Bright Local Schools Staff 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. This is an example of collaboration. This is in real time.

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. Staff will not engage in any act which would constitute a violation of any law, Federal, State, or Board policy. All Staff must have a current, signed AUP on file with their school 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 staff use, including but not limited to: E-mail, Calendar and Docs (Google Apps for Education), ProgressBook, INFOhio, Blackboard, or any future educational online applications.

Acceptable Uses and Terms of the Permitted Use

General

• 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 Internet usage.
• 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's ability to work or receive an education. Staff will treat others with respect at all times and will not undertake actions that may bring the District into disrepute.

Purpose and Use

The school district is providing you access to its Network primarily to support legitimate district business. Other brief, incidental and personal uses are permitted from time to time (e.g., receiving an email from a spouse regarding a change in dinner plans, or from a son or daughter about the starting time of a track meet.) Uses that interfere with normal district business or violate district policies are strictly prohibited, as are uses for the

purposes of engaging in or supporting any kind of business or other profit-making activity. If you have any doubt about whether a contemplated activity is permitted, you may consult with the building administrator or the district's technology supervisor to help you decide if a use is appropriate.

Network

• Staff will not access or use files, utilities or applications capable of altering intended computer or Network performance, settings or access. Staff 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 accounts..
• Staff will refrain from using the Network for financial gain, political gain, and commercial activity or for any illegal activity.
• Staff 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.
• Staff will not create a mobile "hot-spot" or utilize a "proxy site" for the purpose of bypassing network safety measures and filtering tools.

Websites

Websites created through the Network and/or linked with the school district's official web site must relate specifically to district-sanctioned activities, programs or events. Websites created using the Network or the school district's equipment, or web sites created as part of a classroom or club assignment or activity are the sole and exclusive property of the school district. The school district reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed. As appropriate, the school district may also request such a disclaimer on external web sites that relate directly to school district activities, programs or events.

World Wide Web

• Staff 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.
• Staff will report accidental accessing of inappropriate materials in accordance with school procedures.
• Staff will use the Internet for educational purposes only.
• Staff will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
• Staff will never disclose or publicize personal information.
• Staff will only download materials or images relevant to their studies.
• Staff 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

• Staff will use approved school email accounts.
• Staff will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
• Staff will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

Social Networking
• Staff will only have access to chat rooms, discussion forums, Web logs, 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 training for staff 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. Staff 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 staff member will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Updates

• Staff 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.

Please sign and return

STAFF Technology Acceptable Use and Internet Policy

To access email and/or the Internet at school, staff members must sign and return this form. Use of the Internet is a privilege, not a right. The Board's Internet connection is provided for business, professional and educational purposes only. Unauthorized or inappropriate use will result in a cancellation of this privilege.

The Board has implemented the use of a Technology Protection Measures, which is a specific technology that will protect against (e.g., block/filter) Internet access to visual displays that are obscene, child pornography or harmful to minors. The Board also monitors online activity of staff members in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The Superintendent or Technology staff may disable the Technology Protection Measure to enable access for bona fide research or other lawful purposes.

Staff members accessing the Internet through the Board's computers/network assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet. The Board reserves the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the Board's computers/networks. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
To the extent that a staff member has the proprietary rights to the design of a web site hosted on the Board's servers , the staff member agrees to license the use of the web site by the Board without further compensation.

Please complete the following information:
Staff Member's Full Name (please print): _____
School:_____

I have read and agree to abide by the Staff Network and Internet Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy is inappropriate and may constitute a criminal offense. As a user of the Board's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Staff Member's Signature:_____ Date: _____

The Superintendent and School Board is responsible for determining what is unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the Board's Staff Network and Internet Acceptable Use and Safety Policy and related Guidelines and take such other disciplinary action as is appropriate pursuant to the applicable collective bargaining agreement and/or Board Policy.