

River Bend Comm. Unit District 2
Technology/Electronic Network Access
Rules and Regulations

The goal of technology at River Bend School District is to enhance, extend, and enrich the learning process and create new opportunities for teaching and learning. The Administration, staff, and students are encouraged to make use of all technology in order to accomplish these goals and to facilitate diversity and personal academic growth.

All use of electronic networks 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 prescribed behavior by Users. However, some specific examples are provided. **The failure of any User to follow the terms of the *Technology/Electronic Network Access Policy* or its implementing regulations may result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) on the Authorization forms is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms & Conditions

1. *Acceptable Use* – Technology usage and access to the District's electronic network must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District, or (b) for legitimate school use.
2. *Privileges* – The use of the District's technology and electronic networks is a privilege, not a right, and inappropriate may result in discipline, including, but not limited to, expulsion, suspension, or cancellation of access privileges, or any other disciplinary action provided by District policy or law. The Building Administration will make all decisions to deny, revoke, or suspend access privileges at any time; his or her decision is final.
3. *Unacceptable Use* – The User is responsible for his/her actions and activities involving the network and technology. Some examples of unacceptable uses are:
 - a) Using the network for any illegal activity, including violation of copyright or other laws or transmitting any material in violation of any United States or State law;
 - b) Unauthorized downloading of software, regardless of whether it is copyrighted or de-licensed;
 - c) Unauthorized installation or downloading and/or copying of copyrighted material or software on District computers;
 - d) Using the network for private financial or commercial gain;

River Bend CUSD #2

- e) Wastefully using resources, such as file space;
- f) Gaining unauthorized access to resources or entities;
- g) Invading the privacy of individuals;
- h) Using another User's account or password;
- i) Posting material authorized or created by another without his/her consent;
- j) Posting anonymous messages;
- k) Using the network for commercial or private advertising;
- l) Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
- m) Using the network while access privileges are suspended or revoked;
- n) Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the User intends to carry out such threat;
- o) Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information;
- p) Creating or forwarding chain letters, "spam," or other unsolicited or unwanted messages;
- q) Modifying, disabling, compromising, or otherwise circumventing any anti-virus, User authentication, or other security feature maintained on the District network or on any external computer, computer system, or computer account;
- r) Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on any computer;
- s) Using the computer network to participate in acts constituting "prohibited political activities" under the *State Officials and Employees Ethics Act* or "election interference" under the *Election Code* or to participate in any political activities that create an appearance of impropriety under those laws or under any ethics policy of the District relating to political activities of the District's employees;
- t) Any student use of an external computer account (including external e-mail accounts) not maintained by the District, whether or not the User is an authorized User of such external computer, computer system, or computer account, without a teacher's supervision; and
- u) Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

4. *Network Etiquette* – You are expected 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 in messages to others.
 - b) Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
 - c) Do not reveal the personal addresses or telephone numbers of students or colleagues.
 - d) Recognize that electronic mail (E-mail) is not private. Messages relating to or in support of illegal activities may be reported to the authorities.
 - e) Do not use the network in any way that would disrupt its use by other Users.
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 you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your 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 violation of this *Authorization*.
7. *Security* – Network security is a high priority. 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. Attempts to log-on to the Internet as system administrator will result in cancellation of User privileges. Any User identified as a security risk may be denied access to network.
8. *Vandalism* – Vandalism may 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.
9. *Copyright Web Publishing Rules* – Copyright law and District policy prohibit the re-publishing of copyrighted material found on the Web or on District Websites or file servers without explicit written permission.
 - a) For each re-publication (on a Website 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 creating 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.

- b) 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 Website displaying the material may not necessarily be the copyright owner.
- c) The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- d) Individual student pictures, examples of student work, and pre-arranged group photographs may not be published on the website unless there is an express written consent by parents/guardians and the student.
- e) Candid group pictures, crowd shots from school events, etc. may be published on the website at the discretion of the administration.

10. *Use of Electronic Mail* –

- a) The District’s electronic mail system, and its constituent software, hardware, and data files are owned and controlled by the School District. The School District may provide access to e-mail for students when appropriately supervised, and in conjunction with the school’s curricular goals. The School District will provide supervised access to email for staff members in fulfilling their duties and responsibilities, and as an educational 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 User to an electronic mail account 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 any 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 composition of such messages and how such messages 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 mail messages 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 or Building Administrator. Downloading any file attached to any Internet-based message is prohibited unless the User is certain of that message’s authenticity and the nature of the file so transmitted.

Internet Safety

1. Internet access is limited to only those “acceptable uses” as detailed in these procedures.
2. Staff members shall supervise students while students are using District Internet access.
3. The system administrator and Building Principals shall monitor Internet Access.
4. Students should not give out such personal information as their name, age, home address, telephone number(s), photograph, their parents’ or guardians’ work address or telephone number, or the name or location of the school over the Internet or through e-mail. Students should not give out such personal information about other individuals over the Internet or through e-mail.
5. Students should immediately inform their parents, guardians, or a member of District staff if they come across any information on the Internet or in an e-mail that makes them feel uncomfortable. Students should not respond to any e-mail or other message which makes them feel uncomfortable.
6. Students should never agree to meet someone in person whom they have “met” online without parental knowledge, permission, and supervision.
7. Students should never agree to send or accept any item to or from a person whom they have “met” online without parental knowledge, permission, and supervision.

Users and students’ parent(s)/guardian(s) need to sign this *Authorization* on an annual basis and/or after any amendment to the Policy or upon restoration of privilege that was been suspended, restricted or denied.

Technology Protection Measures

Consistent with the District’s legitimate educational and pedagogical concerns, the District shall implement technology protection measures, which may include filtering and/or blocking software, on every District computer which has access to the Internet. Such technology protection measures shall be implemented in the best manner practicable to prevent access to any material, including visual depictions, which is obscene; which constitutes pornography, including child pornography; or which, with respect to use of computers by minors, would be harmful to minors. The Superintendent, Building Principals, or their designees may disable the technology protection measure on an individual computer *during use by non-student adult* to enable access to material needed for bona fide research or other lawful purpose.

The District shall monitor the use of the computer network by students and any other minor Users in order to ensure compliance with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer network access promulgated the Superintendent or Building Principals, and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

Student Authorization for Technology/Electronic Network Access

User/Student Authorization

I understand and will abide by the above *Authorization for Technology/Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of technology/electronic network access, including e-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's technology/electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Technology/Electronic Network.

User Name (*Please Print*)

Grade Level

Date

User Signature

Parent/Guardian Authorization (Required if User is a student)

I have read this *Authorization for Technology/Electronic Network Access*. I understand that access is designed for educational purposes. Even though the District is committed to supervising student access, I also recognize that it is impossible for the District to completely control the content of data an industrious User may discover. I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this *Authorization* with my child. I hereby request that my child be allowed access to the District's Technology/Electronic Network.

Parent/Guardian Name (*Please Print*)

Date

Parent/Guardian Signature

Non-Student Authorization for Technology/Electronic Network Access

Non Student User Authorization

I understand and will abide by the above *Authorization for Technology/Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of technology/electronic network access, including e-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's technology/electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Technology/Electronic Network.

User Name (*Please Print*)

User Signature

Date_____