

# Student Agreement for the Acceptable Use of the District's Electronic Communications Systems

## Acceptable Use Policy

Birdville Independent School District provides a variety of electronic communications systems for educational purposes. **The electronic communications system is defined as the District's network (including wireless access), servers, computer workstations, peripherals, applications, databases, online resources, Internet access, electronic mail, digitized information, telecommunication devices, and any other technology designated for use by students, including all new technologies as they become available.** This also includes any access to the Birdville ISD electronics system while on or near school property, in school vehicles and at school-sponsored activities, and includes the appropriate use of district technology resources via off-campus remote access. Please note that the Internet is a network of many types of communication and information networks, including Web 2.0 resources (Blogs, Wikis, Podcasts, etc.), and is part of the district's electronic communications systems. Web 2.0 applications offer a variety of 21<sup>st</sup> century communication, collaboration, and educational creativity opportunities. With these educational opportunities comes responsibility. It is important that students and parents read the Birdville ISD Administrative Regulation for Acceptable Use and then ask any questions if help is needed understanding the policy. Inappropriate system use of the district's electronic communications system (see definition above) could result in the consequences listed below and/or loss of the privilege to use this educational tool. **Birdville Independent School District reserves the right to monitor all electronic activity.**

In accordance with the Children's Internet Protection Act, Birdville Independent School District educates staff and students regarding appropriate online behavior to insure Internet safety, including use of email and Web 2.0 resources, and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, harmful, or contain potentially offensive information. While every effort is made to provide the most secure and optimal learning environment, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content. **It is therefore each student's responsibility to follow the guidelines for appropriate and acceptable use.**

## Guidelines for Appropriate Use

- **Students must only open, view, modify, and delete their own computer files.**
- **Internet use at school must be directly related to school assignments and projects.**
- **Students will be assigned individual email and network accounts and must use only those accounts and passwords that they have been granted permission by the district to use. All account activity should be for educational purposes only.**
- **Students must immediately report threatening messages or discomfoting internet files/sites to a teacher.**
- **Students must at all times use the district's electronic communications system, including email, wireless network access, and Web 2.0 tools/resources to communicate only in ways that are kind and respectful.**
- **Students are responsible at all times for their use of the district's electronic communications system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them freedom to do otherwise.**

## Examples of Inappropriate Use

- Using the district's electronic communications system for illegal purposes including, but not limited to, **gambling, pornography, and computer hacking.**
- Disabling or attempting to **disable any system monitoring or filtering** or security measures.
- Sharing user names and passwords with others; and/or borrowing someone else's username, password, or account access.

- Purposefully opening, viewing, using, or deleting files **belonging to another system** user without permission.
- **Electronically posting personal information about one's self or others** (i.e., addresses, phone numbers, and pictures).
- Downloading or **plagiarizing copyrighted** information with permission from the copyright holder.
- **Intentionally introducing a virus or other malicious programs** onto the district's system.
- Electronically posting messages or accessing materials that are **abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.**
- Wasting or abusing school resources through unauthorized system use (e.g. **playing online games, downloading music, watching video broadcast, participating in chat rooms, etc.**).
- Gaining unauthorized access to restricted information or network resources.

### Special Note: Inappropriate Use: Cyberbullying

Cyberbullying is defined as the use of any Internet-connected device for the purpose of bullying, harassing, or intimidating another student. This includes, but may not be limited to:

- **Sending abusive text messages to cell phones, computers, or Internet-connected game consoles.**
- **Posting abusive comments on someone's blog or social networking site (e.g., MySpace or Facebook)**
- **Creating a Web page that masquerades as the victim's personal site and using it to embarrass him or her.**
- **Making it appear that the victim is posting malicious comments about friends to isolate him or her from friends.**
- **Posting the victim's personally identifiable information on a site to put them at greater risk of contact by predators.**
- **Sending abusive comments while playing interactive games.**
- **Taking photos — often using a cell phone camera — and posting them online, sometimes manipulating them to embarrass the target.**

### Consequences for Inappropriate Use

- Appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws including monetary damages.
- Suspension of access to the district's electronic communications system;
- Revocation of the district's electronic communications system account(s); and/or
- Termination of System User Account: the district may deny, revoke, or suspend specific user's access to the district's system with or without cause or notice for lack of use, violation of policy or regulations regarding acceptable network use, or as a result of disciplinary actions against the user.
- Possible criminal action

### Telephone

Students will be permitted to use office phones on an "emergency-only" basis, with the permission of an office staff member. In an effort not to interrupt teaching-learning time, only emergency messages will be delivered to students. Lunch money, required homework assignments, transportation plans, etc. should be finalized before leaving home in the morning.

### Textbooks

According to state law, each student and his/her parent shall be responsible to the teacher for all books, materials, or electronic communication devices not returned by the student. Any student failing to return all books, materials, or electronics CD's shall forfeit his right to free material until the materials previously issued but not returned are paid for by the parent. Lost materials shall be paid for by parents on the basis of the net contract price to replace the materials.

Students are responsible for the proper care of all books, materials and electronic communication