TECHNOLOGY SYSTEM USE AND INTERNET SAFETY POLICY

The Board of Education of Richmond-Burton Community High School District 157 hereby determines that it is in the best interest of the District, its personnel and its students, and members of the community to promote use of and familiarity with the District Technology System and with the services which are available through that System to support learning and enhance instruction, and to improve communications between the school and community.

Knowledgeable and appropriate use of the District Technology System can facilitate access to information resources available on-line, create innovative learning environments, and provide for worldwide communication. For purposes of this policy, implementing rules, and acceptable use guidelines, the term "District Technology System", "System", "District Electronic Network" or "Network" shall include all computer hardware and software owned or operated by the District, District electronic mail, District web sites, and District on-line services and bulletin board systems. "Use" of the District Technology System shall include use of or obtaining access to the System from any computer terminal whether or not owned or operated by the District.

The District Technology System was established to comprise part of the school curriculum, and is intended by this Board to function in support of that curriculum and of students' mastery of the curriculum through improved communication between the school and students' parents or guardians. The District Technology System does not constitute a public forum. The District reserves and retains the right to regulate the content of and links to the District Technology System. The District also has the right to and does monitor use of its Technology System. Except as provided by federal and state statutes protecting the confidentiality of students' education records, no user of the District Technology System has an expectation of privacy in connection with such use.

The Board of Education recognizes that although the Internet and on-line services afford access to legitimate sources of information for academic and educational purposes, they also enable access to materials which may be illegal, obscene or indecent. The use of elements of the District Technology System including the Internet shall be consistent with the District's educational mission and the curriculum adopted by the Board.

Acceptable Use Policy

Authorization for Electronic Network Access – Student Authorization

Each student must sign this Authorization as a condition for using the District's Electronic Network connection. Parent(s)/guardian(s) must also sign the Authorization before students will be granted unsupervised access. Please read this document carefully before signing.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Authorization for Electronic Network Access* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

1. **Acceptable Use** - Access to the District's electronic networks must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District, or (b) for a legitimate business use.
2. **Privileges** - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has this *Authorization* and may deny, revoke, or suspend access at any time; his or her decision is final.
3. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
   a. Using the network for any illegal activity, including but not limited to violation of copyright or other contracts with intent to plagiarize, or transmitting any material in violation of any U.S. or State law;
   b. Unauthorized downloading and/or installation of software, regardless of whether it is copyrighted or de-virused;
   c. Unauthorized or non-educational use of games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers or political lobbying;
   d. Downloading copyrighted material for other than personal use;
   e. Using the network for private financial or commercial gain;
   f. Wastefully using resources, such as file space;
   g. Hacking or gaining unauthorized access to files, websites, resources or entities and causing damage or loss;
   h. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature such as student records, names, addressed, phone numbers and pictures (Illinois Records Act 105 ICCS 101 1 et seq.);
   i. Using another user's account or password;
   j. Posting material authored or created by another without his/her consent;
   k. Posting and/or sending anonymous messages and emails that violate network etiquette rules;
   l. Using the network for commercial or private advertising;
   m. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material. Should a user inadvertently access such material he/she must report to school official;
   n. Using or attempting to use the network while access privileges are suspended or revoked;
   o. Posting material or incorporating non-district technologies without consent from the district technology director;
   p. Any and all technologies attached, connected, and/or installed to the district network without prior authorization from the technology director.

4. **Network Etiquette** - You are required to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
   a. Be polite. Do not become abusive, demeaning, profane or insulting in your messages to others.
   b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
   c. Do not reveal the personal information, including the addresses or telephone numbers of students or colleagues.
   d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal or inappropriate activities may be reported to the authorities.
   e. Do not use the network in any way that would disrupt its use by other users.
   f. Consider all communications and information accessible via the network to be District property.
5. **No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. **Indemnification** - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Authorization*.
7. **Sanctions** – Failure to abide by this policy may subject students to appropriate disciplinary measures for corrective action ranging from suspension or permanent revocation of network access privileges to suspension or expulsion. Violations of certain provisions in this policy may subject a member to possible civil and criminal liability according to applicable federal and state laws. When in appropriate use is determined by a supervisor or other administrator, the supervisor will notify in writing the technology director, who is authorized to terminate the user's access privileges.
8. **Security** - Network security is a high priority. No unauthorized personal equipment will be allowed. If you can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.
9. **Electronic Social Networking** – While home based sites, message boards, blogs, forums, and other uses of home based computers may be regarded as a benefit to a student's computer literacy, the student must be aware that using a non-district computer such that the use results in material and/or substantial disruption to the school or an individual will constitute grounds to investigate whether the use violates applicable law or district rules.
10. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses. Vandalism can also include physical damage to district owned equipment.
11. **Telephone Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
12. **Copyright/Web Publishing Rules** - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission. Fair Use Guidelines for multimedia will be abided by.
    a. Authorized users may create web pages as part of a class activity. Material presented on a class site must meet the educational objectives of the class activity. The district has the right to exercise control over the contents and/or style of said pages.

b. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

c. Students engaged in producing Web pages must provide their teacher with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

d. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.

e. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

f. Student work may only be published if there is written permission from both the parent/guardian and student.

g. Any web service created by the student must be district sponsored and authorized by the classroom teacher. All contents of said services must adhere to the strict guidelines of this acceptable use policy.

13. **Use of District Network and Systems**

a. The District's network, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides technology to aid students in fulfilling their duties and responsibilities, and as an education tool.

b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an account and its files is strictly prohibited.

c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the use of such traffic and how such traffic might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic traffic transmitted to external recipients.

e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of authenticity and the nature of the file so transmitted.

f. Files stored on the network and systems are the property of the district. Data may be accessed by the district to ensure strict adhesion to the AUP without prior authorization from the user.

g. Use of the School District's electronic mail system constitutes consent to these regulations.

14. **Internet Safety**

a. Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this Authorization, and otherwise follow this Authorization.

b. Students will be supervised while they are using District technologies and equipment, including the Internet, to ensure that they abide by the Terms and Conditions for Internet access contained in this Authorization.

c. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

d. No students should attempt to circumvent the filtering, the technology director shall monitor any and all Internet related traffic to ensure students comply with the AUP.

15. **Web 2.0 Tools**
    a. The use of blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes but is not limited to profanity; racist, sexist or discriminatory remarks.
    b. Students using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
    c. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
    d. Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the user profile, and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use that login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and follow these guidelines. Comments made on blogs will be monitored and - if they are inappropriate – deleted.
    e. Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
    f. Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat blog spaces as classroom spaces.
    g. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

AUTHORIZATION FOR ACCESS TO DISTRICT TECHNOLOGY SYSTEM BY STUDENTS

This form must be read and signed by each student and parent/guardian as a condition of using the District's Technology System.

By signing this Authorization:

- ✓ I acknowledge that I have received a copy of the "Technology System Use and Internet Safety Policy" and that I have read, understand, and agree to follow the guidelines.
- ✓ I acknowledge that access to the District Technology System is provided as a privilege by the District and that inappropriate use may result in my privileges being revoked and/or other disciplinary action.
- ✓ I acknowledge that I have no expectation of privacy in my use of the District Technology System and that the District has the right to, and does, monitor use of the system.
- ✓ I acknowledge that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material.
- ✓ In consideration for using the District's Technology System, and having access to public networks, I hereby release the School District and its Board Members from any claims and damages arising from my use of the Internet.

Student Name: _____

Student Signature: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____