Bright Local Schools Student Technology Acceptable Use and Internet Policy

The Bright Local School District believes that technology and its utilization enhances the quality and delivery of education and is an important part of preparing children for life in the 21st century. The community of technology users must understand that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable educational tool, there are sections that are not commensurate with community, school, or family standards. The District believes that the Internet's advantages far outweigh its disadvantages and will provide an Internet filtering device which blocks access to a large percentage of inappropriate sites. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, the District considers access to the Internet and computer resources a privilege, not a right. Therefore, users violating the District's Acceptable Use Policy (AUP) may be subject to revocation of these privileges and potential disciplinary action. The District also reserves the right to report any illegal activities to the appropriate authorities. Students will not engage in any act which would constitute a violation of any law, Federal or State, Board policy or the Student Code of Conduct. Ultimately, parents and guardians of minors are responsible for conveying the standards that their children should follow when using media and information sources and upholding the published standards of the District. All students must have a current, signed AUP on file with their school of attendance or they will not be permitted to access the District Network or the Internet.

All Acceptable Use Policies also apply to any online service provided directly or indirectly by the district for student use, including but not limited to: Email, Google Apps for Education (Gmail, Docs, Calendar, etc.), ProgressBook (Parent/Student Grade Book Access), INFOhio, Blackboard, or any future educational online applications.

Acceptable Uses and Terms of the Permitted Use

General

• Computer/Internet sessions will be supervised by a teacher.
• Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material. Attempting to bypass the school's content management filter is prohibited.
• Disrupting or damaging equipment hardware/software or the operation of the system, such as, changing the configuration of an individual network device is prohibited.
• The school district may regularly monitor students' Internet usage.
• Students will be provided with training in the area of Internet safety.
• Uploading and downloading of non-approved software will not be permitted.
• Virus protection software will be used and updated on a regular basis.
• The use of personal personal hard drives/USB drives/flash drives or other digital storage media including online in school requires a teacher's permission.
• Cyberbullying is prohibited. Cyberbullying is the use of information and communication technologies such as e-mail, cell phones, text messages, instant messages, personal websites, social media sites to support deliberate, repeated, and hostile behavior by an individual or group, whose intended to threaten, harm others or which causes emotional distress to an individual to substantially disrupt or interfere with an individual student's ability to receive an education. Students will treat others with respect at all times and will not undertake actions that may bring the District into disrepute.

Network

• Students will access the Network and Internet with specific teacher permission and supervision and further understand that activities on any school computer may be observed directly or remotely.
• Students will not access or use files, utilities or applications capable of altering intended computer or Network performance, settings or access. Students will not use or attempt to gain unauthorized access to student, faculty or administrative passwords; folders, work, files, or accounts; Network administrative programs or equipment; and will only use assigned student accounts..
• Students will refrain from using the Network for financial gain, political gain, and commercial activity or for any illegal activity.
• Students will not participate in ”Hacking” and other illegal activities in attempt to gain unauthorized access to restricted files, other computers or computer systems. Uploading any harmful form of programming, such as a virus, spyware, malware, installing any type of server, aliasing / spoofing, peer-to-peer networking or remote-control software is prohibited.
• Possession of and/or distribution of any of software tools designed to facilitate any of the above actions will also be considered an offense.
• Students will not create a mobile “hot-spot” or utilize a “proxy site” for the purpose of bypassing network safety measures and filtering tools.

World Wide Web

• Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials observing all district Internet filters and posted network security practices.
• Students will report accidental accessing of inappropriate materials in accordance with school procedures.
• Students will use the Internet for educational purposes only.
• Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
• Students will never disclose or publicize personal information.
• Students will only download materials or images relevant to their studies.
• Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or Network management reasons.

Email

• Students will use approved school email accounts under supervision by or permission from a teacher.
• Students will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
• Students will not reveal their own or other people’s personal details, such as addresses or telephone numbers or pictures.
• Students will note that sending and receiving email attachments is subject to permission from their teacher.

Social Networking

• Students will only have access to chat rooms, discussion forums, Weblogs, messaging or other electronic forms of communication that have been approved by the District and will only be used for educational purposes.

Internet Safety Policy - “Say What You Do, Do What You Say”

Introduction

• It is the policy of Bright Local School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

• Key terms are as defined in the Children’s Internet Protection Act.

Access to Inappropriate Material

• To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.
• Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
• Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

• To the extent practical, steps shall be taken to promote the safety and security of users of the Bright Local School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
• Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

• It shall be the responsibility of all members of the Bright Local School District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act.
• Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of BLSD Technology Department or designated representatives.
• The BLSD Technology Department or designated representatives will provide age-appropriate training for students who use the Bright Local School District’s Internet facilities. The training provided will be designed to promote the Bright Local School District’s commitment to:

a. The standards and acceptable use of Internet services as set forth in the Bright Local School District’s Internet Safety Policy;
b. Student safety with regard to:
    i. safety on the Internet;
    ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
    iii. cyberbullying awareness and response.
c. Compliance with the E-rate requirements of the Children’s Internet Protection Act (“CIPA”).

• Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Please sign and return

STUDENT ACCOUNT AGREEMENT

Print Student Name_____Grade_____

Student ID #_____D.O.B._____
I have read the Bright Local School District Acceptable Use Policy. I agree to follow the rules contained in this policy. I understand that if I violate the rules, my account can be terminated and I may face other disciplinary measures.

Student Signature_____ Date_____

PARENT OR GUARDIAN SECTION

I have read the District Acceptable Use Policy. I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims or damages of any kind whatsoever arising from my child's use of, or inability to use, the District system, including, but not limited to, claims that may arise from the unauthorized use of the system to offer, provide, or purchase products or services. I will instruct my child regarding any restrictions against accessing material that are in addition to restrictions set forth in the District Acceptable Use Policy. I will emphasize to my child the importance of following the rules for personal safety. I give permission for my child to access Bright Local's Technology Services and certify that the information on this form is correct.

Print Parent/Guardian Name_____Phone_____

Parent/Guardian Signature_____Date_____

Updates
• Students and/or parents and guardians may be asked from time to time to provide new or additional registration and account information or to sign a new Acceptable Use Agreement, for example, to reflect developments in the law or technology. The Board shall make every effort to communicate and explain all changes in a timely manner.

Adoption
• This Internet Safety Policy was adopted by the Board of Bright Local School District at a public meeting, following normal public notice, on May 15, 2013.