Fort Bend Independent School District

Digital Citizenship

Fort Bend Independent School District makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. These Digital Citizenship Guidelines are intended to minimize the likelihood of such harm by educating District students and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review. To learn proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. All District students shall be required to acknowledge receipt and understanding of all guidelines governing use of the system and shall agree to allow monitoring of their use and to comply with such guidelines. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the District's Digital Citizenship Guidelines as part of their review of the *Parent and Student handbook.* Campuses must provide training on the Digital Citizenship Guidelines to all students.

Definition of District Technology System. The District's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies
- Email accounts
- Servers
- Computer hardware and peripherals
- Software including operating system software and application software
- Digitized information including stored text, data files, email, digital images, and video and audio files
- Internal or external accessed databases, applications, or tools (Internet- or District-server based)
- District-provided Internet access
- District-filtered Wi-Fi
- New technologies as they are identified

Availability of Access

Acceptable Use. Computer/Network/Internet access used with District provided devices and/or personally owned devices will be to enhance learning consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use by all students regardless if the use is for an academic class requirement and/or personal use.

Privilege. Access to the District's computer/network/Internet is a privilege, not a right, and may be revoked if abused.

Any use described below is deemed "acceptable" and consistent with the Fort Bend ISD Digital Citizenship Guidelines for Technology but acceptable uses are not limited to the list below:

- Use is for educational purposes during the school day.
- Users will comply with all software, licenses, copyrights, and all other state and federal laws governing intellectual property.
- Use is limited to the student's own individual account. Students should not share network login information with others or use another person's login information to access the network or computer.

Access to Computer/Network/Internet. Access to the District's electronic communications system, including the Internet, shall be made available to students for instructional purposes. District computers and Wi-Fi (available for students who bring their own personal telecommunication devices) have filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA.

Student Access. Computer/Network/Internet access is provided to all students as defined by the parent selection on the yearly consent form as part of the Parent and Student Handbook. Student Internet access will be under the direction and guidance of a District staff member. Students may also be allowed to use the local network and Wi-Fi with campus

permission using guidelines outlined in this document.

Use of Personal Telecommunication Devices. The District believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information. On an as available basis, students will be provided access to a filtered, wireless network through which students will be able to connect personal telecommunication devices to a designated network. Students using personal telecommunication devices must follow the guidelines stated in this document while on school property, attending any school-sponsored activity, or using the Fort Bend ISD networks.

- **Designated Instructional Areas**– Students are allowed to bring personal telecommunication devices that can access the guest filtered wireless Internet, as available. Students will be allowed to use the device for educational purposes in a digitally responsible manner**.**
- **Designated non-Instructional Areas/Times –** Students are allowed to bring personal telecommunication devices that can access the guest filtered wireless internet, as available. Students will be allowed to use the device as determined by the campus.

Security. A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Digital Citizenship guidelines may be denied access to the District's networks. Other consequences may also be assigned. A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's networks and will be subject to disciplinary action in accordance with the FBISD Discipline Management Techniques and Student Code of Conduct.

Content/Third-Party Information. Students and parents of students with access to the District's networks and resources should be aware that use of the resources may provide access via links to outside material not yet reviewed or approved by the District.

Subject to Monitoring. No District computer/network/Internet usage shall be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Students should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the District computer system and networks will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Students should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose. Personal telecommunication devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Digital Citizenship guidelines have been violated.

Rules for Responsible Digital Citizenship

Fort Bend Independent School District offers students access to a computer, District network and the Internet. District students are bound by all portions of the Responsible Digital Citizenship Guide. A student who knowingly violates any portion of the Responsible Digital Citizenship Guide will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the District's Discipline Management Techniques and The Student Code of Conduct.

The District provides a web filtering software to protect students from accessing inappropriate material. While the purpose of the District network is to use Internet resources for constructive educational goals and instructional activities, no web filtering software can provide 100% protection. The District strives to provide a safe online environment for all students and to protect them from inappropriate content. We will constantly monitor our system and implement new technologies that will strengthen the safeguards currently in place. Fort Bend Independent School District believes however that the educational and instructional benefits that faculty, staff, and students derive from access to the Internet far exceed any disadvantages associated with this privilege.

By utilizing a variety of technological resources, including the Internet, Intranet, hardware, and software, Fort Bend Independent School District is expanding educational opportunities for all stakeholders. With this opportunity come responsibilities regarding responsible digital citizenship. Each Fort Bend Independent School District user is expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use on the Internet, Board Policy, and with the laws of The State of Texas and The United States.

Individual User's Responsibilities. The following rules will apply to all users of Fort Bend Independent School District's system:

1. Students must comply with all software licenses, copyright laws, and all other state and federal laws governing intellectual property.

2. Students may not install/upload/download onto network drives, disks, or any District computer network or run from a USB drive software, shareware, freeware, music files, or an executable, such as software and games, or proxy site software without permission from a teacher or administrator for academic use.

3. Network administrators have the right to search student network storage locations and review data to maintain system integrity to ensure that students are using the system responsibly.

4. Students are prohibited from changing any computer configurations and/or settings.

5. Students are prohibited from accessing, copying or deleting anyone else's files.

6. Students are prohibited from recording audio or video without consent of both the person(s) being recorded and the teacher/administrator.

7. Students are prohibited from including any profane, abusive/bullying, or impolite language in any files or folders stored on any District network or file storage space.

8. Students are prohibited from accessing materials and sites which are not in line with the permitted use as defined by the teacher or administrator and Digital Citizenship guidelines. This is to include but not limited to Social Networking Sites.

9. Students are prohibited from damaging any computer, peripheral or the network in any way.

10. The individual in whose name a system account is issued will be responsible at all times for its proper use.

11. Students are prohibited from sharing their network password with another person. Students are only allowed onto the District network using their own login credentials.

12. Students are not allowed to use another user's password/login credentials.

13. Students are not allowed to access non-District approved social networking or social media sites while using a computer connected to the Fort Bend ISD network. Students may participate in District approved social networking and social media activities that are related to instructional goals/activities. In this capacity, students may utilize tools such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and other digital tools.

14. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, bullying, or disrespectful language in email communications, blogs, wikis, or other electronic communication tools and the use of electronic communication or websites to threaten students, employees, volunteers, or school safety is prohibited (even if the offense is initiated off school property). This is to include but is not limited to Social Networking Sites.

15. Accessing proxy sites or any other sites which hide the user's identity is prohibited.

16. Any attempt to access or circumvent password or other security-related information associated with the District, students, or employees, or to upload or create computer viruses (even if the offense is initiated off school property) is prohibited.

17. Any attempt to alter, destroy, or disable district computer equipment, district data, the data of others, or networks connected to the district's system, (even if the offense is initiated off school property) is prohibited.

18. Harassing, fraudulent, embarrassing, indecent, profane, obscene, intimidating, inaccurate, sexually threatening, offensive, discriminatory, prejudicial, material that is damaging to another person's reputation, illegal, or other unlawful material may not be sent by e-mail or other form of electronic communication or displayed on or stored in the District's computers (even if the offense is initiated off school property). Users encountering or receiving such material should immediately report the incident to a teacher or campus administrator.

19. If a security problem in the District's system is identified or materials which violate the Rules for Responsible Digital Citizenship are encountered, it must be reported to a teacher or campus administrator immediately.

Inappropriate Use of Digital Resources. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to, threatening, harassing, defamatory or obscene material; copyrighted material; plagiarized material; commercial material or product advertisements; political lobbying; materials protected by trade secrets; blog posts, web posts, or discussion forum/replies posted to the Internet which violate federal or state law and illegal activities.

Inappropriate use includes, but is not limited to, violations of the law, uses specifically listed in this document, violations of network etiquette, or uses that obstruct the security or integrity of the FBISD network and all components connected to it. The following rules will apply to all users of Fort Bend Independent School District's system, and violations of these rules will result in revocation of the user's access to the District network and all connected components.

1. Violation of the District's Digital Citizenship guidelines for computer/computer resources or Internet access and/or any rules or agreements signed by the student or the student's parent.

2. Attempting to access or circumvent passwords or other security-related information of the District, students, or employees, and/or to write, produce, generate, copy, or introduce any computer code or virus for the intent to self-replicate, damage, or harm the performance of the network or computers.

3. Attempting to alter, destroy, or disable District computer equipment, District data, the data of other, or other networks connected to the district's system at any time, including off school property.

4. Attempting to use the District's computer equipment to access or distribute the personal data of students or employees.

5. Using the Internet or other electronic communication to threaten and/or bully District students, employees, or volunteers at any time, including off school property.

6. Sending or posting electronic messages, images, audio files or video files that are abusive, disruptive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal at any time, including off school property.

7. Using District or personal technology for cheating or plagiarism.

8. Sending an electronic communication that references a name, domain address, phone number, or other item of identifying information belonging to any person with the intent to reveal the personal identity, harm, or defraud any person.

9. Using e-mail/web sites at school to encourage illegal behavior or threaten school safety.

10. Downloading any application not approved by the District, including but not limited to the purpose of bypassing the District-approved filter.

11. Using the District's technology resources to post, publicize, or duplicate information in violation of copyright law.

12. Attempting to acquire and use the credentials of another individual to log on to the computer network, whether it is a student, administrator, or District employee.

13. Using of the District computer system for any type of advertisement or selling of commercial or personal products or services.

14. Accessing, modifying, copying, or deleting files and/or data belonging to another individual.

Consequences of Digital Citizenship Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken. Students may be held financially responsible for intentionally causing damage to District resources.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building administrator, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Student Safety

Use of personal telecommunication devices during a campus drill or emergency will not be permitted.

To ensure the safety of students, headsets and earbuds are not allowed in non-instructional areas unless approved by a teacher or administrator.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

The District is not responsible for theft or damage to a student's personal device. Administrators will not investigate or conduct searches involving stolen or lost personal devices.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.