IRWIN COUNTY SCHOOLS

Technology Use Handbook and Agreement

For Students and Parents

Updated 7/10/20

Mission:

The Mission of the Irwin County School System is to **CARE** – **C**ollege and Career **R**eadiness – **A**cademic Support – **R**elationships – **E**xcellence

Vision:

Our Vision is to embrace innovation, initiate positive change, and provide an equitable and excellent educational opportunity that prepares all graduates for success in their endeavors

Beliefs

We believe:

- All children can learn
- Children learn in different ways and at different rates
- Students learn best when they are actively engaged and assume ownership for their learning
- Students generally perform at a higher level when high expectations are clearly communicated
- Students need to know that their teachers care about them as unique individuals
- The first five years of life are critical to a child's development and future success
- Teachers should be passionate about their work and the students they teach
- Teacher morale affects teacher effectiveness
- Educators should have high expectations for themselves and their students
- The school should ensure a safe environment for all
- Parents should be active participants in their child's education and in their schools
- The community should expect their schools to provide a high quality educational experience and should be willing to provide the resources necessary

The procedures and information within this handbook apply to all student devices in Irwin County Schools during the school day and outside of the school when applicable. Devices are property of Irwin County Schools (ICS) and are intended to follow the guidelines established by the district for educational use. All students should complete these forms (whether in face-to-face school or virtual school). In the case of a school shutdown, devices can be issued for at home use if these forms are on file.

As in all situations, guidelines and procedures must be established in order to ensure the devices are used properly and handled with care.

Teachers may set additional requirements for use of school owned devices in their classrooms, as well as personal laptops, tablets, and cell phones.

Irwin County School District
Acceptable Use Policy

Introduction

The Irwin County School District believes that using computer resources should be an enjoyable and educational experience. Therefore, the school district provides computing facilities to faculty, students, and staff for educational activities. This policy mandates responsible behavior by individuals given access to these facilities and recognizes the district's responsibility to promote the safety and security of these users.

Since the Internet opens up the world to unrestricted access, the district cannot assume the responsibility for monitoring every document to which a user may gain access. Therefore, the district is not to be held accountable for what the user may access through the Internet beyond instructional directives.

To the extent practical, the Irwin County School District shall take steps to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

In order for students to use the available technology and access the Internet, parents must read this policy with their child(ren) and indicate acceptance of the policy by their signature on the Internet Usage Permission Form. Students in grades four through twelve must also sign the permission form.

Definitions

- **Computing resources** include computers, as well as peripherals, networks, software, data, labs, computer-related supplies and the Internet.

- **Technology Protection Measure** means a specific technology that blocks or filters Internet access to visual depictions that are: (1) Obscene, as that term is defined in section 1460 of title 18, United States Code; (2) Child pornography, as that term is defined in section 2256 of title 18, United States Code; or (3) Harmful to minors.

- **Harmful to Minors** means any picture, image, graphic image file, or other visual depiction that: (1) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) 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 (3) Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

- **Sexual Act and Sexual Contact** have the meanings given in section 2246 of title 18, United States Code.

General Policies Regarding Use of Technology

The use of technology and access to the Internet is a privilege, not a right. Inappropriate use will result in a cancellation of those privileges. In addition to the following guidelines, the administration will deem what constitutes inappropriate use.

- Intentional abuse of computing resources, intentional interference with the operation of computing resources or wasting of computer resources is prohibited. This includes, but is not limited to, the uploading or creation of computer viruses.

- Intentional interference with or destruction of the work of other users is prohibited.

- Users shall not violate confidentiality, copyrights, or license agreements.

- Actions that attempt to circumvent prescribed channels of obtaining computer privileges and resources are prohibited.

- Changing wiring, connections, or placement of computing resources is prohibited.

- Modifying any system configuration, startup files, or applications without the explicit permission of the lab supervisor, teacher, media specialist or technologist is prohibited.

- Reporting improperly working equipment or software is highly encouraged so that computing resources can be better maintained for efficient availability.

- Using computing resources for commercial purposes is prohibited.

- A user may not use or download any software to school computers without permission of the school's technologist.

- All external storage devices (CDs, floppies, etc.) brought to the lab or library to be used in the computers must first be scanned for viruses by the teacher/librarian.
- Under no circumstances shall students, employees of the school system, or any individual exhibit or disseminate obscene/offensive materials on school property by computers or any other means.
- Under no circumstances shall students, employees of the school system, or any individual communicate by way of threatening material in a manner that could be construed as cyberbullying or directly threatening bodily harm and/or illegal activity.

Terms and Conditions for Use of Internet

Internet access has been made available to students and staff. This access offers vast, diverse, and unique resources to both students and staff. The goal of providing this service is to promote educational excellence by facilitating resource sharing, production, innovation, and communication.

Internet users are personally responsible for their use of the Internet. These guidelines are provided so that users are aware of these responsibilities.

- All students must have an Internet Usage Permission Form, signed by their parents, that authorizes them access to the Internet.
- Students are to notify the teacher/librarian immediately of any security problem or inappropriate material they may encounter on the web or in email. Inappropriate material should not be demonstrated to other users.
- Students are not to give out their own or others' personal information like telephone numbers, full names, addresses, etc. to anyone on the Internet.
- Students should not give anyone their password or allow another person to use their account to access the Internet or school network.
- Students must gain clearance from the teacher/librarian before downloading any programs from the Internet.
- Students must gain permission from the teacher/librarian to utilize personal devices brought to campus. All supplementary activities involving the use of personal devices, social media, chat rooms, etc. must be conducted under the permission and supervision of system personnel.
- Adherence to generally accepted rules of network etiquette (*netiquette)* is required. This includes but is not limited to the following:
    - Be polite. Abusive messages to others will not be tolerated.
    - Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.

- Illegal activities are strictly forbidden. Messages relating to or in support of illegal activities, cyberbullying, and other equally offensive activities should be reported to system personnel and proper authorities.

- Electronic mail (e-mail) is not private. System administrators have access to all mail.

- All communications and information accessible via the network should be respected as private property.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter access to inappropriate information received through the Internet or other forms of electronic communication. As described in the district's technology plan, the district currently uses blocking and filtering software and hardware to ensure the safety and protection of the users.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled; or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Enforcement

Violating any of the guidelines of this policy can result in:

- Restricted access to computing facilities and equipment.

- Temporary or permanent loss of access to computing facilities and equipment.

- Disciplinary or legal action including, but not limited to, criminal prosecution under appropriate state and federal laws.

- Users being held responsible for the replacement costs of hardware or software due to damage through misuse or abuse.

In addition to local policy requirements, Georgia law O.C.G.A. 16-9-90, which may be cited as the Georgia Computer Systems Protection Act, also provides definitions, criminal liability and penalties for the crimes related to computer theft, computer trespass, computer invasion of privacy, computer forgery and computer password disclosure. Commission of a computer crime under O.C.G.A. 16-9-90 carries the possible penalty of a fine not exceeding $50,000 and/or incarceration for a period not to exceed one year. Property laws covering theft, vandalism, destruction and copyright also apply to computing resources.

Violation of state law and/or federal law can be reported to proper enforcement authorities. Irwin County School District's internal procedures for enforcement of its policies are independent of possible prosecution under the law.

Adoption

The CIPA-Compliant Internet Safety Policy and the Acceptable Use Policy were adopted by the Irwin County Board of Education at a public meeting following normal public notice.

CIPA Compliance

In compliance with the Children's Internet Protection Act (CIPA) and as outlined in the district's technology plan, Irwin County is currently using software and hardware for filtering/blocking measures to ensure the safety and protection of the users.

Responsible Use and Procedures for Devices

Distributing Student Devices for Home Use

Before the devices are distributed to students, the following items must be completed at the beginning of the year.

Parent/guardians and students must both acknowledge and consent to the *Student Device Responsible Use Agreement* form and the *Internet Usage Permission* form before the device is distributed. The agreement will be part of the registration/orientation process at the beginning of the school year.

Device Use and Care at School and Home

Student devices are school property and all users will follow the *Technology Handbook and Agreement*, and the *Student Code of Conduct*. Students are responsible for the general care of the device that has been issued to them by the school. Students will be taught how to properly handle and care for the device. **If a device is damaged or fails to work properly, it must be reported to school personnel as soon as possible.**

1. **Device Identification**
   Student devices will be labeled as specified by ICS. Devices can be identified in the following ways:
   - Serial number
   - ICS asset tag (silver and purple)
   - Media Center Barcode & Student Name attached to device by school personnel.

2. **Device Care**
   - Do not place anything on or near the device that will press against the screen.
   - Do not lean on top of the device when it is closed.
   - Do not bump the device against lockers, walls, car doors, floors, etc. as it could eventually break the screen.
   - Do not carry your laptop by the screen. Lid should be closed when not in use.

- Never pile things on top of it.
- Keep the device in the center of the desk, not on the edge.
- When closing laptop screen, pay special attention to papers, notecards, pencils, and other items that may get overlooked when closing the screen.
- ONLY use a lint free, microfiber, or soft cotton cloth to clean your computer screen. Do not use bathroom tissues or paper towels because they will scratch the screen.
- NEVER spray any cleaning chemicals such as Windex or other glass cleaners directly on your screen.
- Never leave the device unattended.
- Always carry the device with two hands.
- Follow all directions given by the teacher.
- Do not place device on floor.
- When charging cord is being used, make sure it is properly secured.
- Keep ALL food and drinks away from your device at all times.
- DO NOT leave the device in a vehicle or outside area.
- Devices should not be placed near magnets; magnets may damage computerized equipment.
- Devices should not be exposed to direct sunlight, excessive hear, or severe cold temperatures.
- Cords should be inserted carefully into the device to prevent damage and stored in a way that does not stress the cords.

3. **Home Use Guidelines**
    - Questions often arise regarding the use of the devices at home. THIS DEVICE IS FOR ACADEMIC USE ONLY. All school district rules apply for home use of devices.
    - Keep the device and charging cord away from pets, extreme heat or cold, food and drinks, and small children.
    - Designate a safe location off the floor where your device can be stored and recharged each evening, such as a desk or table.
    - Charge the device fully each night.
    - Students are encouraged to secure their device in a padded case.

Remember, all repairs MUST be done by ICS Technology Department. Never try to repair a device yourself. If you have trouble with your device at home, notify your teacher immediately to report the problem.

Prohibited Actions

Students are prohibited from:

- Listening to music or viewing movies on school devices.
- Downloading any type of media content to your device.
- Putting stickers or additional markings on the device, batteries, or power cord/chargers.
- Defacing ICS issued equipment in any way.
- Inappropriate pictures may not be used at the lock-screen and/or wallpaper. Inappropriate pictures include, but are not limited to, presence of weapons, pornographic materials, inappropriate language, tobacco, alcohol, drug, gang-related symbols or pictures.

Any of these actions on the device will result in disciplinary action per ICS Student Code of Conduct. Consequences will be determined by school administration.

Home/Off Campus Internet

Students are allowed to access wireless internet networks on their devices. ICS provides internet filtering outside of the district's network as a courtesy, but no system is foolproof. These filters ensure that the content retrieved online by students align with Federal and State guidelines for Internet use in school and coincide with the *Children's Internet Protection Act (CIPA)*. Parents/Guardians are responsible for online activities and behavior of their children while away from school.

If connecting to Internet off campus, please remember,

1. **Home Internet Service Provider (ISP) -** There are many Internet service providers. Each one has their own equipment (modem, cables, wireless routers etc.) For help with your wireless Internet at home, please contact your provider for technical support.
2. **Public Internet Access -** Many public places provide free public wireless access. Most will display a sign advertising this service. Many businesses do this as a way to attract business. If you are using free internet access, it is considered good etiquette to either purchase something at the business or thank the business for the service. Examples of free wireless networks may include: restaurants, churches, schools, hotels, libraries, and some communities. Often public locations require that you accept an Acceptable Use Policy (AUP) which states you will not try to do anything illegal or harmful before they will allow you to access their network.
3. **Internet Settings -** When connecting to a free wireless network, be sure it is sponsored by someone you trust. Once you join a wireless network, it is possible for those with malicious intent to try to access your device with the intent of doing harm to your device or trying to access and steal your information. Most businesses who share Internet are prepared and protect you by not allowing users to access each other on the network.

ICS devices are set up to access the Internet before they are given to students. Making changes to the Internet settings is not allowed and can prevent your device from working while at school and/or home. **No additional software** should be added to school devices. This includes networking software.

Managing Files and Saving Documents

1. Saving to Student Device—It is the student's responsibility to ensure that work is saved properly in the correct location as instructed. All work can be saved in the student's Google Drive.
2. Network Connectivity—ICS cannot guarantee that the District network will be up and running 100% of the time. When the network is down, the District will not be responsible for inaccessible, lost, or missing data. When students save documents as instructed, this will not be a problem.
3. Media Stored on Devices –The student device has limited storage. Inappropriate content is NOT allowed on the device. The device storage is for educational use. If non-educational or personal content is on the device and storage space is needed, students must delete the non-educational content, so they have space for their school work.

Operating Systems and Applications

1. District-Installed Apps—Apps installed by ICS must remain on the device in working condition and be easily accessible at all times. From time to time, the school may add apps for use in a particular course.
2. Additional Apps –All devices are initially deployed with a set of basic apps. Students will follow the established procedures when instructed by their teachers to install required apps.
3. Operating System and App Updates—Updated versions of the operating system and apps are available from time to time. The District will provide and maintain updates for the operating system and/or apps. Some updates may require student intervention, such as clicking "ok" or rebooting the machine.

Damaged, Lost, or Stolen Devices

1. Damaged Devices
   Students should notify their teacher, or the IT department immediately. DO NOT WAIT! You can call the school or send an email. Include your name, grade, asset tag number, and description of the problem or damage to the device. Students should never attempt to repair devices. All necessary repairs will be made by the district's technology department.

   IT Department:

Corey Phillips	cphillips@irwin.k12.ga.us
Travis Hutto	thutto@irwin.k12.ga.us

2. Violations and Consequences
   The violations and consequences outlined by this Student Device Responsible Use Handbook and Agreement are listed below. Disciplinary actions will be decided upon by the school administration.

Technology Device Violations	
First report of damage or neglect to equipment	$40 Fee & discipline action
Second report of damage or neglect to equipment	$60 Fee & discipline action
Third report of damage or neglect to equipment	$80 Fee & discipline action

Some examples of damage or neglect:

- Marks or dents beyond normal indicating device has been dropped and was not handled with care
- Writing on the device
- Stickers or other objects attached to the device
- Dirty screen or laptop
- Device screen cracked or detached keyboard
- Keys removed or damaged
- Mouse pad broken

Lost or Stolen Devices

A lost or stolen device MUST be reported to the school administrator, or teacher immediately. If a device is lost or stolen at any time outside of school, parents should take the following steps:

1. Contact the police right away to file a claim for lost/stolen property. Be sure to get a copy of the report for the school, which will include a case number and/or incident number from the officer.
   a. Ocilla Police Department Phone: 229-468-7494
   b. Irwin County Sheriff's Office Phone: 229-468-7459

2. Contact an administrator at your child's school during school hours at number below. Be ready to provide them with the case and/or incident report number which you obtained from the responding officer.

   ICES:
   Call 229-468-9476
   Email Principal-Mrs. Barnes: rfbarnes@irwin.k12.ga.us

   ICMS:
   Call 229-468-5517
   Email Principal-Mr. Tucker: atucker@irwin.k12.ga.us

   ICHS:
   Call 229-468-9421
   Email Principal-Mr. Haskins: shaskins@irwin.k12.ga.us

3. When a device is stolen, ICS administration will investigate to determine if the student and their parent/guardian will be held responsible for full payment for the replacement of the ICS device ($250-$300). If a device is lost, the full payment will be required from the student and their parent/guardian.

Technology Support

Each school has several staff members who are able to provide technical support. However, before you seek help, students will be taught some simple steps to follow. Examples are below:

- Computer Frozen – hold the power key down for 10 seconds and restart
- Application Not Working – close app and restart the device
- Can't Connect to Internet – check wireless connection, rejoin network if needed; Restart
- Broken or damaged devices should be reported to the school immediately for repair.

Internet Safety

Tips for Students and Families

- Keep the device where everyone can see the computer screen.
- Do not post personal information online; beware of requests for personal information online.
- Teach your child how to recognize and avoid online predators.

- Report strangers who solicit information or meetings with any child.
- Do not be a Cyberbully! Report cyberbullying and threats to the school immediately.
- Honor the ICS security software and filters.
- Do not give out personal information such as your name, address, telephone number, and current location without the permission of parents.
- Tell your parents right away if you come across information on the Internet that makes you feel uncomfortable.
- Never agree to get together with someone you "meet" on the Internet.
- Do not respond to any messages that are mean, rude, or make you feel uncomfortable in any way. If you do get a message that worries you, frightens you, or makes you feel uncomfortable, tell your parents about it right away.
- Talk to your parents about the rules of your household concerning how and when you use the computer and access the Internet.

Technology Responsible Use and Digital Citizenship

Statement of Responsibility

The use of student devices and the network is a privilege. The student is responsible for what he or she says and does on the network. It is important for the user to stop and think before communicating and to show respect for others and their ideas. Students must assume that none of their data is private or confidential. Any communication or data may be subject to review by district and/or school administration. Periodic checks may be made by designated staff to ensure that students have not removed required apps or added inappropriate content.

Parent/Guardian Responsibilities

It is expected that Parents/Guardians talk with their children about digital citizenship. This includes discussing the dangers and consequences of cyberbullying, inappropriate use, and other misuses of the Internet. Parents/Guardians must expect their child to use technology appropriately at school and at home. Parents will also be responsible for providing internet access for at-home use.

School and District Responsibilities

- ICS provides internet access to its students at school.
- ICS provides internet filtering/blocking of inappropriate materials in compliance with the Children's Internet Protection Act (CIPA) while using ICS devices.
- ICS reserves the right to review, monitor, and restrict information stored on or transmitted via district owned equipment and to investigate inappropriate use of resources.
- ICS schools will provide device instruction and guidance to students and encourage student adherence to the ICS Technology User Agreement and the ICS Technology Acceptable Use Internet Agreement.
- Student devices may be selected at random for remote or physical device inspection by any staff.

Student Responsibilities

- Students will use ICS technologies in a responsible and ethical manner.
- Students will follow district rules concerning behavior and communication using the district network.

- Students will use all technology resources in an appropriate manner which will not damage school equipment. “Damage” includes, but is not limited to, the loss of data resulting from delays, non-deliveries, or service interruptions caused by the student’s own negligence, errors, or omissions.
- Use of information obtained by the ICS network is at the student’s own risk. The district denies any responsibility for the accuracy or quality of information obtained through the ICS network.
- Students will help ICS protect the district network and devices by contacting school personnel about any security problems they encounter.
- Students will not share their username/log in credentials or passwords with others.
- Students will not allow others to use their assigned device.
- Students will monitor all activity on their school account(s).
- If a student should receive an electronic message containing inappropriate or abusive language, or if the subject matter is questionable, he/she will inform a teacher or other staff member (and if applicable print a copy and turn it into school personnel; or screen shot it and email it to the teacher or administrator).
- Students will turn in the device to their school at the end of each school year, unless specifically authorized by the district, to do so earlier.
- Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment in ICS for any reason, must return the device on the date of termination. The district will report the device as stolen if not returned as described above.
- Students will mute the sound on their device during the instructional day unless otherwise permitted. Headphones or earbuds may be allowed or required for certain applications and settings.

Collecting Student Devices (At-Home Use)

- Device accessories (such as charging cords, cases, & electronic pens) that are furnished by the school must be returned at the end of the school year, with only normal wear and no device modifications.
- Teachers will check student devices *multiple* times during the school year and will report any signs of damage to school administrators and the district technology dept.
- If a student transfers, withdraws, is suspended or expelled, or terminates enrollment at ICS schools for any reason, they must return the device with all accessories on the date of termination. If the device is not returned, it will be assumed the device has been stolen. Action will be taken by the ICSSSSS District to reclaim the device and accessories.