Ridgewood Local School District
Computer Network and Internet Acceptable Use Policy

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 interconnected via cable and/or wireless computers and peripherals, 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. Individual system computers are considered to be part of the "Network" and are subject to the terms of this Policy even when the User is not attempting to connect to another computer or to the Internet.

   - 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 and to facilitate work duties of employees. 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 the Supervising Teacher or Technology Coordinator 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 or not a copy was received and/or signed for by the User.

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 Supervising Teacher or

Technology Coordinator immediately. Any improper use of your account, even if you are not the User, is your responsibility.

5. Student Participation in Bring Your Own Technology (BYOT) Program.

As new technologies continue to change the world in which we live, they also provide many new and positive education benefits for classroom instruction. To enhance learning, students in grades 4 - 12 may now bring their own technology (BYOT) to campuses subject to the terms below:

- **Definitions.** For purposes of BYOT.
  - The term "Technology" means personally owned wireless portable electronic equipment used for ***instructional*** purposes. **All approved devices must allow access to the Internet through a fully functional web browser and be capable of accessing the Ridgewood student network.** Recognizing the rapidly changing world of technology, the list of allowed devices and district software will be reviewed annually. Allowed devices include (but are not limited to): tablet, laptop and netbook computers. Each device must be capable of running district used educational software. The district will provide access through Citrix to virtual productivity applications for all approved devices (both tablet and windows based).

- **Internet.** All Internet access shall occur using the Ridgewood student or staff network. Cellular network adapters (Verizon Wireless, AT&T, 3G wireless, 4G wireless, HotSpots etc.) **are not permitted** to be used by students to access the Internet **at any time.**

- **Security and Damages.** Responsibility to keep privately owned devices secure rests with the individual owner. Ridgewood Local Schools, its employees and agents, are not liable for any device stolen or damaged on campus. If a device is stolen or damaged, it will be handled through the school administrative office in the same manner as other personal items that are impacted in similar situations.

- **Student Agreement.** The use of personal technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, cell phone or other electronic device while at school. When abused, privileges will be taken away. When respected, privileges will benefit the learning environment.
  - Students and parents/guardians participating in BYOT must adhere to all Board policies and the *Ridgewood Local School District Computer Network and Internet Acceptable Use Policy.* Additionally:
    - Students must complete and submit a 'Request to Bring My Own Technology' form on-line at www.ridgewood.k12.oh.us.
    - Students take full responsibility for personal digital devices at all times. The school is not responsible for the security of the device.
    - The Ridgewood Local School District or its staff cannot provide any technical assistance on personally-owned devices. Users are directed to utilize their user manuals and other resources provided by their device manufacturer for technical assistance.

- The device must be in silent mode while on school campuses unless otherwise directed by the teacher.
- The device may not be used to cheat on assignments or tests or for non-instructional purposes during instructional time.
- The device may not be used to record, transmit or post photographic images or video of a person, or persons on campus during school activities and/or hours, unless otherwise directed by a teacher as part of a classroom assignment.
- The device may only be used to access files or internet sites which are relevant to the classroom curriculum. Non-instructional games are permitted at staff discretion.
- Students must comply with a teacher's request to turn off the device.

Students acknowledge and agree that:

- The school's network filters will be applied to the student network access to the internet and shall not be circumvented unless approved by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.
- The school district may collect and examine any device at any time when there are reasonable grounds for suspecting that there has been a violation of the terms of this agreement, the Student Code of Conduct, other school rules, or the law.
- Personal technology must be charged prior to bringing it to school, and the device must run off its own battery while at school.
- Students remain subject to all other school behavior rules, including but not limited to the Student Code of Conduct.

6. **Reporting Misuse of the Network**: Users must report any misuse of the Network to the Supervising Teacher or Technology Coordinator. "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.

7. **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 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 related to the violation and seizure for a period of up to thirty (30) days.

8. **Discipline for Violation of Policy:** Violations of each of the provisions of this Policy are considered violations of the Student Code of Conduct (or if an employee, of the contract of employment), 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, or up to termination and referral to law enforcement for employees. The District reserves the right to seek reimbursement of expenses and/or damages arising from

violations of these policies. Disciplinary action relating to employees is always subject to the provisions of any applicable collective bargaining agreement.

9. **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 (e-mail) and other forms of electronic communication (including instant messaging of all forms and SMS messages originating from email) are not guaranteed to be private. The District owns all data in the system. Systems managers have access to all messages 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.

10. **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.

11. **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 Supervising Teacher or Technology Coordinator. 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 Technology Coordinator. You may be held financially responsible for the expense of any equipment repair or replacement.

12. Active Restriction Measures. The School, either by itself or in conjunction with the Data Acquisition Site providing internet access, will utilize filtering software or other technology protection measures to prevent all users from accessing visual depictions that are (a) obscene, as that term is defined in 18 U.S.C. §1460; or (b) child pornography, as that term is defined in 18 U.S.C. §2256; and to prevent students from accessing visual depictions that are harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors, as determined by the Board and/or the Superintendent or designee. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 U.S.C. §254(h)(7)), as meaning any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The School District shall provide education to all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and regarding cyberbullying awareness and response.

13. 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, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene, or pornographic materials. 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 Technology Coordinator. Moving, "repairing," reconfiguring, reprogramming, modifying, or attaching any external

devices (including flash drives) to Network equipment, computers or systems without the permission of the Technology Coordinator. Removing, altering, or copying District software for personal use or for the use of others.

- **USE OF OUTSIDE SERVICES:** All e-mail, document storage, blogs or any and all other services must be provided 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. Outside document storage, such as Google Docs, and other services, such as blog hosting, may be used for instructional purposes only with the permission and supervision of a Ridgewood Local teacher as part of their curriculum.

- **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 or work project, receiving or posting messages to web sites or other social networking or blog sites not part of an educational or work 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 or designated work time.

- **POLITICAL USE:** Creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office or the passage of a levy or a bond issue. Soliciting political contributions through the Network or conducting any type of official campaign business.

- **GENERAL MISCONDUCT**: Using the Network in a manner inconsistent with the expectations of the Ridgewood Local Schools for the conduct of students and employees 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.

14. <u>Specific Limits on Communication Over the District Network:</u>

- ***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. The e-mail 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.

- ***Personal E-mail:*** Limited personal use of District e-mail by employees to communicate with family, friends, and colleagues who are willing recipients is permitted as a personal convenience, but must not impact paid work time and is subject to all of the provisions of this Policy. Misuse of the privilege is prohibited, and includes but is not limited to excessive volume, frequency, inappropriate content, mailing to unwilling addressees, or uses that may bring the District into disrepute. Violations will be determined in the sole discretion of the Superintendent. "Limited personal use" shall be defined as no more than ten (10) messages during any one day, with no attachments large enough to impede the normal functioning of the computer or the Network, as determined by the e-mail System Administrator. Exceptions to this limitation may be permitted for personal emergencies and other extenuating circumstances.

- ***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 Supervising Teacher or Technology Coordinator.

- ***Alternative Networks:*** No alternative network shall be created or used by any staff or student. 'Alternative Network' is defined as any wired or wireless network or sub-network located on or accessible from any Ridgewood Local Schools property that is not part of the primary network managed by the IT Department. All network equipment must be installed by the IT Department staff.

15. <u>System Security and Integrity</u>: 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, e-mail addresses, 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, or which exposes the system to undue risk of compromise from the standpoint of security or functionality.

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 or employee 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 Technology Coordinator or other person designated by the School District to receive this information.

18. **Records Retention and Production:** Users must comply with all District directions regarding the retention and management of e-mail or documents. **Instant messaging or text messaging for District business is prohibited.** All District employee e-mails are archived and retained.

19. **Web Sites:** Web sites created through the Network and/or linked with the School District's official web site must relate specifically to District-sanctioned activities, programs or events. Such web sites must be created according to District guidelines. Web sites created using the Network or the School District's equipment, or web sites created as part of a classroom or club assignment or activity are the sole and exclusive property of the School District in perpetuity without any ownership rights existing in the page creator(s). The School District reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed for any reason or for no reason, in the sole judgment of the Superintendent or Technology Coordinator. The School District does not intend to open web pages for the expression of opinion, and specifically does not intend for its web pages to be a public forum or limited public forum for students, staff, or citizens. Web pages exist solely in support of the School District functions and mission as determined by the Board**.**

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
Protecting Children in the 21st Century Act, 15 USC §6551, et seq.
Revised: 05/17/2013

cut here

RECEIPT FORM

I acknowledge receipt of the 'Computer Network and Internet Acceptable Use Policy' for the Ridgewood Local School District.

_____
User Signature

Print:_____

Date signed:_____

Please return to building secretary.