

# ***ECHOLS COUNTY SCHOOLS***

## ***TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY AGREEMENT***

### **Employee 2023 - 2024**

#### **Introduction**

*Please read carefully.*

Echols County Schools agrees 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)]. Employees must also adhere to the Georgia Code of Ethics for Educators (<http://www.gapsc.com/rules/current/ethics/505-6-.01.pdf>).

The intranet/internet is an electronic communications network delivery via computer and telephone line. A vast number of resources are accessible locally, nationally, and internationally. The goal of the Echols County Board of Education is to provide this service to teachers, staff, and students to promote educational excellence and to facilitate resource sharing, innovation and communication. In an attempt to aid the students and staff in a better understanding of proper computer, network and Internet safety, the following agreement is set forth. This agreement does not purport to be an all-inclusive list of inappropriate behaviors. Violation of the following rules will not be tolerated. Each user is responsible for all actions and activities involving the computers and the network. Violations of the Employee Acceptable Use Agreement may result in revocation of employee's access privileges, Board of Education disciplinary action (including employment termination), and possible law enforcement authorities and/or Georgia Professional Standards Commission.

#### **Guidelines**

Internet access is coordinated through a complex association of government agencies and regional networks. Intranet access is coordinated through the individual school. The operation of the intranet/internet relies heavily on the proper conduct of the users, who must adhere to strict guidelines. To protect users against access to inappropriate materials, Echols County Schools has installed a qualifying "technology protection measure" as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000 (CIPA). This firewall and filtering program is designed to aid in the prevention of access to visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors as those terms are defined in Section 1703(b)(1) and (2) of the CIPA of 2000. This program filters and blocks only known sites that feature nudity, pornography, violence, hatred of others, inappropriate chat rooms, and inappropriate language. This list of restricted sites is updated daily; however, inappropriate sites are published frequently during the day and no filtering software has proven to be 100% effective.

#### **Employee use of system technology resources:**

##### **Inappropriate conduct includes but is not limited to the following:**

- Employees will not use district computers and laptops to copy or download copyrighted software, music or images, or for other violation of copyright laws. Peer-to-peer, file-sharing, torrent software may not be installed on a school system computer or laptop.
- Accessing or using the Internet for inappropriate materials that are damaging to another person's reputation, abusive, illegal, obscene, sexually oriented, threatening or demeaning to another person's gender or race, violation of the school's agreement on harassment. Accidental access to any of this material must be reported immediately to the Technology Director.
- Purposely infecting any school computer or network with a virus or program designed to damage, alter or destroy data.
- Invading the privacy of other individuals by gaining unauthorized access to their files or documents.
- Using or attempting to use another person's user name or password.
- Posting or plagiarizing work created by another person without their consent.
- Posting anonymous messages or the sending of inappropriate, private or direct message to students using social networks such as Facebook or Twitter--see eBoard policy IFBG-R(2).
- Online gaming and related activities is not an acceptable activity for staff members to knowingly engage in with students.
- Using the school's computer hardware, network or Internet links while access privileges are suspended.
- Attempting to alter the configuration of a computer or any of the software of the school.
- Personal equipment is not allowed nor supported at Echols County Schools.
- Employees and approved volunteers may not establish an Echols County School District social media site without the permission of the Echols County Board of Education. Board of Education approved meeting minutes will serve as

documentation stating the social media site that is to be created, purpose of the site and the person(s) responsible for maintaining the site.

## **Hardware**

- ❑ Personal equipment is not allowed to be connected to the wired network nor supported at Echols County Schools (exceptions to be considered for academic purposes only). Any deviation from this agreement must be presented to the Technology Director.
- ❑ Attempts to replace or repair hardware without permission from the technology department is not permitted.
- ❑ School district technological resources are provided for school-related purposes. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning. Use of school district technological resources for political purposes or for commercial gain or profit is prohibited. Personal use of school district technological resources for amusement or entertainment is also prohibited.

## **Security**

- ❑ Any security problem must be reported to the Technology Director.
- ❑ Users will not show or identify a security problem to others.
- ❑ Users will not reveal their password or allow another person to use their password.
- ❑ Users will not use another individual's password.
- ❑ Users will not attempt to log on as another user.
- ❑ Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

## **Expectations and Acceptable Use**

- ❑ Usage must be in support of education and research consistent with board policy.
- ❑ Pictures of students for use by the district is covered in the section “News Media Coverage, School District/School Publications and Websites” below
- ❑ Personal information with regards to faculty and staff will not be divulged on the school web site. Contact information may include a name, position, and school phone number from the teacher, support staff or administrator web page.
- ❑ Use internet sites related to academic assignments. Gaming and other sites could infect the computer with malware or spyware.
- ❑ Student access to the intranet/internet will be under the supervision of a faculty or staff member. The faculty or staff member will be aware that the filtering system is not 100% effective and requires vigilant monitoring and correction of student activity.
- ❑ Any materials being displayed to student through the Internet must be carefully reviewed in their entirety and related to instructional objectives.
- ❑ School system software installations are to be requested through the Technology Department. Personal software or applications are not installed on school system computers or devices.
- ❑ Each user is responsible for storing school related files on the server.
- ❑ Users will not share or reveal their password or allow another person to use their password. Never allow a student or another staff member to login with a staff member’s username and password. Remember, this would allow the person access to email and private documents under the home directory. Make sure others do not see you enter your password. If you feel your password has been compromised, contact the Technology Director. Do not leave written passwords lying on a desk or in an unlocked drawer.
- ❑ Login with their school system assigned username and password. Do not post or display login information as this is confidential information.
- ❑ Students are to be supervised at all times when using a computer, laptop or mobile device. Do not allow students to use computers or computer labs unsupervised.
- ❑ Email accounts are provided to employees of ECS. Electronic mail is not guaranteed to be private. Email accounts should not be used for personal gain or to promote personal business activities. Employees should conduct themselves in an appropriate manner representing Echols County School System. Personal email accounts are not supported by ECS and are not accepted as a method of communicating the students or parents. Emails should be written in a professional manner with regards to word selection, tone, grammar and subject matter.
- ❑ Employees are responsible for making sure all external devices are virus free and that the device does not contain any inappropriate files. Students are not allowed to bring external devices for use on the school network.
- ❑ Live streaming of video and audio (streaming media) must be for academic instruction.

## Email Accounts

- Login with the information provided by the district
- Do not select to “Remember password” on the login screen or at any other login
- Violations that relate to the Technology Acceptable Use and Internet Safety Agreement and Employee Ethics Standards according to the PSC will be submitted to the school administrator to determine appropriate action.
- The district purchases a service that scans Office 365 Outlook email (inbound and outbound) and Office 365 documents for compliance in cyberbullying, FERPA, CIPA, violence, child abuse, objectionable content policies language indicating cyberbullying, violence to self or others, objectionable content, child abuse, and CIPA.
- All district emails and attachments are archived and retained and scanned for threat protection. Save important documents to your network drive on the server.
- Employee accounts are able to communicate with student district email accounts for academic reasons.

## Penalties

Any user violating these provisions, applicable state and federal laws, posted classroom rules (students) or system policies is subject to loss of network privileges and any other District disciplinary options, including criminal prosecution. Illustrations of disciplinary options are contained in the Teachers’ Handbook and Students’ Handbook. Intranet/internet access is a privilege, not a right. If a system user violates any of the acceptable use provisions outlined in this document, his/her account may be terminated and future access may be denied. Some violations may also constitute a criminal offense and may result in legal action. Any user violating these provisions, applicable state and federal laws, or posted classroom and district policies, is subject to loss of access privileges and any other Board disciplinary options.

The Technology Director will recommend to the Superintendent the determination as to what constitutes unacceptable use and the decision by the Superintendent is final. The employee shall be responsible for compensating the school system for any losses, costs, or damages incurred by the school system relating to or arising out of the users’ violation of this agreement.

## Warranty

Echols County Schools makes no warranties of any kind, whether expressed or implied, for the technology resources it is providing. ECS will not be responsible for any damages you suffer. This includes loss of data resulting from hard drive failures, mail delays, non-deliveries, or service interruptions caused by system negligence or by your errors or omissions. Use of any information obtained via the Internet is at your own risk. ECS specifically denies any responsibility for the accuracy or quality of information obtained through its technology resources.

ECS may not at any time be held responsible for any loss or damage to a student’s personal device. Students bring devices at their own risk. Help and support will not be provided for personal devices.

## NEWS MEDIA COVERAGE, SCHOOL DISTRICT/SCHOOL PUBLICATIONS AND WEBSITES

Events and programs in public education are often considered newsworthy and of interest to local communities. Schools often solicit media coverage to publicize successful programs and special events concerning students and faculty. Students may on occasion be interviewed or photographed by the news media for positive school news coverage, or publicly recognized at a School Board meeting or have student work displayed. Additionally, a student’s image (including video), name, or intellectual property may be included in School District publications or school web pages and through social media.

Parents/guardians can **object** to their student being published (print or digital) as mentioned above. The objection must be presented in writing to the principal of the school where the student is enrolled within 10 days after the student’s enrollment date.

If more than one child, a letter must be written for each child and presented to the appropriate school principal. Students will only be **excluded** if written objection is presented to the principal of the school. Each school principal will email the correspondence to the Technology Director for record. The faculty/staff will be notified through email of any objections from a parent/guardian. If there is no written objection turned in to the principal, the district will include the student in all publications.



## MICROSOFT FOR EDUCATION (OFFICE 365)



Microsoft for Education was adopted by Echols County Schools to provide online communication and productivity tools for students and teachers. Microsoft for Education accounts (Office 365) are provided to all faculty/staff and students in grades Pre-K through 12. Active student email accounts are only grades 6-12. Outlook (email) for grades Pre-K through 5 have not been activated at this time. Teachers and students will be able to create dynamic learning experiences in and outside of the classroom with an internet connection. Student will be able to share with teachers and collaborate with peers. MS for Education (Office 365) can be used to develop college and career ready skills of communication, collaboration, creativity and critical thinking.

Echols County School District is providing this notification to the parents of children under the age of 13 so that ECSD can be compliant with the Children's Online Privacy Protection Act (COPPA). The only information ECSD transfers to Microsoft in creating an account is the child's first name and last name.

Employee/Student data will be used only to provide the employee/student the Online Services including purposes compatible with providing those services. Microsoft will not use employee/student data or derive information from it for any advertising or similar commercial purposes. Microsoft provides an overview of their commitment to student security and privacy at <https://www.microsoft.com/online/legal/v2/?docid=31>

When there is reason to believe violations of law or district policies related to the Technology Acceptable Use and Internet Safety Agreement, the district maintains the right to withdraw access to the Microsoft account. Consequences for violations will be determined by the Technology Director and this stated agreement.

### STUDENT RECORDS

It is the policy of the Board of Education that all employees shall comply with the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Pupil Protection Rights Amendment (PPRA). The Board has developed and adopted student privacy policies in consultation with parents in accordance with federal law. Additionally, parents will be directly notified of these policies at least annually via the Student/Parent Handbook issued to students at the beginning of the school year or at the student's time of enrollment.

The Superintendent shall implement procedures whereby every principal is directed to develop a means to notify, on an annual basis, students and parents, including non-English-speaking parents, of their rights under the Family Educational Rights and Privacy Act and the Pupil Protection Rights Amendment, either by letter or through a student handbook distributed to each student in the school.

The Superintendent shall implement procedures whereby every principal is directed to develop a means to include student participation in school sponsored clubs and activities as part of their permanent records.

## **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)**

Confidentiality of student records shall be preserved while access is provided to parents, eligible students (those over eighteen years of age or enrolled in post-secondary educational institutions), professional educators with legitimate educational interests, and those federal or state officials whose access is authorized in connection with an audit or evaluation of federal or state supported education programs or for the enforcement or compliance with federal legal requirements related to those programs. The Superintendent shall direct the publication of procedures through which parents or eligible students may request the correction of errors in student records.

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the school receives a request for access.
  - a. Parents or eligible students should submit to the school principal a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.
2. The right to request the amendment of the student's education records that the parent or eligible student believes is inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.
  - a. Parents or eligible students who wish to ask the School to amend a record should write the school principal, clearly identify the part of the record they want changed and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment (Federal regulation 34 C.F.R. 99.21-99.22 and any state regulations that may apply). Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing. If the school decides not to amend a record in accordance with a parent's request, the school must inform the parent of his or her right to a hearing on the matter. If, as a result of the hearing, the school still decides not to amend the record, the parent has the right to insert a statement in the record setting forth his or her views. That statement must remain with the contested part of the student's record for as long as the record is maintained.
3. The right to consent to disclosures of personally identifiable information (PII) contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.
4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the Echols County Schools System to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

Family Policy Compliance Office  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202-5901

There are several exceptions to the rule regarding the privacy of students' educational records. One exception is that the Echols County Schools may disclose certain "directory information", which is generally not considered harmful or an invasion of privacy if released, without prior written consent unless you have advised the school system otherwise. The primary purpose of directory information is to allow the system to include this type of information from your child's education records in certain school publications. Examples include:

- a. A playbill, showing the student's role in a drama production
- b. The yearbook
- c. Honor roll or other recognition lists
- d. Sports activity sheets showing weight and height of the team members
- e. Graduation programs

"Directory information" may also be included on school, classroom or school system Web sites or blogs that can be downloaded or viewed inside or outside the school system. Additionally, the school system may release this information to the following outside organizations: law enforcement agencies, State and Federal Child Welfare Agencies, District Attorney and Solicitor's Offices, PTA/PTSA, booster clubs, U.S. Armed Forces recruitment agencies, schools and colleges accredited by the Southern Association of Colleges and Schools, and companies the school system uses to manufacture school items such as class rings or yearbooks. If you do not want Echols County Schools to disclose directory information from your child's education records without your prior written consent, you must notify the school principal in writing within ten (10) days of enrollment that such information not be designated

directory information on the individual student. A letter must be received or directory information will not be considered confidential and may be disclosed upon request.

Echols County Schools has designated the following as directory information:

- a. Each student's name, address, email, and telephone number;
- b. The date and place of birth of each student;
- c. Each student's participation in clubs and sports;
- d. The weight and height of a student if he or she is a member of an athletic team;
- e. Dates of attendance at Echols Schools;
- f. Most recent school attended
- g. Teacher or coach assignment
- h. Degrees, honors and awards received while enrolled in Echols County Schools; and
- i. Photographs of students, certain audio recordings or video clips. Not included are any recordings, photos or footage of a student or students committing, witnessing or being involved in a violation of law, school system or school rule, procedure, or policy. The school system may also determine that other images or recordings do not qualify as directory information on a case-by-case basis.

Another exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. A school official is person employed by the School as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the School Board; a person or company with who the School has contracted to perform a special task (such as an attorney, auditor, medical consultant, or therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill is or her professional responsibility.

Other exceptions may include, but are not limited to:

- a. Student records sent upon request of the institution a student has enrolled (within or outside the school district: Georgia Board of Education Rule 160-5-1-.14 Transfer of Student Records)
- b. Disclosures for audit or evaluation of Federal- or State- supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs
- c. Financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid.
- d. State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system.
- e. Organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction.
- f. Accrediting organizations to carry out their accrediting functions.
- g. Parents of an eligible student if the student is a dependent for IRS tax purposes.
- h. Comply with a judicial order or lawfully issued subpoena.
- i. Appropriate officials in connection with a health or safety emergency.

The Uninterrupted Scholars Act (Public Law 112-278) enacted on January 14, 2013, amends the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g; 34 CFR Part 99, to permit educational agencies and institutions to disclose a student's education records, without parental consent, to a caseworker or other representative of a State or local child welfare agency or tribal organization authorized to access a student's case plan "when such agency or organization is legally responsible, in accordance with State or tribal law, for the care and protection of the student." In specified types of judicial proceedings in which a parent is involved, the Act also allows educational agencies and institutions to disclose a student's education records pursuant to a judicial order without requiring additional notice to the parent by the educational agency or institution.

Upon request, the School releases educational records, including disciplinary records and records that were created as a result of a student receiving special education services under Part B of the Individuals with Disabilities Education Act (IDEA), to officials of another school district or postsecondary institution at which the student seeks or intends to enroll. Such release of records will be initiated upon receipt of an official written request on school or district letterhead paper.

## **ACCESSING STUDENT RECORDS**

FERPA gives custodial and noncustodial parents alike certain rights with respect to their children's education records, unless a school is provided with evidence that there is a court order or State law that specifically provides to the contrary. Otherwise, both custodial and noncustodial parents have the right to access their children's education records. A parent will be permitted to obtain a copy of the child's educational records upon reasonable notice.

## **INFORMATION RELEASE**

In the instance of divorce, legal documentation or copy of the divorce decree stating that a parent does not have access to the child or his/her records must be received by the school or the school is obligated to treat both parents as a legal parent with access to the child and the child's records.

Each records custodian in the school district shall maintain a record of each request for access to and each disclosure of personally identifiable information from the educational records of a student in accordance with regulations governing the Act.

## **STUDENT DATA PRIVACY COMPLAINTS**

It is the policy of the Echols County Board of Education that the School District ("District") shall comply with the Family Educational Rights and Privacy Act (FERPA) and the Student Data Privacy, Accessibility, and Transparency Act, which are designed to ensure that education records and student data are kept confidential and secure from unauthorized access and disclosure.

For the purposes of this policy, a "parent" is defined as a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or guardian. An "eligible student" is defined as a student who has reached 18 years of age or is attending an institution of postsecondary education.

Any parent or eligible student ("Complainant") may file a complaint with the District if that individual believes or alleges that a possible violation of rights under the above laws has occurred not more than one (1) year prior to the date the complaint is received by the District.

Complaints shall be handled in accordance with the following procedures.

1. The Superintendent shall designate at least one individual ("Designee") to respond to student data privacy complaints.
2. Upon the receipt of a request from a Complainant, the Designee shall provide within 3 business days a complaint form, which may also be made available on the District's website.
3. A written response shall be provided to the Complainant within 10 business days of the Designee's receipt of the completed complaint form.
4. The Complainant may file an appeal with the Superintendent within 10 business days of receipt of the Designee's response.
5. The Superintendent shall provide a written response to the Complainant within 10 business days of receipt of the appeal.
6. The Complainant may file an appeal to the Board of Education within 10 business days of receipt of the Superintendent's response.
7. The Board of Education shall render a final decision within 10 business days of receipt of an appeal.

Complaint forms are available at each school office and on the district website ([www.echols.k12.ga.us](http://www.echols.k12.ga.us)) under eBoard, Student Policies, JRA-E(1) for Elementary/Middle School and JRA-E(2) for High School.

### ***CIPA Compliance:***

Echols County Schools purchases firewall and content filter service. ECS currently has a Technology Acceptable Use and Internet Safety Agreement which is reviewed annually and updated as situations apply. The current agreement remains in effect until ECBOE approval of any amended agreement during a school term or until the annual agreement/policy review. An updated Technology Acceptable Use and Internet Safety Agreement will be provided for parents and students in the appropriate Student Handbook and on the district and school websites. Any corrections or additions after the Echols County School District Board approval will be provided for parents in the Echols Echo newspaper and on district and school websites.

### **CIPA BACKGROUND**

Full text of the Children's Internet Protection Act

<http://www.fcc.gov/cgb/consumerfacts/cipa.html>

<http://www.ifea.net/cipa.html>

FCC regulations implementing CIPA; FCC 01-120

[http://www.fcc.gov/Bureaus/Common\\_Carrier/Orders/2001/fcc01120.doc](http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc)

SLD's FAQ on E-rate certification procedures and timing

<http://www.usac.org/sl/tools/reference-area.aspx>

<http://www.e-ratecentral.com/default.asp>

### **COPPA**

Children's Online Privacy Protection Rule

<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

A list of software/applications used by students is available on the district website

<https://echolscountyboe.schoolinsites.com/> at Technology>Technology Documents

### **INTERNET SAFETY CURRICULUM**

To promote appropriate use of technology and to encourage students to be responsible digital citizens, the Technology Department of Echols County Schools District will develop and implement an Internet Safety Curriculum for all students Prek – 12<sup>th</sup> grade and faculty/staff. The implemented curriculum is available upon request by contacting the district's Technology Director.



## Adoption

The Echols County Board of Education adopted this TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY AGREEMENT for employees on April 10, 2023. Previous versions of this agreement are rescinded.

**The Echols County Board of Education makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Echols County Board of Education will not be responsible for any damages a user may suffer, including loss of data. The Board will not be responsible for the accuracy or quality of information obtained through the intranet/internet.**

## Staff Supervision, Monitoring and Notice of Web Filtering and Threat Protection Scanning

Staff members should become familiar with and enforce this agreement (along with CIPA, COPPA, eBoard, local, state and federal policies) and the parent and student ECS Technology Acceptable Use and Internet Safety Agreement used for the education of minors. In addition, faculty and staff members will be aware that a filtering system is installed, but that no filter is 100% effective. Vigilant monitoring (being present in the room and watching student's computer activity) and correction of student activity is required. When staff members become aware of student violations of this agreement, they will correct the student and address the matter to the Technology Director or designated technology personnel. The user is responsible for not seeking or initiating access to inappropriate material.

Echols County School District purchases a service that is a monitoring and alert system to identify incidents of cyberbullying, violence, self-harm and inappropriate content along with violations of FERPA, HIPAA and CIPA in school provided Office 365 accounts for all faculty/staff and students. Scanning includes Outlook email and all Office 365 features (Documents, Spreadsheets, Presentations, PDFs, Images & Photos, Videos) and all file types supported in Microsoft One Drive. ECSD seeks to provide improved data security and insights into potential exposures through this scanning process. ECSD monitors Office365 for the following reasons:

- Because for K12 schools, monitoring student online activities of students is a requirement for Federal e-Rate technology discounts.
- For cyberbullying, violence, mental health, radicalization, and hate speech that are clear and present dangers.
- Due to unauthorized app installs, visiting questionable websites can become the gateway for malware and ransomware.
- As student data theft and privacy violations can have serious consequences for student safety.
- Due to regulatory requirements such as FERPA, CIPA (for K12), and HIPAA requires an online safety monitoring system in place.

Staff members should also be aware that a system-wide computer monitoring system is in place that visually captures all computers in our district. Echols County School reserves the right to review any stored and transmitted information/files/documents with school system technology or on school provided network resources without the employee's consent.

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

This agreement was approved on April 10, 2023. It is also published in the Employee Handbook each school year and on the district website.

I have read the entire agreement and agree with the terms and conditions as stated.

THIS PAGE INTENTIONALLY  
LEFT BLANK

**2023 - 2024**

I acknowledge that I have read and will comply with the terms of this agreement.

I understand that this form must be completed in order to access the district network and district assigned accounts.

This Employee Sign-off page must be completed and given to the Technology Director.

---

BOE/Faculty/Staff Member Name (**PRINTED**)

---

BOE/Faculty/Staff Member **Signature**

---

Date