Superintendent/designee.
- If permission is granted, staff members will set up the site following any District guidelines developed by the Superintendent's designee.
- Guidelines may specify whether access to the site must be given to school/District technology staff
- Follow all guidelines of the District's Internet Safety Standards
- If written parental consent is not otherwise granted through AUP forms provided by the District, staff shall notify parents of the site and obtain written permission for the students to become "friends" prior to the students being granted access. This permission shall be kept on file at the school as determined by the Principal.
- Once created, the sponsoring staff member is responsible for the following:
 - Monitoring and managing the site, application or account to promote safe and acceptable use; and observing confidentiality restrictions concerning release of student information under state and federal law.

District Employees are discouraged from doing the following:

- Creating personal social networking sites to which they invite students to be friends; or Engaging in personal interactions with students via postings on other networks. Employees taking such actions do so at their own risk.

ELECTRONIC MAIL

Standards for use of email by students and staff communication:

- Do not send or attach documents containing pornographic, obscene, or sexually explicit material
- Do not transmit obscene, abusive or sexually explicit language
- Do not transmit any illegal, alcohol, drug or drug related information.
- Do not use electronic mail for communications, which are not directly related to instruction, sanctioned school activities, or a person's job.
- Do not use electronic mail, for instance, for private business or personal, non-work related communications
- Do not access, copy or transmit another's messages and or attachments without permission.
- Do not use electronic mail to transmit any form of aggression (e.g. threats, anger, or harassment, bullying).
- Do not send or forward any form of a chain letter.
- Do not use electronic mail to transmit information or communicate with gangs, hate groups or groups with violent themes.

- Do not use electronic mail to transmit any data relating to violent themes.

SPECIAL SAFETY CAUTIONS, WHICH ARE AGAIN ANALOGOUS TO COMMON PRACTICE:

Students should not reveal their name and personal information to or establish relationships with "strangers" on the network, unless the communication has been coordinated by a parent or teacher. The school should not reveal a student's personal identity unless the parent has given written consent. The school should not transmit a student's work or picture with personally identifiable information without written parental consent.

CYBER BULLYING-as defined is harassing, threatening, or any other type of communication via means of internet or email, and telecommunications including cell phones that threatens a person or persons character or personal safety. You should report any form of "Cyber Bullying" to your teacher, principal, or supervisor as soon as possible.

With respect to the privacy rights of students, teachers, and staff, this policy states clearly that email is not guaranteed to be private. Systems administrators can, and may be required sporadically, to inspect email. This aspect of an acceptable use policy might be analogous to the Board's policy on school lockers; while generally private, lockers may be searched under certain circumstances.

LOCAL TECHNOLOGY RESOURCES

Standards for student, teacher, and staff use of local technology resources (hardware, software, and communications devices) and use of other school property and instructional materials in traditional formats.

- Copyrights must be respected. Copyrighted software and other instructional materials must not be copied or transferred to another except as provided under the license agreement or copyright notice. Resources should not be used for private business or personal gain.
- Authorship and/or publishers of information in electronic form must be appropriately acknowledged in writing and research (footnotes, bibliographies, etc.).
- Vandalism or theft of resources (including data and files) will not be tolerated.
- Passwords must not be exchanged and other's passwords must not be used. The individual is responsible for the security of his/her own password.

THE NETWORK

The Floyd County Schools network and computer resources are provided for instructional and educational purposes only. **The following list items that will not be permitted or tolerated.**

- Accessing, displaying, possession, or transferring pornography, drugs, or other illegal activities.
- Carrying out activities deemed to be a security risk to the network (Use of VPNs, hacking, denial of services, etc.). Use of Non-KETS approved email or online chat service.
- Displaying, sending or publishing obscene, threatening, or harassing messages or pictures.
- Use of the network for private, criminal or malicious intent.
- Trespassing in others computers, network accounts, files, directories, or work.
- Alterations misuse, abuse, or damage to computer or network equipment.

- Loading of illegal, non-approved or non-licensed software, on board owned equipment including uploading and downloading from the Internet and unreliable sources.
- Misuse or intentionally wasting resources via Internet or email.
- Software installation without permission by proper school or district authorities including (Games or Freeware).
- Employment of the network for private, profit, personal, or commercial gain.
- Do not use the network to access, display, send, receive or communicate with gangs, hate groups or groups with violent themes or to participate in any form of "Cyberbullying".
- Any activity deemed inappropriate by school or district authorities.
- Only authorized personnel may post or publish school related information.
- Only school related files or information is to be placed, posted, or published on the Floyd County School Network.
- All school related information placed, posted, or published on the web shall be proofed and approved by authorized school personnel prior to posting/publishing.
- School related information shall not be placed, posted, or published outside the Floyd County School district network without the permission of the Superintendent.

SOCIAL, WEB AND COLLABORATIVE CONTENT

The district recognizes that Internet-based resources that can enhance educational activities are growing in number each day. The district may provide access to web sites or tools that support communication and collaboration with others in addition to general productivity. Students are reminded to communicate appropriately and safely via these resources and that communication may be monitored. Use of any website outside of the district control is subject to their use and may require specific permission in addition to the AUP.

USE OF ARTIFICIAL INTELLIGENCE

Floyd County Schools recognizes the dynamic nature of technology and its profound influence on our global society, local community, and classrooms. As artificial intelligence (AI), including generative AI, becomes increasingly integrated into daily life, it is our duty to instruct and prepare students for its ethical and educational use. While Floyd County Schools does not prohibit the use of AI by students or teachers, there are specific limitations and guidelines that students must be mindful of:

- Student email accounts and Chromebook access to certain open AI software, such as ChatGPT, may be blocked due to concerns about data and security. Any inappropriate use, including hacking or data alteration, is strictly forbidden.
- Teachers may permit the use of AI for educational purposes, and access to specific websites will be granted on a case-by-case basis, adhering to data and privacy guidelines, including age restrictions.
- Additional restrictions and limitations on the use of Artificial Intelligence may apply to College Board and Dual Enrollment college and university classes.
- Students using AI software on personal devices and/or with personal credentials assume the associated risks, acknowledging that each platform collects various forms of data.
- Students must explicitly acknowledge the use of AI in any school-related work, whether it involves text, images, multimedia, etc.
- The use of AI may be subject to the Disciplinary Referral Procedures.
- Students should recognize that AI is not always factually accurate or considered a credible source. Users must be capable of providing evidence to support AI-generated claims and be aware of the potential for bias and discrimination in AI tools and applications.

- Always review and critically assess outputs from AI tools before submission or dissemination. Staff and students should never rely solely on AI-generated content without review.

INTERNET SAFETY STANDARDS

Internet safety standards address all of the following issues:

- Access by minors to inappropriate matter on the Internet
- Internet access through the school is to be used for instruction, research, and school administration. School access is not to be used for private business or personal, non-work related communications.
- The Internet is accessed through assigned user id and password only. Access is not permitted through the use of anonymous proxy sites or sites that permit access to restricted sites via means of a Virtual Private Network (VPN) service.
- The safety and security of minors when using email, chat, and other forms of direct electronic communications
- Unauthorized access including "hacking" and other unlawful activities by minors online

The Floyd County Schools network and computer resources are provided for instructional and educational purposes only. The following list items that will not be permitted or tolerated.

- Accessing, displaying, possession, or transferring pornography, drug, or other illegal activities.
- Carrying out activities deemed to be a security risk to the network (hacking, denial of services, etc.).
- Use of Non-KETS approved email, online chat service.
- Displaying, sending or publishing obscene, threatening, or harassing messages or pictures.
- Use of the network for private, criminal or malicious intent.
- Trespassing in others computers, network accounts, files, directories, or work.
- Alterations misuse, abuse, or damage to computer or network equipment.
- Loading of illegal, non-approved or non-licensed software, on district owned equipment including uploading and downloading from the Internet and unreliable sources.
- Misuse or intentionally wasting resources via Internet or email.
- Software installation without permission by proper school or district authorities including (Games or Freeware).
- Employment of the network for private, profit, personal, or commercial gain.
- Do not use the network to access, display, send, receive or communicate with gangs, hate groups or groups with violent themes or to participate in any form of "Cyberbullying".
- Any activity deemed inappropriate by school or district authorities.
- Only authorized personnel may post or publish school related information.
- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Only school related files or information is to be placed, posted, or published on the Floyd County School Network.
- All school related information placed, posted, or published on the web shall be proofed and approved by authorized school personnel prior to posting/publishing.

- School related information shall not be placed, posted, or published outside the Floyd County School district network without the permission of the Superintendent.
- Students should not reveal their name and personal information to or establish relationships with "strangers" on the Internet, unless a parent or teacher has coordinated the communication.
- The school should not reveal a student's personal identity or post a picture of the student or the student's work on the Internet with personally identifiable information unless the parent has given written consent.
- Schools are encouraged to create and maintain a school website, however only school and related educational information shall be displayed on school or Floyd County School Communication networks.

Measures designed to restrict minors' access to materials harmful to minors. To manage the student or staff member, who is determined or occasionally tempted to violate acceptable use policies, certain deterrents can be put in place:

- Certain network management software packages allow the systems administrator to view or intervene and "take over" a user's screen. These packages are designed for problem diagnosis, to troubleshoot network problems, and to support help desk activities. Although they are not designed to scan network activity for inappropriate use, the district may decide to use them for that purpose on an as needed basis. Regardless, if the user is informed that such scanning is feasible that fact alone may deter inappropriate use.
- With implementation of web filtering services, schools should familiarize parents, students, faculty, and staff with the information contained in web filter logs. The fact that these logs contain detailed information about Internet access, which can be traced to the individual user usually, serves as a powerful deterrent.

Education Process

- All students will have access to the I-SAFE Gold Curriculum for a comprehensive approach to online safety. K-12 students will be exposed to a variety of topics including digital literacy, cyber citizenship, identity protection/reputation, cell phones/texting, cyber security and predator identification. All students will learn online safety, security and responsibility.
- The curriculum will be implemented through a tiered approach. The School Technology Coordinator will receive comprehensive training on the implementation and management of the I-SAFE Gold Curriculum. The STC and School Leadership will then design an implementation model that best suits the needs of the school and ensures that all students receive training in all features of this program.
- Assessment and reporting features of the ISAFE program will be conducted at the school level from which school and district administrators can monitor the implementation of the program.
- Implementation of this program is a mandate of the FCC Child Internet Protection Act (CIPA), Senate Bill 230, and Schools and Libraries E-RATE discount grant as well as other state and local policies. I-SAFE reports will track educators' usage of the curriculum in their classrooms and will provide valuable documentation for compliance audits.

VIDEO, AUDIO, AND MEDIA PRESENTATIONS

On occasion, it may be necessary for school administration to provide video/audio presentations containing visual representations and/or sound recordings of student/staff for public viewing. The means may include

News Media, Public Television, New Letters, Radio, Training Videos, School Internet Web Pages, Social Media, and other related school and or district projects to be used for instruction, research, and school administration.

By signing the agreement and/or parent permission form, the student or staff member has agreed to allow identification and or publication of their name, photographic or video image and/or voice for purposes of recognition, celebration, and or other school/district related events.

TELECOMMUNICATION DEVICES

PERSONAL TELECOMMUNICATION DEVICES

A personal telecommunications device is defined as a device that emits an audible signal, vibrates, displays a message, takes a picture, causes a disruption of the learning environment, or otherwise summons or delivers a communication to the possessor, including but not limited to a cellular telephone, mp3 player, IPAD, or IPOD, or Tablet PC.

Acceptable use for any personal telecommunications device shall be for instructional purposes only with the approval and supervision of school staff. Otherwise, students shall keep personal telecommunications devices out of sight and shall not activate nor use such devices either during the instructional day or while attending or participating in school-related activities held during the instructional day.

For these purposes, the instructional day shall be defined as the first bell of the day through the last bell of the day. The Board does acknowledge the authority of the school council to alter this definition to better serve the needs of individual schools.

Students shall not use personal telecommunication devices and other related electronic devices, in a manner that disrupts the educational process, including, but not limited to, use that:

- Poses a threat to academic integrity, such as cheating,
- Violates confidentiality or privacy rights of another individual,
- Is profane, indecent, or obscene,
- Constitutes or promotes illegal activity or activity in violation of school rules, or violates the District's Acceptable Use Policy or Student Code of Conduct
- Constitutes or promotes sending, sharing, or possessing sexually explicit messages, photographs, or images using any electronic device.

Device contents, while generally private, may be searched under certain circumstances including, but not limited to, reasonable suspicion of threat of safety, violation of confidentiality, or privacy rights of another individual, and may result in a report being made to law enforcement.

Upon violation of this policy, students are subject to discipline as outlined in the Student Handbook and Code of Conduct. Floyd County Schools shall not be responsible for the loss, damage, or theft of any personal telecommunications device

Any form of VPN (Virtual Private Network) found to be in use on a personal telecommunication device in the effort to bypass the district's web filtering service can result in that device being banned or "blacklisted" from accessing the district's network and internet service without prior notice.

TELEPHONE AND OTHER VOICE SYSTEMS

Floyd County Schools, in compliance with KERA, has installed Voice Systems (Telephones) in all schools. Every classroom is equipped with a handset and voice port connected to the school voice system. The district also has issued cellular phones to appropriate staff.

- The school, classroom, and cellular telephones are designed to aid and support the educational instructional process and should not be used for personal, public, private or commercial purposes. To protect the instructional process, students and staff, no telephone calls from outside the school shall go directly into the classroom.
- All SBDM will adopt policies and develop specific procedures on how the school will address telephone calls or messages (Voice mail, secretary messages, etc.) to and from the classroom including student/staff use of cell phone and text messaging during school hours of operation.
- All SBDM will adopt policies and develop specific procedures for student use of voice (telephone) systems and cell phone use and text messaging.

PREPARATION OF EDUCATORS

Teachers and others whose duties include classroom management and/or student supervision should be provided with guidance on detecting, deterring, and documenting inappropriate use, on safe-guarding personal privacy, and on dealing with unsolicited online contact as a school safety issue.

RESPONSIBILITY OF USE

Individuals shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care.

Individuals bringing privately or personally owned computers/software/peripherals into the Floyd County School System, it shall be the responsibility of the owner for its transportation to and from and for its security while on school property.

Floyd County School System will not be liable for damages, loss, theft, or vandalism of such equipment.

DETERRENTS

To manage the student or staff member, who is determined or occasionally tempted to violate acceptable use policies, certain deterrents can be put in place:

Certain network management software packages allow the systems administrator to view or intervene and "take over" a user's screen. These packages are designed for problem diagnosis, to troubleshoot network problems, and to support help desk activities. Although they are not designed to scan network activity for inappropriate use, the district may decide to use them for that purpose on an occasional basis. Regardless, if the user is informed that such scanning is feasible that fact alone may deter inappropriate use. With implementation of web filtering services, schools should familiarize parents, students, faculty, and staff with the information contained in web filter logs. The fact that these logs contain detailed information about Internet access, which can be traced to the individual user usually, serves as a powerful deterrent.

Disciplinary Actions and Other Consequences

All users and all parents will be informed of the consequences of violating appropriate use policies. Consequences will be conveyed via Code of Conduct user agreement and during initial training. Generally the consequences will be one or more of the following:

- Loss of Access
- Disciplinary Action (Code of Conduct)
- Legal Action

NOTICE OF POLICY

Notice of this policy, along with the disciplinary penalties for violation, shall be published annually in the district's Student Handbook and Code of Conduct and presented publicly via means of Floyd County Board Meeting.

TELECOMMUNICATIONS, INTERNET, E-MAIL, VIDEO AND AUDIO EMPLOYEE RESPONSIBILITIES AND RULES FOR TECHNOLOGY USE

Before supervising student use of Internet / E-mail or Video, media specialists/teachers/staff/admin will:

- Receive training on ethics that includes acceptable use
- Confirm that all students have a signed Access User Contract with permission on file in the school.
- Teach and discuss with students the rights and responsibilities of using electronic telecommunications.
- Teach and discuss with students the importance of responsibility and monitoring themselves.

- Help students define acceptable behavior and develop their own sense of responsibility.

*All substitute teachers must complete training that includes acceptable use of Internet/e-mail before they will be allowed to supervise student use of Internet/e-mail.

*All students must complete training on acceptable use of Internet, e-mail, and Video in addition to Code of Conduct review before using Internet, e-mail, or Video.

FLOYD COUNTY PUBLIC SCHOOLS
TELECOMMUNICATIONS, INTERNET, E-MAIL,
VIDEO AND AUDIO
EMPLOYEE AND BOARD USER ACCESS CONTRACT

I have read the ACCESS RULES FOR TELECOMMUNICATIONS, INTERNET, E-MAIL, VIDEO AND AUDIO. I agree to follow and abide by the stated rules of use. I understand that I am responsible for my own personal behavior, and violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, I understand my access privileges may be revoked, disciplinary action taken, and/or appropriate legal action initiated. I will agree to complete ethics training including acceptable use before using or supervising student use of Internet/e-mail. I understand that this contract, once signed, shall be kept on file for the duration of my career at Floyd County Schools unless otherwise dictated by policy change or termination of employment.

Name (Print name here): _____

Signature: _____

Date: _____ School/Work Location: _____



Floyd County Schools
Student & Guardian Technology Integration
Implementation Pledge

Student Implementation Pledge

Student:

- I accept responsibility for the care and protection of my device.
- I accept responsibility for the care and protection of a "loaner" device assigned to me.
- I will bring my device to school every day and ensure my device is fully charged and ready to use daily.
- I will complete my digital citizenship pledge (Pre K-4) or Digital Driver's Licenses (5-12), model appropriate online behavior, and demonstrate that I understand that my device is for educational use only.
- I will always supervise my device or leave it in a secure location.
- I will carry my device in my assigned case and ensure that no food or drink is around my device.

- I understand I am responsible for backing up all data on my device.
- I will report loss, theft, and/or malfunction immediately.
- I will not change the appearance of my device with drawings or stickers and I will keep identifying codes on my device.
- I understand that my device is subject to inspection at any time without notice and remains the property of the Floyd County Public Schools.
- I will follow the policies outlined in the Device Handbook and the Acceptable Use Policy at all times.
- I agree to return the device, case, and power cords in good condition at the end of the school year or if I terminated enrollment at FCS for any reason.
- I have read, understand, and agree to the Acceptable Use Policy (AUP) for the Floyd County Schools.

Parent/Guardian:

As the parent(s) or guardian(s) of _____, we have read, understand, and agree with the requirements outlined in this Technology Integration Handbook, Student Implementation Pledge and the Floyd County Acceptable Use policy. Additionally, we agree to support the digital conversion initiative by monitoring the use of the device while at home.

We will:

- Investigate and apply parental controls
- Develop a set of rules/expectations for laptop use at home.
- Only allow laptop use in common rooms of the home (e.g. living room or kitchen) and not in bedrooms
- Demonstrate a genuine interest in what my student is doing on the laptop. Ask questions and request that they show us their work often.
- Ensure students bring the device to school daily fully charged.
- Ensure the student turns the device in at school before summer break or participates in the buy-back program at the end of the 8th & 12th-grade years.
- I have read, understand, and agree to the Acceptable Use Policy (AUP) for the Floyd County Schools. I agree with all requirements outlined in the Technology Integration Handbook, Student Implementation Pledge, and Acceptable Use Policy.

Student Name (Please Print): _____

Parent/Guardian Name (Please Print): _____

Student Signature: _____

Parent/Guardian Signature: _____

Date: _____

Date: _____