- VOLUME 12-

1:1 User Agreement

Model Lab School has initiated a 1:1 initiative for students and teachers in grades K – 12 in an effort to embrace 21st Century Learning. Students will be using these devices in the classroom as a part of routine instruction each day. After reading and returning the required agreement, students in grades four (4) through twelve (12) will be allowed to take their designated devices home to continue schoolwork. Please remember the devices are the property of the School and their contents may be viewed at any time. **Students are expected to have their devices with them each day, fully charged and ready for use.**

GOALS FOR STUDENT USERS

- Increase 21st Century Learning/skills
- Increase productivity and organization
- Increase student ownership of their learning and the learning process
- Utilize a wide array of digital educational materials
- Achieve "Technology Proficiency"

GUIDELINES

Student use of the issued devices falls under the Acceptable Use Policy for technology. Internet and device use will be monitored through school level management software. Anyone found to be violating acceptable use will be disciplined. All software, applications, and documents stored on the issued devices are the property of the School and subject to review/monitoring.

School Devices should NOT:

- Be modified in any way other than instructed by administration or school personnel.
- Have applied marks, stickers, or other decoration placed on the device.
- Be exchanged with anyone.
- Have school asset/inventory tags modified or tampered with in any way.
- Have heavy objects placed on top of them.
- Closing lid with items inside of device (i.e. pencils/pens).
- Have browsing history cleared of disabled.

Failure to comply with these guidelines will be treated as a violation of the Acceptable Use Policy and will be handled according to the school discipline code.

CARE AND USE OF ISSUED DEVICES

- Use a soft, lint-free towel to clean the screen – **do not use spray or liquid cleaners.**
- Make sure hands are clean before using device.
- Keep devices away from food and drink.
- Use only the included charger and a standard outlet to charge your device. Charge daily.
- Report software/hardware issues as soon as possible to the Tech Help Desk.
- Keep the issued device in a climate-controlled environment – do not expose to extreme temperatures.

SAVING DOCUMENTS

Documents are saved with your device using cloud storage. This will require you to have a school issued Google Apps for Education account, an Office 365 account and/or iCloud account. Using this account, you can save, export, and import documents. This allows you to access your documents from other devices via the Internet. You can also share your documents with other students or your teacher and collaborate using the above accounts. (@model.eku.edu)

REPORTING TECHNICAL ISSUES

Errors or problems should be reported as soon as is practical. This can be done by informing the Tech Help Desk, so the issue can be addressed in a timely manner. Damage due to a determined accidental cause will be addressed by the school through normal procedures. Damage due to negligence or carelessness will result in the student assuming the financial responsibility of the replacement/repair of the issued device. Students taking the device from school property must sign and submit the User Agreement Application. Student use of the device off school grounds may be revoked at any time by school administration.

1:1 User Agreement

SECURITY

Students should NEVER share their account passwords with others, unless requested by an administrator.

Students are responsible for following the guidelines and rules set forth in the Acceptable Use Policy.

Violations of these policies may result in disciplinary actions.

If a violation of the Acceptable Use Policy or discipline code occurs, appropriate consequences will be imposed by school administration.

It is expected that students will:

- Maintain control of their assigned device unless otherwise directed by administration.
- Not have the device out around food/drink (breakfast, lunch, snacking).
- Not leave the device unattended.
- Not play games during instructional time.
- Not clear or disable browsing history.
- Maintain adequate battery charge for school use.

**Not adhering to these guidelines will be considered negligence*.

GENERAL RULES

- After failing to bring your device to school five (5) times in a semester (or less by recommendation of Director), the student may become a "day user" until appropriate by administration.
- General misconduct or failing to have the assigned device at school/charged may result in student being assigned to "day user" status for a length of time determined by administration.

Please Remember:

- Devices may be monitored by administration at any time.
- Administration reserves the right to take a school issued device at any time.
- Teachers reserve the right to limit the device use during class.
- The device is the property of the School.

REMINDER OF NO PRIVACY GUARANTEE

School personnel have the right to access information stored in any user directory, on the current user screen or in electronic mail. They may review files and communications to maintain system integrity and ensure that individuals are using the system in accordance with School policies and guidelines. Students should not expect files stored on School servers or through School provided technology services to be private. By accepting these terms and conditions, students waive any right to privacy or confidentiality to material that was created, sent, accessed or stored using a school computing device or school provided account.

LOSS OR DAMAGE

If a issued device is damaged or lost, please report to the Tech Help Desk as soon as possible. If theft is suspected, a police report must be filed. If an incident happens in the evening, please inform the Tech Help Desk via email immediately and in person by 8:00 A.M. the following school day.

Students (and their parent/guardian) are responsible for replacement costs of technology equipment and peripherals that are lost, stolen, damaged or vandalized while under their issue.

2019-2020 Repair Costs are as follows:

- Apple 9.7 6th Gen iPad - $375.00
- STM dux Case for 9.7 iPad - $35.00
- Apple 12W USB Power Adapter for 9.7 iPad - $19.00
- Apple USB to Lightning cable - $19.00
- Apple 10.54 iPad Air - $553.00
- Apple 12W USB Power Adapter for 10.5 iPad Air - $19.00
- Apple USB to Lightning cable - $19.00
- Brydge Keyboard 10.5 - $100.00
- Brydge Micro USB Charging cable - $19.00
- Apple 12.9 iPad Pro - $1,075.00
- Apple 61W USB-C Power Adapter - $69.00
- Apple USB-C Charge Cable (1m) - $19.00
- Brydge Keyboard 12.9 - $135.00

MODEL LABORATORY SCHOOL
AT EASTERN KENTUCKY UNIVERSITY

User Agreement Terms

Student Name: (please print) _____Student Grade: _____

☐ I agree to the terms in the user agreement 08.2323 AP.2.

☐ I have read and understand the Acceptable Use Policy (AUP) found on Model's website – Technology Page.

☐ As a user of the Model Laboratory School computer network, I hereby agree to comply with the School's Internet and electronic mail rules and to communicate over the network in a responsible and appropriate manner while abiding by all relevant laws and restrictions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action and/or legal action may be taken.

☐ As the parent or legal guardian of the student (under 18) signing below, I grant permission for my child to access networked computer services such as electronic mail and the Internet. I understand that this access is designed for educational purposes; however, I also recognize that some materials on the Internet may be objectionable, and I accept responsibility for guidance of Internet use by setting and conveying standards for my child to follow when selecting, sharing, researching, or exploring electronic information and media.

CONSENT FOR USE

By signing this form, you hereby accept and agree that your child's rights to use the electronic resources provided by the School are subject to the terms and conditions set forth in School policy/procedure. Please also be advised that data stored in relation to such services is managed by the School pursuant to policy 08.2323 and accompanying procedures. You also understand that the e-mail address provided to your child can also be used to access other electronic services or technologies that may or may not be sponsored by the School, which provide features such as online storage, online communications and collaborations, and instant messaging. Use of those services is subject to either standard consumer terms of use or a standard consent model. Data stored in those systems, where applicable, may be managed pursuant to the agreement between designated service providers or between the end user and the service provider. Before your child can use online services, he/she must accept the service agreement and, in certain cases, obtain your consent.

Parent/Guardian Name – Print _____ Signature _____

Student Name – Print _____ Signature _____

Date: _____

- VOLUME 12-

Access to Electronic Media

(Acceptable Use Policy)

The School supports reasonable access to various information formats for students and employees and believes 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 School technology.

SAFETY PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for access to electronic media and students will follow EKU's Code of Ethics for Computing and Communications. Guidelines shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail, and other technological resources), and issues of privacy versus administrative review of electronic files and communications. In addition, guidelines shall prohibit utilization of networks for prohibited or illegal activities, the intentional spreading of embedded messages, or the use of other programs with the potential of damaging or destroying programs or data.

Students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

Internet safety measures, which shall apply to all School-owned devices with Internet access or personal devices that are permitted to access the School's network, shall be implemented that effectively address the following:

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

A technology protection measure may be disabled by the School's designee during use by an adult to enable access for bona fide research or other lawful purpose.

The School shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate its initial Internet safety measures.

Specific expectations for appropriate Internet use shall be reflected in the School's Code of Conduct including appropriate orientation for staff and students.

PERMISSION/AGREEMENT FORM

A written parental request shall be required prior to the student being granted independent access to electronic media involving School technological resources.

Access to Electronic Media

(Acceptable Use Policy)

PERMISSION/AGREEMENT FORM (CONTINUED)

The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges, and penalties for policy/procedural violations, must be signed by the parent or legal guardian of minor students (those under 18 years of age) and also by the student. This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Superintendent with a written request.

EMPLOYEE USE

Employees shall not use a code, access a file, or retrieve any stored communication unless they have been given authorization to do so. (Authorization is not required each time the electronic media is accessed in performance of one's duties.) Each employee is responsible for the security of his/her own password.

Employees are encouraged to use electronic mail and other School technology resources to promote student learning and communication with the home and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

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.

School employees and activity sponsors may set up blogs and other social networking accounts using School resources and following School guidelines to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

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 School employees and activity sponsors to utilize a social networking site for instructional, administrative or other work-related communication purposes, they shall comply with the following:

1. They shall request prior permission from the Superintendent/designee.
2. If permission is granted, staff members will set up the site following any School guidelines developed by the Superintendent's designee.
3. Guidelines may specify whether access to the site must be given to School technology staff.
4. If written parental consent is not otherwise granted through AUP forms provided by the School, staff shall notify parents of the site and obtain written permission for 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.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

5. Once the site has been created, the sponsoring staff member is responsible for the following:
    a. Monitoring and managing the site to promote safe and acceptable use; and
    b. Observing confidentiality restrictions concerning release of student information under state and federal law.

Staff members are discouraged from creating personal social networking sites to which they invite students to be friends. Employees taking such action do so at their own risk.

All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified faculty staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

UNIVERSITY CODE OF ETHICS FOR COMPUTING AND COMMUNICATIONS

All faculty, staff and students shall also abide by Policy 11.2.2P Code of Ethics for Computing and Communications.

DISREGARD OF RULES

Individuals who refuse to sign required acceptable use documents or who violate School rules governing the use of School technology shall be subject to loss or restriction of the privilege of using equipment, software, information access systems, or other computing and telecommunications technologies.

Employees and students shall be subject to disciplinary action, up to and including termination (employees) and disenrollment (students) for violating this policy and acceptable use rules and regulations established by the School.

RESPONSIBILITY FOR DAMAGES

Individuals shall reimburse the School for repair or replacement of School property, including technology, that is lost, stolen, damaged, or vandalized while under their care. Students or staff members who deface a School web site or otherwise make unauthorized changes to a web site shall be subject to disciplinary action, up to and including disenrollment and termination, as appropriate.

RESPONDING TO CONCERNS

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

Access to Electronic Media

(Acceptable Use Policy)

AUDIT OF USE

Users with network access shall not utilize School resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system.

The Superintendent/designee shall establish a process to determine whether the School's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
2. Maintaining and securing a usage log; and
3. Monitoring online activities of minors.

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least ten (10) years after the last day of service in a particular funding year.

ISSUE/CHECKOUT OF SCHOOL OWNED ELECTRONIC DEVICES

Electronic devices may be made available for student checkout but shall be the responsibility of the person to whom the device is issued and be subject to all provisions set out in the policy and related procedures. In addition, a signed AUP form must be on file at the school before an electronic device is issued to a student. Participants in the School's 1:1 Program shall refer to the user agreement for program guidelines and details.

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 5:120
16 KAR 1:020 (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 47 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516
15-ORD-190
Code of Ethics for Computing and Communications

RELATED POLICIES:

03.13214/03.23214
03.1325/03.2325
08.1353; 08.2322
09.14; 09.421; 09.422; 09.425; 09.426; 09.4261
10.4; 10.5

- VOLUME 12-

Access to Electronic Media

ELECTRONIC MAIL/INTERNET

The School offers students, staff, and members of the community access to the School's computer network for electronic mail and Internet. Because access to the Internet may expose users to items that are illegal, defamatory, inaccurate, or offensive, we require all students under the age of eighteen (18) to submit a completed Parent Permission/User Agreement Form to the Principal/designee prior to access/use. All other users will be required to complete and submit a User Agreement Form.

Except in cases involving students who are at least eighteen (18) years of age and have no legal guardian, parents/guardians may request that the school:

- Provide access so that the parent may examine the contents of their child(ren)'s email files;
- Terminate their child(ren)'s individual email account and/or Internet access; and
- Provide alternative activities for their child(ren) that do not require Internet access.

Parents/guardians wishing to challenge information accessed via the School's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

GENERAL STANDARDS FOR USERS

Standards for users shall be included in the School's electronic access plan, which shall include specific guidelines for student, staff, and community member access to and use of electronic resources.

Access is a privilege—not a right. Users are responsible for appropriate behavior and digital citizenship on school computer networks. Independent access to network service is given to individuals who agree to act in a responsible and appropriate manner. Users are required to comply with School standards and to honor the Acceptable Use Policy they have signed. Beyond clarification of user standards, the School is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network independently.

The network is provided for users to conduct research, develop presentation, participate in "flipped" lessons, and to communicate with others. Within reason, freedom of speech and access to information will be honored. During school hours, teachers of younger children will guide their students to appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio, the Internet, and other media that may carry/broadcast information.

NO PRIVACY GUARANTEE

The Director/DTC/designee has the right to access information stored in any user directory, on the current user screen, or in electronic mail. S/he may review files and communications to maintain system integrity and insure that individuals are using the system responsibly. Users should not expect files stored on School servers or through School provided or sponsored technology services, to be private.

Access to Electronic Media

RULES AND REGULATIONS

Violations of the Acceptable Use Policy (08.2323) include, but are not limited to, the following:

1. Violating State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
2. Using third party providers or any other nonstandard electronic MAIL systems.
3. Using student email accounts for non-educational purposes.
4. Sending or displaying offensive messages or pictures, including those that involve:
   - Profanity or obscenity; or
   - Harassing or intimidating communications.
5. Damaging computer systems, computer networks, or School websites.
6. Violating copyright laws, including illegal copying of commercial software and/or other protected material.
7. Using another user's password, "hacking" or gaining unauthorized access to computers or computer systems, or attempting to gain such unauthorized access.
8. Trespassing in another user's folder, work, or files.
9. Intentionally wasting limited resources, including but not limited to gaming, streaming audio or video for non-educational purposes and downloading of freeware or shareware programs.
10. Using the network for commercial purposes, financial gain or any illegal activity.
11. Using technology resources to bully, threaten or attack a staff member or student or to access and/or set up unauthorized blogs and online journals, including, but not limited to social media sites such as Facebook, Twitter, Instagram, etc.
12. Students revealing their name and personal information to, or establishing relationships with, "strangers" on the network, unless a parent or teacher has coordinated the communication.

Users are held accountable for the additional rules and regulations found in Acceptable Use Policy. Violations of these rules and regulations may result in loss of access/usage as well as other disciplinary or legal action.

RELATED POLICIES AND PROCEDURES:

08.2322
09.14

11.2.2P
Volume 11, Information Management
Chapter 2, Technologies
Section 2, Code of Ethics for Computing and Communications
Approval Authority: Board of Regents
Responsible Executive: Vice President for Administration
Responsible Office(s): Information Technology
Effective: 10/8/94 **Issued:** 10/8/94
Last Revised: 01/25/13 **Next Review Date:** 01/25/18

Code of Ethics for Computing and Communications

Policy Statement

This policy defines the privileges and responsibilities of computer and communications users at Eastern Kentucky University. It is the expectation that all members of the University community adhere to every aspect of this Code. In addition to representing University regulations, many items are mandated by federal and state laws. Violations may result in severe penalties, up to and including expulsion or termination from the University.

Entities Affected by the Policy

All EKU Students, Faculty, and Staff

Policy Background

N/A

Policy Procedures

I. Using Information Technology Resources

A. University information technology resources are provided to faculty, staff, and students for the purposes of study, research, service and other work-related activities. Because resources are limited, all computer users must respect the priority of these purposes at all times.

1. To support these purposes, the University provides users with computers, peripherals, software, networks, and electronic communication services, including electronic mail, Internet access and electronic storage. Use of these devices and services may not interfere with the user's responsibilities to the University, or conflict with this Code. For example, computer users engaged in activities that are not directly related to work, study, research, or University related service must yield their computers to others who need them for those purposes.

2. University users must not share individual accounts or passwords with others (this includes co-workers, friends, and relatives); acquire accounts for which they are ineligible, or maintain accounts and privileges which are not relevant to their current role and assigned responsibilities.

3. The use of information technology resources must comply with U.S. and international copyright and licensing laws and their acceptable use provisions. Such use must also comply with laws defined by the Digital Millennium Copyright Act of 1998. The transmission or storage of all reproduced, distributed, altered, enhanced and/or manipulated copyrighted material must have prior written permission of the copyright holder.

B. The policies in this code apply to all hardware and software that make use of University resources, regardless of who owns the equipment or software licenses.

C. Use of University information technology resources to support a personal, profit-making activity is strictly forbidden.

D. The University generally does not monitor or restrict the content of material transmitted, stored, or posted on University information technology resources. However, the University reserves the right to monitor, limit or remove content or access to resources, when it has been determined by the appropriate University official that there is a violation or potential violation of applicable University regulations, contractual obligations, or state or federal laws. Individuals who use University information technology resources and email for any work-related or personal matters do not acquire an absolute right of privacy for data, documents and communications transmitted or stored on University information technology resources. Individuals are reminded that University information technology is University property and the individual has no expectation of privacy regarding any electronic communications, data or documents sent, received, or stored on University information technology.

II. Protecting Information Technology Resources and Institutional Data

A. Because information technology resources are limited and constitute a large investment by the University, all users must take proactive measures to protect these resources from malicious software, physical damage, and unauthorized access.

1. Individuals must comply with University protocol to minimize risks from viruses, phishing, and other technological threats.

2. Individuals must comply with all software licensing provisions, paying particular attention when installing software on multiple computers. No one should make copies of software for which permission to copy is not explicitly given. If the software does not allow users to copy it, then the software should not be copied.

3. Individuals must not use their access to computer systems to maliciously destroy or alter University accounts, files, software or hardware. Individuals must not attempt to obtain resources for which they are ineligible, or deprive others of resources.

4. Publishers may establish copyrights on digital material only in accordance with Eastern Kentucky University policies and U.S. laws.

B. Individuals with access to view or change sensitive institutional data must maintain the appropriate confidentiality, integrity, and security of that information, in accordance with University policies, as well as state and federal laws.

1. Individuals must not access information beyond that directly related to their current job assignments. Intentionally disclosing protected information to any unauthorized person is a violation of federal law (FERPA, HIPAA, etc.) and can subject the violators to University administrative, criminal and civil penalties.

2. Individuals with access to Personally Identifiable Information (PII) must take special care to use and transmit that data in an acceptable manner to prevent interception or misuse. For example: Email is not an acceptable method of transmitting PII.

III. Privacy of Information Technology Accounts

A. Account passwords are the primary means of ensuring privacy. Individuals must not share accounts or passwords.

B. When necessary for enforcing this Code, University policies or regulations, or public law, and when cause exists, authorized University personnel may access an individual's accounts and content to investigate possible violations. This may be done without securing permission.

C. University personnel who are authorized to access others' accounts to investigate possible violations must do so only under the direction of authorized personnel, and for no other purpose.

D. Electronic data and records will be released to appropriate authorities with authorization through a subpoena, warrant or other legal directive and may be subject to Open Records Requests.

IV. Electronic Communications

The use of information technology resources for unlawful purposes is prohibited. Examples of unlawful use include, but are not limited to: defrauding, threatening, abusing, defaming, harassing, intimidating or transmitting obscene messages or media. Using information technology is no different than similar conduct carried out in person, by telephone or by mail. Violations through electronic media will subject the individual to the same University sanctions.

In addition to the above, starting or extending email chain letters or spam is an example of an improper use of University resources.

Definitions

Information Technology Resources – Any technology, data, or service owned, housed, or contracted for use by the University, regardless of physical location.

PII – Personally Identifiable Information – Data which can be used alone, or with other information to uniquely identify, contact, or locate an individual. (e.g. social security number, date of birth, driver's license number, credit card number)

University-Eastern Kentucky University

Responsibilities

Associate Vice President for Information Technology:

Oversees University information technology resources.

Violations of the Policy

Violations of this policy could subject individual(s) to appropriate administrative and legal action; including any applicable provisions of faculty, staff, and student handbooks in coordination with other University units/departments e.g. Internal Audit, Office of University Counsel, or Equal Opportunity Office.

Interpreting Authority

Vice President for Administration

Statutory or Regulatory References

Digital Millennium Copyright Act of 1998 (DMCA)
Family Educational Rights and Privacy Act of 1974 (The Buckley Amendment) (FERPA)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Relevant Links

University Communications via University Email Accounts Policy 11.2.1P

Policy Adoption Review and Approval

Approved by EKU Board of Regents October 8, 1994
Revisions approved by EKU Board of Regents January 25, 2013