

Warren County Public Schools

Electronic Resources Acceptable Use Procedures, Guidelines, and Signature Forms

(including WCBE 08.2323 AP.21 and WCBE 08.2323 AP.23)

Revised June 2017

Overview and Rational of the Warren County Public Schools Acceptable Use Policy

(Adapted from WCBE Policy 08.2323)

Who has access to WCPS electronic resources?

The Warren County Board of Education supports the rights of students, staff, and community members to have reasonable access to various information formats and believes it is incumbent upon students, staff, and community members to use this privilege in an appropriate and responsible manner.

What is the purpose of an acceptable use policy?

The policy provides appropriate standards to guide the behavior of students, staff, and community members involved in accessing electronic media. Specifically, the guidelines address the ethical use of various electronic media, the policies covering issues of privacy versus administrative review of electronic files and communications, and prohibits the use of electronic resources for noneducational and illegal activities.

What forms are required in order for a student to have access to the electronic resources of the WCPS?

The forms required may vary with the age of the student and the type of access requested. Students will be granted supervised access to district owned electronic resources upon signed agreement with the policies/procedures outlined in the District's Student Handbook. Electronic resources include, but are not limited to: collaborative and communication tools, document storage space, instructional resources, and Internet sites. A separate permission form, signed by a parent/guardian is required for any student to independently access the electronic resources, including Internet sites, provided by the school district. An additional student email account request form is required before a student can be given access to a district sponsored email account. The required permission/agreement form(s) specifies acceptable uses, rules of on-line behavior, access privileges, and penalties for policy/procedural violations. This document(s) 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 (or designee) with a written request for modification or termination.

How will appropriate content be determined?

As described in WCPS School Board Policy 08.2322, school officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning the appropriateness of web sites and electronic resources.

A complete copy of the Acceptable Use Procedures, Guidelines, and Signature Forms can be obtained from the Warren County Schools web site, <http://www.warrencountyschools.org>.

Warren County Public Schools

Acceptable Use Procedures and Guidelines

for

Electronic Resources

Part 1 -- Definition

Electronic resources include, but are not limited to, the following types of materials:

- a. computers and related equipment
- b. computer network resources including email, Internet sites, district owned cloud-based collaboration sites, and district sponsored social media sites
- c. electronic media and content

Part 2 -- Access Privileges and Privacy

The Warren County Public Schools maintains the right to limit access to all types of electronic resources in order to assure that district resources are used for the intended educational purpose. A network administrator or the Director of Technology has the right to access information stored on any device attached to the district network, in any user directory (local or WCPS owned cloud-based sites), on the current user screen, or in electronic mail. Users are advised that placing confidential documents in their user directory does not guarantee absolute security or privacy. Network management and monitoring software packages may be used for random access to any networked device to review progress and for security purposes.

Part 3 -- General Information for Users

All Students:

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 shall be implemented that effectively address the following:

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

Students in Grades PK - 8:

- Students are allowed to use network resources using a “student” login. This type of user login allows student read-only access to instructional software and data files.
- Students are allowed to have an independent school network user account and may access the WCPS owned, cloud-based private storage directory for student work/collaboration.
- Students access to the Internet is only available under the direct supervision of a teacher or instructional assistant. Students are not allowed to have unsupervised access to the Internet at school.
- Students will be given access to electronic mail when requested by a sponsoring teacher and upon return of a signed parental permission form.
- Student use of the WCPS provided G Suite services shall be for classroom/instructional related assignments only. Students are not allowed to use the collaboration services to share documents or communicate with others outside of the WCPS G Suite environment without specific authorization from the sponsoring teacher of that assignment. Students are responsible for declining all sharing/collaboration requests that they receive which are not specific to a school sponsored assignment and approved by the sponsoring teacher.

Students in Grades 9-12:

- High school students are allowed to use network resources using a “student” login. This type of user login allows student read-only access to instructional software and data files.
- High school students are allowed to have an independent school network user account and may access the WCPS owned, cloud-based private storage directory for student work/collaboration. In addition, students may be permitted access to district sponsored social media sites when applicable to the educational purposes of the school district.
- Student access to the Internet is available on an independent basis if requested by a sponsoring teacher and upon return of a signed parental permission form.
- High school students will be given access to electronic mail when requested by a sponsoring teacher and upon return of a signed parental permission form.
- Student use of the WCPS provided G Suite services shall be for classroom/instructional related assignments only. Students are not allowed to use the collaboration services to share documents or communicate with others outside of the WCPS G Suite environment without specific authorization from the sponsoring teacher of that assignment. Students are responsible for declining all sharing/collaboration requests that they receive which are not specific to a school sponsored assignment and approved by the sponsoring teacher.

Employees:

For every staff person whose position requires network access, an account with appropriate rights will be established. The account will include access to electronic mail, Internet sites, and an individual cloud-based directory for files/collaboration. If job related access to the Internet is not needed, the school principal or employee's supervisor must notify the Director of Technology to have these services restricted.

Community Members:

If used for educational purposes, community members may have access to the electronic resources of the WCPS. Community members requesting Internet access must attend a 1 hour training/awareness session provided by the Director of Technology (or designee) prior to being given access to this resource.

Part 4 -- Rights, Responsibilities, and Privileges

A. Privileges:

Access to the electronic resources of the WCPS is a privilege, not a right. Violation of the acceptable use policy may result in the immediate loss of network services including, but not limited to, Internet access and could impact future access to the electronic resources of WCPS. Additional consequences may include student suspension (in-school/out-of-school), student expulsion, employee letter of reprimand, or termination of employment in accordance with school board policy. In addition, any attempted or executed criminal violations involving the electronic resources of WCPS will be prosecuted to the fullest extent of the law.

B. General Responsibilities:

The use of your account must be in support of educational and research activities consistent with the objectives of the Warren County School District, access to educationally inappropriate materials is prohibited. Use of other organization's networks or computing resources must comply with the rules appropriate for that network. Access to, sharing, or transmission of any material in violation of any federal or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, vulgarity, sexually explicit material, or information protected by trade secret. The use of your WCPS account to play games (including online multi-user games) or participate in peer-to-peer file sharing (LimeWire, Kazaa, BitTorrent, etc.) is not acceptable. Illegal activities, including the installation and use of unlicensed software, are strictly prohibited. Use for product advertisement or political/religious statements that are not consistent with the educational purposes of the WCPS is inappropriate. In addition, use of an electronic mail or WCPS account to buy, sell, or trade personal items is not an acceptable use of district resources.

C. Specific Network and Internet Responsibilities:

1. You may not give your password to anyone.
2. You may not use or alter any one else's account.
3. You may not offer Internet access to other individuals via your WCPS account.
4. You may not break in or attempt to break into other computer networks.
5. You may not intentionally spread embedded messages or other programs which have the potential of damaging or destroying programs or data.
6. You may not destroy another person's data.
7. Purposefully annoying other WCPS or Internet users is prohibited.
8. Harassment as defined in board policy shall not be allowed.
9. All communications and information accessible via the network is assumed to be for the individual consumption of the user, however, privacy is not guaranteed.
10. Collaborative documents shall only be shared with users who have specifically requested shared access. Intentionally sharing collaborative documents with users who have not requested access may be treated as bullying, hazing, and/or harassment.
11. Use of social networking web sites from district resources must be consistent with the educational objectives of the school district.
12. Notify the school principal or Director of Technology of any violations of this contract taking place by other users or outside parties. This may be done anonymously.

D. Specific Electronic Mail Responsibilities:

1. Be polite. Do not write or send abusive messages to others.
2. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
3. Do not reveal the personal address or phone number of other students or yourself.
4. Note that electronic mail is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities shall be reported to the authorities.
5. Only Kentucky Department of Education approved email systems may be accessed from the district's network. Access to the approved email system is for educational purposes only.
6. Notify the school principal or Director of Technology of any violations of this contract taking place by other users or outside parties. This may be done anonymously.

E. Specific Employee Web Site Responsibilities:

Web sites created, maintained, and hosted on the electronic resources of WCPS should adhere to the following guidelines.

1. This is not a personal, private web site. The web site is to be used in support of educational and research activities consistent with the objectives of the Warren County School District.
2. If you have a “list of favorites” or an “about me” page where you are introducing yourself to your students, you have the right to determine your own favorites in such categories as books, authors, quotes, etc. as long as these items are representative of you and your profession.
3. You should refrain from posting religious or political statements about your personal beliefs.
4. Copyrighted materials shall not be posted on publicly available or WCPS intranet web sites.
5. District web sites which are not password protected should be considered available for public access. The material on publicly available sites is subject to federal accessibility and accommodation guidelines as well as potentially other federal/state law requirements. It is the specific employee’s responsibility to ensure that sites comply with all applicable guidelines.

F. Data Access Responsibilities:

Warren County Public School information (hereafter data) must be managed, used, and protected in accordance with federal law, state law, and school district policies so as to ensure its integrity, availability, privacy, and confidentiality. Each employee, agent, or affiliate of WCPS, who handles data for the purpose of performing his/her job duties, or other functions directly related to his/her contractual affiliation with the district, is a steward of data and is responsible for the proper handling of data resources under his/her control. It is the obligation of all employees to protect the security and integrity of all data under their control. No data should be copied or stored on portable computing devices. All data should remain on district network servers and resources. Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately altering, damaging, or destroying data; inadequately protecting restricted data; or ignoring the explicit requirements for the proper management, use, and protection of data resources. Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal, pursuant to district policies.

G. Student Assigned Device (“Take-Home” Use):

Any device/resource and its use is the responsibility of the student to whom it is assigned. Any violation of the acceptable use policy, procedures, or guidelines is the responsibility of the student. Violations occurring off school grounds on a “take-home” device will be addressed in the same manner as if the violation occurred on school property and during school hours.

Any device (computer, laptop, MP3 player, camera, etc.) or resource (cd, dvd, MP3 files, movie files, web pages, etc.) is to be used for instructional purposes only.

It is the student’s responsibility to ensure that the device is ready for instructional use each day. This includes, but is not limited to, enough battery life, hard drive space, RAM, and proper network configuration settings. Any modification (addition or deletion) of the district installed operating system, settings, and/or instructional resources is prohibited without the prior approval of the Director of Technology or designee.

Students shall not vandalize or deface the assigned device in any way. This includes, but is not limited to, the use of markers, stickers, or tape on the device. Obscene language or materials, including screen savers, backdrops, wallpapers, photos, and/or desktop images are prohibited.

Students may not remove any manufacturer or district labeling on any device or resource. Students may not take apart any device or attempt to repair any hardware component of the system.

Downloading music, games, videos, or applications during school hours is prohibited unless approved by a classroom teacher. File sharing must be approved and directed by a classroom teacher. Students may not use any district-owned device to transfer illegal or copyrighted materials to other devices. Copyrighted district resources may not be transferred to any other device not owned by the school district.

Students are prohibited from using another student’s user name or password to access any device or resource.

Students are prohibited from sending non-instructional emails, chat messages, instant messages, and text messages with district-owned devices. Additionally, non-instructional web sites shall not be hosted on any district-owned device.

The district is only responsible for the original district loaded software. All personal software and files loaded or created by a user are subject to removal at any time during routine upgrades, maintenance, repairs, or as a result of an Acceptable Use Procedures violation. The user is responsible for backing up all files added or created on the device.

H. Student Owned Devices:

Students who demonstrate an understanding of good digital citizenship may be allowed to connect their personally owned devices to Warren County Schools Computer network provided they observe the following conditions:

1. Devices shall not be used in a manner that disrupts the educational process, including, but not limited to, use that:
 - a. Poses a threat to academic integrity, such as cheating,
 - b. Violates confidentiality or privacy rights of another individual,
 - c. Is profane, indecent, or obscene,
 - d. Constitutes or promotes illegal activity or activity in violation of school rules, or
 - e. Constitutes or promotes sending, sharing, or possessing sexually explicit messages, photographs, or images using any electronic device.
2. Unless an emergency situation exists that involves imminent physical danger or a certified employee authorizes the student to do otherwise, devices shall be turned on and operated only before and after the regular school day and during times designated by the school.
3. When students violate prohibitions of this policy, they shall be subject to disciplinary action, including losing the privilege of bringing the device onto school property and being reported to their parent/guardian. A violation also may result in a report being made to law enforcement. In addition, an administrator may confiscate the device.
4. Students are responsible for keeping up with devices they bring to school. The school and/or district shall not be responsible for loss, theft, or destruction of devices brought onto school property.
5. Students shall comply with any additional rules developed by the school concerning appropriate use of personally owned electronic devices.

Any device connected to the district network is subject to monitoring by network administrators or the Director of Technology to review progress and for security purposes. The district does not guarantee and the user should not assume absolute privacy. Routine maintenance, updates, and support are the responsibility of the device owner, no technical support, troubleshooting, or repairs will be made by district employees on any student owned device.

The minimum requirements for any student owned device connected to the district network are as follows: the device must run an Apple, iDevice, Chrome, or Android based operating system, have a wireless network card, and must sustain battery power for at least two hours. Student owned devices that are part of an approved IEP, 504, or PSP document may be exempted from these requirements.

I. Employee Owned Devices:

Employees may be allowed to connect their personally owned devices to Warren County Schools Computer network provided they observe the following conditions:

1. Devices shall not be used in a manner that disrupts the educational or administrative process, including, but not limited to, use that:
 - a. Occurs during times of established instructional or assigned duties
 - b. Violates confidentiality or privacy rights of another individual,
 - c. Is profane, indecent, or obscene,
 - d. Constitutes or promotes illegal activity or activity in violation of school rules, or
 - e. Constitutes or promotes sending, sharing, or possessing sexually explicit messages, photographs, or images using any electronic device.
2. When employees violate the conditions of this policy, they shall be subject to disciplinary action, including, but not limited to, losing the privilege of bringing the device onto school property, reprimand, corrective action plan, and/or termination of employment. A violation also may result in a report being made to law enforcement for any suspected illegal activity.
3. Employees are responsible for keeping up with devices they bring to the workplace. The school and/or district shall not be responsible for loss, theft, or destruction of devices brought onto school property.
4. Employees shall comply with any additional rules developed by their direct supervisor concerning appropriate use of personally owned electronic devices.
5. Employees should not connect personally owned devices to other district equipment (e.g. projectors, interactive panels, displays) or resources. Repairs for any damage to district owned equipment resulting from a personal owned device shall be the financial responsibility of the employee.

Any device connected to the district network is subject to monitoring by network administrators or the Director of Technology to review progress and for security purposes. The district does not guarantee and the user should not assume absolute privacy. Routine maintenance, updates, and support are the responsibility of the device owner, no technical support, troubleshooting, or repairs will be made by district employees on any employee owned device.

The minimum requirements for any employee owned device connected to the district network are as follows: the device must run an Apple, iDevice, Chrome, or Android based operating system.

J. Rights:

In the event of a policy violation, the Superintendent or designee will evaluate the extent of the violation and take appropriate action. This action may include the suspension or closure of the student/employee account. The account holder must be notified in writing within two weeks of the reason for suspension or termination of an account. As specified in board policy, the account holder may request an appeal of the decision to close their account.

Part 5 -- District Sponsored Social Media Sites:

In order for employees and activity sponsors to utilize a district sponsored social networking site for instructional, administrative, or other work-related communication purposes, they must comply with the following:

1. Request prior permission in writing from the Superintendent.
2. If permission is granted, staff members will set up the site in a manner that allows the District Technology Office staff access to monitor and review site usage. In addition, staff members must also configure the site in a manner consistent with all school level/SBDM and/or direct supervisor requirements.
3. Staff members shall notify parents of the site and obtain written permission for students to become “friends” prior to the students being granted access to the site. This permission shall be kept on file at the school as determined by the building Principal.
4. 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.

Employees 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.

Part 6 -- Disclaimer:

A. Reliability:

WCPS shall not be responsible for any damages resulting from delays, non-deliveries, misdeliveries, or service interruptions resulting from the use of any electronic resource.

B. Security:

WCPS will take reasonable steps to assure individual privacy on the network but does not guarantee confidentiality and reserves the right to inspect all local and cloud-based accounts, files, and logs, as well as any/all connections to the district network. Security on any computer system is a high priority, especially when the system involves many users. If any user can identify a security problem, s/he must notify the Director of Technology or the school technology coordinator. Do not demonstrate the problem to any other users.

C. Archives/Backups:

Individual users are responsible for the archive/backup of all data that is critical to the performance of assigned job duties and/or completion of student assignments. WCPS shall not be responsible for any damages or disruptions resulting from loss of data from any electronic resource.

D. Access to Online Student Individual Learning Plans (ILP)

If requested, the District may enable a feature of the web based Individual Learning Plan (“ILP”) software, which allows students to invite third parties to have access to his/her ILP information or portions of such information via the web (internet). The purpose of this feature is to help students with career and college plans by permitting him/her to share ILP information with persons or organizations such as college admissions officers, organizations offering scholarships, and potential employers. The Family Educational Rights and Privacy Act (FERPA) and similar state statutes (KFERPA) generally require parents to consent before the educational records relating to their student(s) are disclosed to third parties. A completed Student Individual Learning Plan (ILP) Web Release Request Form shall be completed and returned to the school principal before this feature is enabled. The District, its employees, and agents shall not be responsible, nor shall they incur any liability for any disclosure made by the student using this software feature.

E. Google G Suite Service

Use of the WCPS sponsored G Suite services by shall be for instructional related assignments and duties only. Users are responsible for declining all sharing/collaboration requests that they receive which are not specific to a classroom/school sponsored assignment or job duty. Sharing of documents and communication with others by any of the G Suite collaboration tools without a specific classroom/school sponsored assignment or job duty is a violation of the AUP and may result in disciplinary action.

F. KDE Electronic Mail System for Students:

The Kentucky Department of Education requires the following statement related to student electronic mail accounts be included in district acceptable use procedures documentation.

The email solution is provided to your child by the district as part of the Office365 service from Microsoft. By signing this form, you hereby accept and agree that your child's rights to use the email service, and other Office365 services as the Kentucky Department of Education may provide over time, are subject to the terms and conditions set forth in district policy/procedure as provided and that the data stored in such services, including the email service, are managed by the district 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 District, 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 KDE/District and designated service providers or between the end user and the service provider. Before your child can use services provided direct to the end user, he/she must accept the providers Service Agreement and, in certain cases, obtain your consent. Data and activity related to a service not sponsored by KDE/District may not be subject to review without a court order.

Part 7 -- Internet Safety Procedures and CIPA Compliance

These Procedures are in place 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 personally identifiable information of minors; and (d) comply with the Children’s Internet Protection Act (“CIPA”).

This document is intended to be read together with the district’s Acceptable Use Policy and Acceptable Use Guidelines. All limitations and penalties set forth in the Acceptable Use Policies are deemed to be incorporated into this document.

A. Technology Protection Measures:

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors.

B. Access to Inappropriate Material:

To the extent practical, Technology Protection Measures (or “Internet filters”) shall be used to block/filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or in the case of minors, minimized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat, or circumvent the Technology Prevention Measures is punishable as a violation of the Acceptable Use Policies.

C. Inappropriate Network Usage:

To the extent practical, steps shall be taken to promote the safety and security of users of the Warren County School District online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions, and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the district’s Acceptable Use Policies and Acceptable Use Guidelines.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

D. Supervision and Monitoring:

It shall be the responsibility of all employees of the Warren County School District to supervise and monitor student usage of the district's computers, computer network, and access to the Internet in accordance with this Procedure and the district's Acceptable Use Policies. Procedures for the disabling or otherwise modifying and technology protection measures shall be the responsibility of the Director of Technology or designated representatives.

E. Education:

The Warren County Public Schools will advocate and educate employees, students and parents and the community on Internet safety, "cyber-bullying," and appropriate online behavior. Education will be provided through such means as professional development training and materials to employees, PTA presentations, and community outreach opportunities such as local public access television and School District websites.

Acceptable Use Guidelines Summary

(A copy of the complete Acceptable Use Procedures can be found on the district's web site.)

A. Privileges:

Access to the electronic resources of the Warren County Public Schools (WCPS) is a privilege not a right. Violation of the acceptable use policy may result in the immediate loss of any or all network services. In addition, any attempted or executed criminal violations on the network will be prosecuted to the fullest extent of the law.

B. General Responsibilities:

The use of your account must be in support of educational and research activities consistent with the objectives of the Warren County School District, access to educationally inappropriate materials is prohibited. Access to, sharing, or transmission of any material in violation of any federal or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, vulgarity, or material protected by trade secret. Use of your WCPS Internet account to play games (including online multi-user games) or participate in peer-to-peer file sharing (LimeWire, Kazaa, BitTorrent, etc.) is not acceptable. Use for product advertisement or political/religious statements that are not consistent with the educational purposes of the WCPS is inappropriate. In addition, use of electronic mail or WCPS account to buy, sell, or trade personal items is not acceptable.

C. Specific Network and Internet Responsibilities:

1. You may not give your password to anyone.
2. You may not use or alter any one else's account.
3. You may not offer Internet access to other individuals via your WCPS account.
4. You may not break in or attempt to break into other computer networks.
5. You may not intentionally spread embedded messages or other programs which have the potential of damaging or destroying programs or data.
6. You may not destroy another person's data.
7. Purposefully annoying other WCPS or Internet users is prohibited.
8. Harassment as defined in board policy shall not be allowed.
9. All communications and information accessible via the network is assumed to be for the individual consumption of the user, however, privacy is not guaranteed.
10. Collaborative documents shall only be shared with users who have specifically requested shared access. Intentionally sharing collaborative documents with users who have not requested access may be treated as bullying, hazing, and/or harassment.
11. Use of social networking web sites from district resources must be consistent with the educational objectives of the school district.
12. Notify the school principal or Director of Technology of any violations of this contract taking place by other users or outside parties. This may be done anonymously.

D. Specific Electronic Mail Responsibilities:

1. Be polite. Do not write or send abusive messages to others.
2. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
3. Do not reveal the personal address or phone number of other students or yourself.
4. Electronic mail is not guaranteed to be private. Network administrators have access to all mail messages. Any message relating to or in support of illegal activities shall be reported to the proper authorities.

E. Specific Employee Web Site Responsibilities:

Web sites created, maintained, and hosted on the electronic resources of WCPS should adhere to the following guidelines.

1. This is not a personal, private web site. The web site is to be used in support of educational and research activities consistent with the objectives of the Warren County School District.
2. If you have a "list of favorites" or an "about me" page where you are introducing yourself to your students, you have the right to determine your own favorites in such categories as books, authors, quotes, etc. as long as these items are representative of you and your profession.
3. You should refrain from posting religious or political statements about your personal beliefs.
4. Copyrighted materials shall not be posted on publicly available or WCPS intranet web sites.
5. District web sites which are not password protected should be considered available for public access. The material on publicly available sites is subject to federal accessibility and accommodation guidelines as well as potentially other federal/state law requirements. It is the specific employee's responsibility to ensure that sites comply with all applicable guidelines.

Acceptable Use Guidelines Summary - Continued

(A copy of the complete Acceptable Use Procedures can be found on the district's web site.)

F. Data Access Responsibilities:

Warren County Public School data must be managed, used, and protected in accordance with federal law, state law, and school district policies so as to ensure its integrity, availability, privacy, and confidentiality. Each employee, agent, or affiliate of Warren County schools, who handles data for the purpose of performing his/her job duties, or other functions directly related to his/her contractual affiliation with the district, is a steward of data and is responsible for the proper handling of data resources under his/her control.

G. Student Assigned Devices:

Any device/resource and its use is the responsibility of the student to whom it is assigned. Any violation of the acceptable use policy, procedures, or guidelines is the responsibility of the student. Violations occurring off school grounds on a "take-home" device will be addressed in the same manner as if the violation occurred on school property and during school hours.

H. Student Owned Devices:

Students who demonstrate an understanding of good digital citizenship may be allowed to connect their personally owned devices to Warren County Schools Computer network provided they observe all specified conditions. In addition, any device connected to the district network is subject to monitoring by network administrators or the Director of Technology to review progress and for security purposes. The district does not guarantee and the user should not assume absolute privacy. Routine maintenance, updates, and support are the responsibility of the device owner. No technical support, troubleshooting, or repairs will be made by district employees on any student owned device. The minimum requirements for any student owned device connected to the district network are as follows: the device must run an Apple, iDevice, Chrome, or Android based operating system, have a wireless network card, and must sustain battery power for at least two hours. These requirements are subject to change without notice.

I. Employee Owned Devices:

Employees may be allowed to connect their personally owned devices to Warren County Schools Computer network provided they observe all specified conditions. In addition, any device connected to the district network is subject to monitoring by network administrators or the Director of Technology to review progress and for security purposes. The district does not guarantee and the user should not assume absolute privacy. Routine maintenance, updates, and support are the responsibility of the device owner. No technical support, troubleshooting, or repairs will be made by district employees on any employee owned device. The allowed operating systems for any employee owned device connected to the district network are Apple Mac, iDevice, Chrome, and Android based operating systems. These requirements are subject to change without notice.

J. Rights:

In the event of a policy violation, the Director of Technology or school principal may suspend or close an account. Within two weeks, the account holder must be notified in writing of the reason for suspension or termination of an account. The account holder may request an appeal of the decision to close their account. For additional information see board policies found in the Student Code of Conduct, Personnel Policies for Certified Staff, and Personnel Policies for Classified Staff.

High School Student Independent Internet Access Account Request Form

Directions: Read and fill out the appropriate portions of the following contract completely and legibly. When complete, please return the contract to the sponsoring or homeroom teacher. It is the responsibility of the sponsoring teacher to forward the completed form to the school technology coordinator. A copy of this form is to be kept on file at the school. **Note: The signature of a parent or guardian is required for all students.**

Student Information:

Last Name: _____ First Name: _____ M.I.: _____

Student ID Number: _____

School: _____ Year of Graduation: _____ Grade: _____

I have read the Acceptable Use Policy for Electronic Resources and will abide by the conditions described in the policy. 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, school disciplinary action and/or appropriate legal action may be taken.

Student's Signature: _____ Date: ____/____/____

Sponsoring or Homeroom Teacher:

I have read the Acceptable Use Policy for Electronic Resources and agree to support this policy with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held solely responsible for all of the student's use of the network. However, as the sponsoring or homeroom teacher, I do agree to instruct the student in following the acceptable use policy and provide reasonable supervision of the student's actions.

Teacher's Name (please print): _____

Teacher's Signature: _____ Date: ____/____/____

Parent or Guardian:

As the parent or guardian of this student I have read the Acceptable Use Policy for Electronic Resources. I understand that this access is designed for educational purposes and the Warren County Public School District has taken reasonable precautions to eliminate access to controversial material. However, I also recognize it is impossible for the district to restrict access to all controversial materials and I will not hold them responsible for materials this student may acquire on the network. I hereby certify that the information contained on this form is correct and give my permission for the student named above to be issued an account. I further agree that use by this student shall not include any transaction which may result in criminal or financial liability for the Warren County Schools. If such does occur, the undersigned accepts full responsibility.

Parent or Guardian (please print): _____

Signature: _____ Date: ____/____/____

Daytime Phone Number: _____ Evening Phone Number: _____

Student Email Account Request Form

Directions: Read and fill out the appropriate portions of the following contract completely and legibly. When complete, please return the contract to the sponsoring or homeroom teacher. It is the responsibility of the sponsoring teacher to forward the completed form to the school technology coordinator. A copy of this form is to be kept on file at the school. **Note: The signature of a parent or guardian is required for all students.**

Student Information:

Last Name: _____ First Name: _____ M.I.: _____

Student ID Number: _____

School: _____ Year of Graduation: _____ Grade: _____

I have read the Acceptable Use Policy for Electronic Resources and will abide by the conditions described in the policy. 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, school disciplinary action and/or appropriate legal action may be taken.

Student's Signature: _____ Date: ____/____/____

Sponsoring or Homeroom Teacher:

I have read the Acceptable Use Policy for Electronic Resources and agree to support this policy with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held solely responsible for all of the student's use of the network. However, as the sponsoring or homeroom teacher, I do agree to instruct the student in following the acceptable use policy and provide reasonable supervision of the student's actions.

Teacher's Name (please print): _____

Teacher's Signature: _____ Date: ____/____/____

Parent or Guardian:

As the parent or guardian of this student I have read the Acceptable Use Policy for Electronic Resources. I understand that this access is designed for educational purposes and the Warren County Public School District has taken reasonable precautions to eliminate access to controversial material. However, I also recognize it is impossible for the district to restrict access to all controversial materials and I will not hold them responsible for materials this student may acquire on the network. I hereby certify that the information contained on this form is correct and give my permission for the student named above to be issued an account. I further agree that use by this student shall not include any transaction which may result in criminal or financial liability for the Warren County Schools. If such does occur, the undersigned accepts full responsibility.

The Kentucky Department of Education requires that parents/guardians agree to the following statement:

The email solution is provided to your child by the district as part of the Office365 service from Microsoft. By signing this form, you hereby accept and agree that your child's rights to use the email service, and other Office365 services as the Kentucky Department of Education may provide over time, are subject to the terms and conditions set forth in district policy/procedure as provided and that the data stored in such services, including the email service, are managed by the district 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 District, 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 KDE/District and designated service providers or between the end user and the service provider. Before your child can use services provided direct to the end user, he/she must accept the providers Service Agreement and, in certain cases, obtain your consent. Data and activity related to a service not sponsored by KDE/District may not be subject to review without a court order.

Parent or Guardian (please print): _____

Signature: _____ Date: ____/____/____

Student Assigned Device (Take-Home Use) Request Form

Directions: Read and fill out the appropriate portions of the following contract completely and legibly. When complete, please return the contract to the teacher responsible for device assignment. It is the responsibility of the sponsoring teacher to forward a copy of the completed form to the school technology coordinator. A copy of this form is to be kept on file at the school by the sponsoring teacher. **Note: The signature of a parent or guardian is required for all students.**

Student Information:

Last Name: _____ First Name: _____ M.I.: _____

Student ID Number: _____

School: _____ Year of Graduation: _____ Grade: _____

I have read the Acceptable Use Procedures for Electronic Resources Addendum and will abide by the conditions described. 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, school disciplinary action and/or appropriate legal action may be taken.

Student's Signature: _____ Date: ____/____/____

Parent or Guardian:

As the parent or guardian of this student I have read the Acceptable Use Procedures for Electronic Resources. I understand that this access is designed for educational purposes and the Warren County Public School District has taken reasonable precautions to eliminate access to controversial material. However, I also recognize it is impossible for the district to restrict access to all controversial materials and I will not hold them responsible for materials this student may acquire on the network. I hereby certify that the information contained on this form is correct and give my permission for the student named above to be issued "take-home" access to devices and resources owned by Warren County Public Schools. I further agree that use by this student shall not include any transaction which may result in criminal or financial liability for the Warren County Schools. If such does occur, the undersigned accepts full responsibility.

Parent or Guardian (please print): _____

Signature: _____ Date: ____/____/____

Daytime Phone Number: _____ Evening Phone Number: _____

Sponsoring Teacher:

Description of Electronic Resource (including serial number):

Teacher Name (please print): _____

Signature: _____

Date Equipment Assigned: ____/____/____ Date Equipment Returned: ____/____/____

Student Individual Learning Plan (ILP) Web Release Request Form
(only applies to students under the age of 18)

Directions: Read and fill out the appropriate portions of the following contract completely and legibly. When complete, please return the contract to the sponsoring or homeroom teacher. It is the responsibility of the sponsoring teacher to forward the completed form to the school technology coordinator. A copy of this form is to be kept on file at the school.

Student Information:

Last Name: _____ First Name: _____ M.I.: _____
Student ID Number: _____
School: _____ Year of Graduation: _____ Grade: _____

Parent or Guardian:

As the parent or guardian of the student named above, I hereby authorize the District to enable a feature of web based Individual Learning Plan (“ILP”) software, which will permit my student to invite third parties to have access to his/her ILP information or portions of such information via the web (internet). The purpose of this feature is to help my student with career and college plans by permitting him/her to share ILP information with persons or organizations such as college admissions officers, organizations offering scholarships, and potential employers. However, I understand this feature could permit my student to release ILP information to other third parties. I agree that the District, its employees, and agents shall not be responsible, nor shall they incur any liability for any disclosure made by the student using this software feature. The Family Educational Rights and Privacy Act (FERPA) and similar state statutes (KFERPA) generally require parents to consent before the educational records relating to their student(s) are disclosed to third parties.

I understand that the above software feature is not itself a disclosure of education records, but it will enable my student to disclose confidential educational records information. I specifically authorize and give my consent to the disclosure of ILP educational records information to third parties by my student through the use of the software feature as described above.

I understand that once this signed form is returned to the school, it will stay in effect as long as my child is enrolled in the District (unless I or my child on turning 18 requests a change).

I also understand that the sharing feature will not be enabled for my child unless this completed form is returned to the school. I further agree that the use of this feature by this student shall not include any transaction/activity which may result in criminal or financial liability for the Warren County Schools. If such does occur, the undersigned accepts full responsibility.

Parent or Guardian (please print): _____
Signature: _____ Date: ____/____/____

Community Member AUP Signature Form

I have read the Acceptable Use Policy for Electronic Resources and agree to follow the conditions outlined in this policy. I understand that I am responsible for my own personal behavior when using the WCPS electronic resources, including but not limited to the wide area network and the Internet. I realize that non compliance with terms of agreement or engaging in criminal activity via the network may result in loss of access privileges and/or civil or criminal prosecution.

Name (please print): _____

Signature: _____

Date: ____ / ____ / ____

A completed form for each community member should be kept on file at the district's Technology Office.

WCBE 08.2323.AP.5

Employee AUP Signature Form

I have read the Acceptable Use Policy for Electronic Resources and agree to follow the conditions outlined in this policy. I understand that I am responsible for my own personal behavior when using the WCPS electronic resources, including but not limited to the wide area network and the Internet. I further realize that I am responsible for reasonable supervision of student electronic resource use, including training in safe, acceptable online behavior. I acknowledge that non compliance with the terms of this agreement or engaging in criminal activity via the network may result in disciplinary or criminal action.

Employee Name (please print): _____

Signature: _____

School/Department: _____

Date: ____/____/____

This is an optional school level signature form that may be used in addition to the district employee handbook/personnel policies signature form. A completed form for each staff member may be kept on file by the School Technology Coordinator or Supervisor.