# Berkshire Local School District
# Computer Network and Internet Acceptable Use Policy
(STUDENTS)

This document constitutes the School District's Computer Network and Internet Acceptable Use Policy ("Policy"), and applies to all persons who use or otherwise access the Network and/or Internet, whether with District or personal equipment or whether on-site or by wireless or other remote access ("Users").

1. **Definitions.** For purposes of this Policy:

- ❏ The term "Network" shall mean the District's group of computers and peripherals, whether interconnected via cable, wireless and/or any other means whatsoever, all other District software and hardware resources including all Web-based material and all Web hosting, all data, databases and storage media, all standalone, portable and/or borrowed devices, and all provided connectivity between and among Users and from Users to the global Internet, including any and all Instructional Technology Centers or other third-parties providing connectivity and other services, and any and all identifiers, accounts, rights, permissions, and current or future hardware, software, or connectivity owned or managed by the District to which access is provided to Users.

  The rules of appropriate use and conduct created by this Policy apply to all District-owned computers and devices, even when such computers or devices are not connected with the Network. Such rules of appropriate use and conduct also apply to the use of privately-owned computers and mobile devices which are connected to the Network, communicate with Network Users by means of other non-District networks, or which are used in any way which is illegal, violates the Student Code of Conduct, or may be reasonably anticipated by District administrators to disrupt or materially interfere with school activities.

- ❏ The term "Use" of the Network shall mean any and all actions of a User which create traffic on the Network, including traces or remnants of traffic that pass through District equipment, wiring, wireless networks, or storage devices regardless of any other factor such as passage of time, user deletion, transit of the Network without storage or origination and/or storage on personal equipment.

2. **Purpose and Use**: The School District is providing Users access to its Network to support and enhance the educational experience of students. Access to system computers and the Network is a privilege, not a right. The District reserves the right to withdraw access at any time for any lawful reason. The District reserves the right to determine what constitutes an improper use of system computers or the Network, and is not limited by the examples of misuse given in this Policy. Users may violate this Policy by evading or circumventing the provisions of the Policy, alone or with others. If Users have any doubt about their obligations under this Policy, including whether a certain activity is permitted, they must consult with their building administrator to be informed whether or not a use is appropriate.

3. **Users Bound by Policy in Accepting Access**: The User consents to the terms of this Policy whenever he or she accesses the Network. Users of the Network are bound to the terms of this Policy regardless of whether they received and/or signed a copy of this Policy.

4. **Personal Responsibility:** Users are responsible for their behavior on the Network just as they are in a classroom, school hallway, or other School District property. Each User is responsible for reading and abiding by this Policy and any and all future amendments**,** which will be made readily available in both electronic and printed form. Anonymous use is not permitted and access (including passwords) may not be shared or transferred. If a

User suspects that a password is not secure, he or she must inform the building administrator immediately. Any improper use of your account, even if you are not the User, is your responsibility.

5. **Reporting Misuse of the Network**: Users must report any misuse of the Network to building administrator. "Misuse" means any apparent violation of this Policy or other use which has the intent or effect of harming another person or another person's property. This includes, but is not limited to, the transmission of sexually explicit images or messages which would constitute bullying, sexual harassment, or a violation of the Student Code of Conduct.

6. **Violating Policy with Personal Equipment:** The use of personal equipment and/or personal Internet access to violate this Policy or to assist another to violate the Policy is prohibited. Exceeding permission (such as abusing access to unfiltered Internet connectivity) is a violation of this Policy. Using private equipment to divert student time and/or attention from scheduled educational, co-curricular, or extracurricular activities, or to divert paid work time from its proper purpose, is always strictly prohibited. Personal equipment used to violate this Policy on school property is subject to search and seizure, reasonably related to the violation, for a period of up to [thirty (30)] days, unless the personal equipment has been provided to law enforcement officials.

7. **Discipline for Violation of Policy:** Violations of each of the provisions of this Policy are considered violations of the Student Code of Conduct, and each violation is a separate infraction. Violations may result in disciplinary action for students up to and including suspension or expulsion and/or referral to law enforcement. The District reserves the right to seek reimbursement of expenses and/or damages arising from violations of this Policy.

8. **Waiver of Privacy:** By accepting Network access, Users waive any and all rights of privacy in connection with their communications over the Network or communications achieved through the use of District equipment or software. Electronic mail (email) and other forms of electronic communication (including instant messaging, social media of all forms, and SMS messages originating from e-mail) are not guaranteed to be private. The District owns all data in the system. Systems managers have access to all messages and other data for purposes of monitoring system functions, maintaining system efficiency, and enforcing computer/network use policies and regulations, District policies, and state and federal laws. Illegal activities or suspected illegal activities may be reported to the authorities.

9. **Confidentiality and Student Information:** Users are responsible for maintaining security of student information and other personally identifiable data that they access, even if they access such data accidentally or without permission, and for upholding FERPA (20 U.S.C. § 1232g), the student confidentiality law (Ohio Revised Code Section 3319.321), the Ohio Privacy Act (Chapter 1347 of the Ohio Revised Code), and any other applicable privacy policies and regulations. Users are responsible whether such data is downloaded from the Network to their computer screen, transmitted by e-mail, stored on a flash drive, portable device or laptop, copied by handwriting or by any or all other devices, forms of storage or methods. Negligence with respect to protecting the confidentiality of such data will be considered a violation of this Policy whether or not such negligence results in identity theft or other harm. Users shall not engage or attempt to engage in unauthorized computer access, including but not limited to cyber-attacks, hacks, circumvention of password-protected content, and/or access to inappropriate material, including without limitation personally identifiable student information.

10. **District-Owned Equipment:** Desktop computers, laptops, portable devices, and other equipment belonging to the District are your responsibility. Any misuse, failure, damage or loss involving such equipment must be reported to the building administrator. Periodic maintenance on laptops and other hardware is required. It is your responsibility to make such equipment timely available for maintenance at the request of the building administrator. You may be held financially responsible for the expense of any equipment repair or replacement.

11. **Unacceptable Uses of the Network:** All Users must use the Network in an appropriate and responsible way, whether their specific actions are described in this Policy or not. Examples of unacceptable uses include, but are not limited to, the following:

- ❑ **OFFENSIVE OR HARRASSING ACTS**: Creating, possessing, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene, or pornographic materials, including but not limited to pictures, text messages, e-mails or sexually-oriented content ("sexting") in electronic or any other form. Using language inappropriate to the school environment, including swearing, vulgarities or language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening. Making, distributing or redistributing images, jokes, stories or other material that would violate this Policy or the School District's harassment or discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation, or other protected characteristics. Engaging in harassment, stalking, or other repetitive unwanted communication or using the Internet in support of such activities.

- ❑ **VIOLATIONS OF PRIVACY**: Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers of others, or intercepting communications intended for others. Copying, downloading, uploading, or transmitting student or School District confidential information.

- ❑ **CREATING TECHNICAL PROBLEMS:** Knowingly performing actions that cause technical difficulties to the system, other users or the Internet. Attempting to bypass school Internet filters or to "hack" into other accounts or restricted information. Uploading, downloading, creating, or transmitting a computer virus, worm, Trojan horse, or other harmful component or corrupted data. Attempting to hack, alter, harm, destroy or interfere with the normal operation of software, hardware, data, other District Network resources, or using the District Network or to do any of the same acts on the Internet or outside Networks. Downloading, saving, and/or transmitting data files large enough to impede the normal functioning of the computer or the Network (such as many music, video, image, or software files) unless given permission by the System Administrator. Moving, "repairing," reconfiguring, reprogramming, modifying, or attaching any external devices to Network equipment, computers or systems without the permission of the System Administrator. Removing, altering, or copying District software for personal use or for the use of others.

- ❑ **USE OF OUTSIDE SERVICES AND APPLICATIONS:** All e-mail, document storage, blogs, social media, or any and all other services and applications ("apps") must be provided or specifically authorized by the School District on its Network. The use of other providers of such functionality or storage (such as Yahoo) through the Network is prohibited.

- ❑ **VIOLATING LAW:** Actions that violate state or federal law or encourage others to do so. Offering for sale or use, soliciting the purchase or provision of, or advocating the use of any substance that the possession or use of is prohibited by law or District Policy. Seeking information for the purpose of creating an explosive device or biohazard, or communicating or seeking materials in furtherance of criminal activities, terrorism, or other threatening acts.

- ❑ **VIOLATING COPYRIGHT:** Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Users should assume that materials are protected under copyright unless there is explicit permission for use.

- ❑ **PERSONAL USE:** Personal shopping, buying or selling items, soliciting or advertising the sale of any goods or services, or engaging in or supporting any kind of business or other profit-making activity. Interacting with personal web sites or other social networking sites or tools that are not part of an

educational project, receiving or posting messages to web sites or other social networking or blog sites not part of an educational project, participating in any type of gaming activity, engaging in social or hobby activities, or general recreational web browsing if such browsing occurs during instructional time.

- ❑ **POLITICAL USE:** Creating, transmitting or downloading any materials that support or oppose the passage of a levy or a bond issue. Soliciting political contributions through the Network or conducting any type of official campaign business. Unless authorized by a teacher as part of an educational assignment, creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office.

- ❑ **GENERAL MISCONDUCT**: Using the Network in a manner inconsistent with the expectations of the Cardinal Local School District for the conduct of students in the school environment. Uses that improperly associate the School District with Users' personal activities or to activities that injure the District's reputation. Uses that mislead others or violate the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or using another's password or some other user identifier. Creating, possessing, copying, viewing, transmitting, downloading, uploading materials that cause or are likely to cause a substantial disruption of the educational environment, regardless of whether the User uses the Network or a personal or District-owned device.

12. **Specific Limits on Communication Over the District Network:**

- ❑ ***Expressing Opinion:*** The Network has been created at public expense and exists for purposes relating to education and administration. It does not exist to serve as a personal blog for the expression of opinions or as a public forum of any kind. It is not the intention of the District to allow the public, staff, or students to use the Network, including the web hosting or linking ability, for purposes of expressions of private opinions, or to support private or public causes or external organizations.

- ❑ ***Large Group Mailings:*** The sending of messages to more persons than is necessary for educational or school business purposes is a misuse of system resources and User time. Large group mailings, such as "all district" or "all building" are reserved for administrative use, subject to any exceptions which may be developed by the Administration or the System Administrator. Users may not send e-mails to more than ten (10) recipients in a single message, subject to exceptions developed by the Administration or the System Administrator. The System Administrator may also develop specific limitations on the use of graphics, the size, number, and type of attachments, and the overall size of e-mail messages sent on the system. The use of multiple messages, non-system addresses, or other techniques to circumvent these limitations is strictly prohibited.

- ❑ ***Electronic Signatures:*** Users shall not legally verify documents or use "electronic signatures" in any way unless they have been trained in an approved verification or signature system approved by the Administration. Users asked to legally verify or electronically sign documents should report the situation to the building administrator.

13. **System Security and Integrity:** The District reserves the right to suspend operations of the Network, in whole or in part, at any time for reasons of maintaining data security and integrity or any other lawful reason. The District reserves the right to block or filter any web sites, social networking sites, e-mail addresses, applications, servers or Internet domains which it, in its sole judgment, has determined to present a risk of exposing students or employees to sexually explicit or otherwise inappropriate content, exposing the system to undue risk of compromise from the standpoint of security or functionality, or creating a substantial likelihood of disruption of educational or co-curricular, or extracurricular activities.

14. **Filters:** The School will have the following in continuous operation, with respect to any computers belonging to the School and having access to the Internet:

a. A qualifying technology protection measure, as required by CIPA. The protection measures are designed to block or filter internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors; and
b. Procedures or guidelines that provides for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA. Such procedures or guidelines will be designed to:
a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
e. Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.

15. **Training Related to Online Behavior**: Pursuant to Federal law, students shall receive education about appropriate online behavior, including: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors while interacting with other individuals on social Networking websites, using e-mail, chat rooms, other forms of direct electronic communications, and cyberbullying awareness and response; (c) unauthorized access (e.g., "hacking") and other unlawful activities by minors on line; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

16. **No Warranties Created:** By accepting access to the Network, you understand and agree that the School District, any involved Information Technology Centers, and any third-party vendors make no warranties of any kind, either express or implied, in connection with provision of access to or the use of the Network. They shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any student arising out of that User's use of and/or inability to use the Network. They shall not be responsible for any loss or deletion of data. They are not responsible for the accuracy of information obtained through electronic information resources.

17. **Updates to Account Information:** You must provide new or additional registration and account information when asked in order for you to continue receiving access to the Network. If, after you have provided your account information, some or all of the information changes, you must notify the building administrator or other person designated by the School District to receive this information.

Legal Ref.: Ohio Rev. Code 3313.20, 3313.47, 3319.321
*Children's Internet Protection Act of 2000*, 47 USC § 254 (h), (l)
*Family Educational Rights and Privacy Act* (FERPA), 20 U.S.C. § 1232g

Revised: 08/10/17

**RECEIPT FORM**

I acknowledge receipt of the “School District Computer Network and Acceptable Use Policy” for students of the Berkshire Local School District (revised 08/10/17)

_____

Student Signature

Printed Name:_____

Date above signed:_____

_____

Parent/Guardian Signature

Printed Name:_____

Date above signed:_____