Access to Electronic Media

(Acceptable Use Policy)

The Board supports reasonable access to various information formats for students, employees and the community 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 District technology.

SAFETY PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for access to electronic media. 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 District technological resources including portals used to access data), 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 District-owned devices with Internet access or personal devices that are permitted to access the District'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 Board's designee during use by an adult to enable access for bona fide research or other lawful purpose.

The District 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 District's code of acceptable behavior and discipline 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 District 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.

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 or District level before an electronic device is issued to a student.

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 school technology, including e-mail and the Internet to:

1. Promote student learning
2. Promote communication with the home and education-related entities
3. Continue their professional education;
4. Improve their technology skills;
5. Improve the delivery of curriculum related material to the classroom;
6. Share educational ideas with colleagues;
7. Communicate with others to better understand global issues and world culture; and/or
8. Improve public relations between the school and the outside community at large.

Employees may not use the school technology system or any of its components to:

1. Engage in illegal activities;
2. Promote non-school related business;
3. Seek to attain personal financial gain;
4. Provide for personal entertainment not related to education;
5. Promote for profit organizations; and
6. Promote non-profit organizations whose goals are contrary to those of the Board, the District’s schools, or the community at large.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

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.

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

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

In order for District employees 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 District guidelines developed by the Superintendent's designee.
3. Guidelines may specify whether access to the site must be given to school/District technology staff.
4. If written parental consent is not otherwise granted through AUP forms provided by the District, staff shall notify parents of the site and obtain written permission for 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.
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 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.

Employees shall not install software on any school equipment unless the school owns a license for that software or unless they personally have a license for that software and have that license on file with the School Technology Coordinator or the District Technology Coordinator.

Access to Electronic Media

(Acceptable Use Policy)

WEBPAGES

All teachers involved in the creation of school-related web pages shall follow the guidelines set forth in procedure 08.2323 AP.1. All policies from the District's technology AUP shall apply to the creation of any school-related and/or posted website.

PARENTAL PORTALS

Access to the Parent Portal is a privilege, not a right. Users of the portal shall follow the District's Acceptable Use Policy (Access to Electronic Media) and accompanying procedures. In addition, any guidelines set forth by KDE concerning the use or misuse of the data system shall be followed.

Parents/guardians are responsible for their use of the Parent Portal. The District makes no guarantee that the Parent Portal will be error-free or without defect. The District is not responsible or liable for any damage that a user may suffer as a consequence of using the Parent Portal or information contained in the Parent Portal.

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which computer equipment, software and information access systems will be available to the community.

Upon request to the Principal/designee, community members may have access to the Internet and other electronic information sources and programs available through the District's technology system, provided they attend any required training and abide by the rules of usage established by the Superintendent/designee.

DISREGARD OF RULES

Individuals who refuse to sign required acceptable use documents or who violate District rules governing the use of District 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 expulsion (students) for violating this policy and acceptable use rules and regulations established by the school or District.

RESPONSIBILITY FOR DAMAGES

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

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 District 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 District'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.

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 005:120
16 KAR 1:020 KAR 001:020 (Code of Ethics (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

RELATED POLICIES:

03.13214; 03.23214; 03.1325/03.2325; 03.17/03.27
08.1353; 08.2322
09.14; 09.421; 09.422; 09.425; 09.426; 09.4261
10.5

Adopted/Amended: 4/16/2020
Order #: 202096

Acceptable Use Procedures

STUDENT ACCEPTABLE USE PROCEDURES

All students in the District will be required to sign an Acceptable Use Agreement to obtain a network account. A written request, signed by the student and his/her parent or legal guardian for minors [those under eighteen (18) years of age or non-emancipated] shall be required before a student will be allowed access to the Internet or e-mail. This document shall be kept as a legal, binding document and shall be in effect for the entire time period the student is enrolled in that school. The student's parent/guardian ([or the student who is at least eighteen (18) years old or emancipated] must provide the Superintendent with a written request to rescind this agreement.

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/District:

- 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 District's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

Users should not expect files stored on District servers or through District provided or sponsored technology services, to be private.

RULES AND REGULATIONS-STUDENTS

Although other conduct that materially or substantially disrupts the educational process, poses a threat to District property, or endangers others is prohibited, the following is a partial list of activities that are not permitted:

1. Violating State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
2. Sending or displaying obscene messages or pictures, including those that involve:
   - Profanity or obscenity or sending or displaying offensive messages or pictures. (Content is offensive under this procedure if it interferes with another individual's access to educational services or disrupts the educational environment.)
   - Harassing or intimidating communications. (Harassment is addressed in Board Policy 09.42811.)
3. Entering chat rooms except under the supervision of a teacher for a planned instructional activity.
4. Damaging computers, school/District websites, computer systems, or computer networks, including the intentional uploading of a computer virus or the creation of a virus.
5. Violating copyright laws, including illegal copying of commercial software and/or other protected material. (Each user is individually responsible for ensuring his/her usage does not violate any federal or state laws.)
6. Using other user's passwords or allowing someone else to use your password.

Acceptable Use Procedures

RULES AND REGULATIONS-STUDENTS (CONTINUED)

7. Trespassing in other user's accounts, files, directories or work and/or harming or destroying data of another user.
8. Modifying system files used in the operation of the computer, the network or software installed on them.
9. Intentionally wasting limited resources which includes, but is not limited to, time, memory space, and paper, including downloading of freeware or shareware programs. (Resources are deemed to be wasted if they are consumed or used for something other than a legitimate educational purpose related to the class or activity in which the individual utilizes the computer or if they are used or consumed without the permission of the teacher or network administrator.)
10. 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 MySpace.com, Facebook.com or Xanga.com. (Bullying is defined in Board Policy 09.422)
11. Employing the network for commercial purposes or financial purposes.
12. Posting personal information of students and/or staff on any server without a signed Media/Web Page Release Form (09.14 AP.251).
13. Activities deemed to be a security risk to the network.
14. Vandalism/Defacement of the physical equipment.
15. Installation of any unauthorized software obtained from any source.
16. Bringing software from home and using it on the school system. (Except software that may be written by the student as part of a District programming class.)
17. Creation and/or posting of Internet material without the supervision of a staff member.
18. Revealing personal information including, but not limited to, home addresses, birth dates, social security numbers, phone number, credit card information, bank account number(s) or any other financial information. Your personal signature on any e-mail must use the school address only.
19. Printing any material accessed from the Internet without permission of the staff person supervising your internet activity.
20. Students in Primary through Fourth grade (P-4 may not visit any Internet site that has not been bookmarked for them by a staff member. They are allowed links to other sites only under the specific instruction of a staff member.)
21. Accessing the Internet without staff permission.
22. Accessing inappropriate sites. (A site is inappropriate if it is unrelated to the educational purpose of the class or activity for which the system is being utilized or if it causes a disruption to the educational environment.)
23. Using any e-mail software (i.e., Hotmail, yahoo, rocket, etc.) that is not school provided Exchange.

Acceptable Use Procedures

RULES AND REGULATIONS-STUDENTS (CONTINUED)

If the user violates any of these provisions, District administrators may suspend his/her account subject to review by the Principal/designee. Disciplinary action could result in suspension from school and/or a notation on the student's permanent record card and future telecommunication access denied. The observing staff member who notes the infraction will complete a Discipline Report. All disciplinary actions shall be subject to the procedures outlined in other District Board policies, the District code of conduct and the school handbook. School Technology Coordinators shall be notified of action(s) taken regarding the offending student

STAFF ACCEPTABLE USE PROCEDURES

RULES AND REGULATIONS -STAFF

Access to technology is a privilege, not a right. Therefore, based upon the acceptable use guidelines outlined by the District, the school administrators will deem what is appropriate use and may close an account at any time. The appeals process will follow accepted District guidelines under Board policies 03.16 and 03.26.

Employees are encouraged to use school technology, including e-mail and the Internet to:

- Continue their professional education;
- Improve their technology skills;
- Improve the delivery of curriculum-related materials to the classroom;
- Share educational ideas with colleagues;
- Communicate with others to better understand global issues and world culture; and/or
- Improve public relations between the school and the outside community at large.

Staff members are responsible for:

- Setting and conveying standards that should be followed when using media and information services;
- Following generally acceptable rules for public behavior and communications;
- Supervising Internet activity on the workstation assigned as their staff workstation;
- Supervising on the Internet students to whom they have provided access to an Internet browser;
- Visiting all web sites that are to be used in class presentation within 32 hours prior to their display in class; and/or
- Completing a discipline report and submitting it to the school administration for any student who is involved in inappropriate activities on a school network.
- Instructing students about Internet safety/digital citizenship, including appropriate online behavior, interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.
- Providing documentation of instruction yearly on Internet safety/digital citizenship for all students.

Acceptable Use Procedures

RULES AND REGULATIONS –STAFF (CONTINUED)

Employees are prohibited from using the school technology system or any web site authorized by the school as well as any of its components to:

- Engage in illegal activities;
- Set up or update personal electronic social networking websites;
- Promote non-school related business;
- Seek to attain personal financial gain (use of public property for personal financial gain is a felony and is subject to prosecution);
- Provide for personal entertainment not related to education;
- Promote for-profit organizations;
- Promote non-profit organizations whose goals are contrary to those of the Board, the District's schools or the community at large;
- Engage in political lobbying;
- Disclose personal staff and/or student information including, but not limited to, names or lists without prior signed permission from the individual and his/her legal guardian. (A Media/Web page Release Form/09.14 AP.251must be completed.)
- Transmit any material in violation of U.S. or state regulations including copyrighted, threatening, or obscene material;
- Use the Internet or e-mail in a classroom presentation that is not part of a planned curriculum activity.

ELECTRONIC SOCIAL NETWORKING

Employees who set up personal electronic social networking web pages on their home or personal computers are responsible for the content of their web pages, including but not limited to, content added by the employees, friends or members of the public who can access the web page, or content that is linked to the employee's web page.

Requirements:

Employees must be Internet certified and E-mail certified by the District Director of Technology/Chief Information Officer to attain access to these network utilities.

Employees shall have an acceptable password on file with District Director of Technology/Chief Information Officer.

Acceptable Use Procedures

RULES AND REGULATIONS –STAFF (CONTINUED)

The District uses Internet filtering software to monitor student and staff Internet activity. The Network Account Administrator is responsible for monitoring the Internet activity reports. Employees do not have any privacy right in their internet usage at work. Employees' email may be subject to disclosure to the public under the Kentucky Open Records Act, and District administrators may perform searches of document on the network or individual computers to identify materials that are responsive to a record request.

The Network Account Administration is responsible for:

- Monitoring Internet activity reports (Reports are kept for thirty (30) days.);
- Reporting any Acceptable use Policy (AUP) and related procedure violations to the appropriate building Principal;
- Blocking inappropriate sites when found; and/or
- If network integrity is threatened, removing user rights as directed by the building Principal or District Technology Administrator when a violation has occurred.
- Taking appropriate action with the violator of the AUP and related procedures;
- Notifying Network Account Administrator to disable/enable violator's account; and/or
- Notifying classroom teacher of the violation that occurred in his/her classroom.
- **Internet activity reports are kept for thirty (30) days.**

WEB PAGES

All teachers involved in the creation of school-related web pages shall be responsible for assuring that:

- Information is kept current,
- All entries, uploads, links, pages, etc. relate to education,
    - Athletic pages are kept separate from teacher's classroom web pages,
- Students are not permitted access to the admin portion of the site,
- Student photo permission to publish is checked BEFORE placing a student's photo on the web page,
- "Student Information Directory Notification", Board procedure 09.14 AP.12, is checked before publishing a student's name. This information is located in each school office, and
- Links to the teacher's site should be added to the schools websites. See the School Webmaster.

WEB PAGE/BLOGGING SITES FOR TEACHERS

Blogging is allowed only with permission of the building level Principal under the following circumstances:

- A signed copy of the "MCS Hosted Student Blogging Permission Form" is on file with the building Principal; and
- The site is set up so that ALL comments are held for moderation.

Acceptable Use Procedures

STUDENT INTERACTIVE WEB PAGE RESOURCES NOT HOUSED ON DISTRICT SERVERS

Use of student interactive web pages allowed only with permission from building level Principal.

A signed copy of the "MCS Hosted Student Blogging Permission Form" must be on file with the building Principal.

REPORTING VIOLATIONS

Anyone who has knowledge of a violation of this procedure is encouraged to report the violation to a school administrator or the network administrator. Any student or employee who believes he/she has been the victim of bullying, harassment, or other prohibited behavior under this procedure is requested to report the matter immediately to the school administrator or the network administrator so that an investigation can be conducted and disciplinary action taken if warranted.

PARENT PORTAL USE

The Mercer County School District uses Infinite Campus for student information management. Infinite Campus (IC) has developed a parent portal to allow parents/guardians to view the records of their child(ren) via the Internet. Mercer County Schools will provide parents/guardians of currently enrolled students the privilege of free access to the Parent Portal. Only parents or guardians of students enrolled in the district will be allowed access to the Parent Portal. Mercer County Schools reserves the right to deny or cease access to the Parent Portal due to the abuse of the portal, court orders, or any other legal proceedings that limit the availability of private, educational data.

PURPOSE

Mercer County Schools has opened the Parent Portal to enhance communication between the district and parents/guardians. Users of the Parent Portal will have access to the following information about their children:

- Personal Data
- Attendance
- View/Print Student Schedule
- Gradebook and Assignments

Mercer County Schools reserves the right to add to or remove any of the above functions from the Parent Portal at any time.

USE OF THE PARENT PORTAL

Access to the Parent Portal on the district's system is a privilege, not a right. Users of the Parent Portal are required to adhere to the following guidelines:

1. Users will act in a responsible, legal and ethical manner.
2. Users will not attempt to harm or destroy data, the school or the district network.
3. Users will not attempt to access data or any other account owned by another user.
4. Users will not use the Parent Portal for any illegal activity, including violation of data privacy laws. Anyone found to be in violation of these laws may be subject to civil and/or criminal prosecution.

Acceptable Use Procedures

USE OF THE PARENT PORTAL (CONTINUED)

5. Users who identify a security problem with the Parent Portal must notify the district's Department of Pupil Personnel immediately without demonstrating the problem to anyone else.
6. Users will not share their password with anyone, including their own children.
7. Users will not set their own computer to automatically log-in to the Parent Portal.
8. Users identified as a security risk to the Parent Portal or the Mercer County Schools' network will be denied access to the Parent Portal.

PORTAL USER ACCOUNT SECURITY FEATURES

Three unsuccessful login attempts will disable the user's Portal account. In order to reactivate, the user will need to contact the Department of Pupil Personnel to reset login information. User will automatically be logged off if Portal web browser is open and inactive for a period of time. All attempts at logging in to the system are recorded and monitored.

TECHNICAL ISSUES WITH THE PARENT PORTAL

There are times when there will be a need to shut down the Parent Portal for maintenance purposes. Mercer County Schools is not liable for any issues related to your personal computer and reserves the right to refuse technical assistance directly related to your personal computer. Technical issues should be directed to the District's Director of Pupil Personnel office.

SYSTEM REQUIREMENTS

Computer

Processor 486 running at 66MHZ; Pentium recommended

Windows 98 or Newer Operating System

16 MB Memory or greater

45 MB of disk space or greater

Internet Connection

56K or faster

Monitor

The Parent Portal is best viewed with a resolution of 800 x 600 or greater.

DATA INTERPRETATION

Data posted on the Parent Portal will vary based on the school your child attends. Teachers should have grades posted to the Parent Portal within one week from receiving the assignment. Some large assignments such as projects take more time to grade, thus will take more than the standard one week. Please contact your child's teacher with any questions. Schedules will be different from school to school as well as grading scales.

Personal Data

Personal Data is typically updated within one week of student registration. The volume of changes collected during the fall registration may delay updates beyond one week. Contact the Director of Pupil Personnel office if there is incorrect information displayed.

Acceptable Use Procedures

DATA INTERPRETATION (CONTINUED)

Class Assignments

Class assignments and scores can be viewed once teachers have posted them in Infinite Campus grade book. Student scores are an APPROXIMATE grade at a specific point in time. Other factors influence grades such as the value given to the assignment and individual student progress.

REQUESTING PARENT PORTAL ACCESS

Users must complete a "Portal Activation Request" form available online at www.mercer.kyschools.us or by visiting your student's school. This form, along with photo ID, must be completed and returned to the school prior to activation of your account.

STEPS FOR CREATING A PARENT PORTAL ACCOUNT

1. Go to www.mercer.kyschools.us.
2. Click on LINKS/RESOURCES located top right of the screen below the picture banner.
3. Then, click on the Infinite Campus Portal login icon (green graphic) on the right side of the page.
4. Click on the orange HELP link located on the bottom right hand corner
5. Select the "If you have been assigned a Campus Portal Activation Key, click here" option.
6. Enter your "Person GUID" number you received from your child's school in the "Activation Key" field.
7. Enter a unique username and password. Password must be 8 characters in length.

RELATED POLICIES:

09.14; 09.422; 09.42811

Review/Revised:4/16/2020

Electronic Access/User Agreement Forms

Local Network/Staff Use

User's Name __________________________________ ________________________ ________________________
Last Name *First Name* *Middle Initial*

User's Address ____ _________________ ___________________
Address *City* *Zip Code*

Date of Birth ____________________ **Gender □ M or □ F Phone Number** _____________________

School/Building Assignment ______________________________ **Position** _____________________

Subject or grade level ___________________________
If applicable

Please check □ certified employee □ classified employee □ bus driver □ substitute □ board member □ member of the community □ Other: _________________.

As a user of the Mercer County School District's computer network, I hereby agree to comply with the District's Internet and electronic mail rules and to communicate over the network in a responsible 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.

User's Full Legal Name (Please print) ____

____ _____________________
User's Signature ***Date***

Staff login name _________________(dot)_____________________@mercer.kyschools.us
First name **Last name**

The default staff password will be: [redacted] - User's will be required to change their password upon first logon to a District workstations. Please note the password requirements listed below. Passwords must meet the following requirements:

- Minimum Password Length – 15 characters minimum (use an easy to remember passphrase)
- Complexity – Not required.
- Password Expirations – Every 180 days; or after a suspected data breach or compromised account
- Lockout Threshold – 10 attempts or fewer
- Lockout Duration – 10 minutes or more
- Minimum Password Age – 3 days
- Password History Count – Previous 12 passwords

Mercer County Email Address: firstname.lastname@mercer.kyschools.us

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