| Bridges Charter School | Board Policy<br>**Acceptable Use and Internet Safety** | |
|---|---|---|
| **Policy Number:**<br>**BP 6163.4** | **Adopted**<br>**8-21-17** | **Revised:** |

**PURPOSE:**
Bridges Charter School ("BRIDGES") believes in the educational value of technology and recognizes its importance for supporting curriculum instruction and management. The BRIDGES network has been developed to promote educational excellence, innovation and communication for students and staff.

**SCOPE:**
Internet access, electronic mail (e-mail), computers, iPods, iPads, emerging technology and network resources are available to teachers, administrators, and students at BRIDGES solely for educational and instructional purposes and other purposes consistent with the educational mission of the school.

**GENERAL POLICY STATEMENT:**
It is BRIDGES intent to protect students and staff from inappropriate information by:

1) Meeting or exceeding all state and federal content filtering guidelines
2) Requiring adult supervision and monitoring of student Internet use
3) Directing each user to accept personal responsibility for managing the resources appropriately.

**POLICY DETAILS:**
The following provisions specify the expectations for all users of the BRIDGES network. The Student's and Adult's use of the network at school is a privilege conditioned on the Student and Parent/Guardian/Adult agreeing to and abiding by the conditions. All users must sign the Acceptable Use Agreement specifying user obligations and responsibilities in order to access the network.

1. Use of technological information resources must be for educational purposes, research, communication, and support the educational goals and objectives of BRIDGES
2. Illegal activities of any kind are strictly forbidden.
3. Inappropriate activity or use will be grounds for disciplinary action as per BRIDGES policy. The Director or designee shall make all decisions regarding whether or not the user has violated the Acceptable Use and Internet Safety Policy. His/her decision shall be final.
   - 3.1 Users will not transmit any material in violation of the law, including copyrighted, threatening or obscene material.
   - 3.2 The BRIDGES network may not be used for personal financial gain, advertising or political activities.
   - 3.3 Users may not interfere with or bypass the security of filtering systems used to protect the BRIDGES network.

3.4 Users must notify their teacher/specialist or administrator if they identify a security problem.
3.5 Any user identified as a security risk will be denied access to the information system.
3.6 Users may not send chain letters, annoying or unnecessary messages, and they may not send unnecessary mail to a large number of people.
3.7 Users may not download programs to the network or any computer or iPod or iPad from either software or the Internet without securing approval.
3.8 Users will be polite abiding by the BRIDGES Core Values at all times, and will never send or encourage others to send abusive messages.
3.9 Users must use appropriate language: never swear, use suggestive, threatening, obscene or other offensive language.
3.10 Users must not make any attempt to harm or destroy data or equipment. Any such vandalism will result in loss of network use and will be grounds for disciplinary action as per BRIDGES policy.

4. Network privacy
   4.1 Users must never reveal any person's home address, phone number or other important personal information.
   4.2 Users must never ask for personal information from another person.
   4.3 The BRIDGES network may not be used in any way that would disrupt others.
   4.4 All BRIDGES network systems and files are BRIDGES property.
      4.4.1 User email is not guaranteed to be private
      4.4.2 Sending or receiving encrypted or encoded messages is strictly forbidden.
      4.4.3 Users shall not read other users' email or files.
      4.4.4 Users shall not attempt to interfere with other users' ability to send or receive e-mail, nor shall they attempt to delete, copy, modify or forge others' mail.
      4.4.5 Abusive or threatening e-mail messages may be turned over to law enforcement.

5. Cyber-bullying is a term used to refer to bullying over electronic media. Cyber- bullying is willful and involves recurring or repeated harm inflicted through electronic text. Cyber-bullying will be grounds for disciplinary action as per BRIDGES policy and California Education Code §§ 32261, 32265, 32270, and 48900 .
   5.1 Users shall not use the system to threaten, intimidate, harass, or ridicule other students or staff. (Penal Code 653.2 makes it a crime for a person to distribute personal identification or information electronically with the intent to cause harassment by a third party and to threaten a person's safety or that of his/her family.)
      5.1.1 Users must not continue to send e-mail to someone who has said they want no further contact with the sender.
      5.1.2 Users must not threaten, "put down", or use hate-motivated speech at any time when using electronic media.
      5.1.3 Users must not publish the personal contact information of any one.
      5.1.4 Users must not assume the identity of any other person for the purpose of publishing material in their name that defames or ridicules them.

**NON-COMPLIANCE TO POLICY:**
Non-compliance to this policy by a student will result in the disciplinary actions defined in the BRIDGES Student Code of Conduct and Discipline policy. Lack of adherence to this policy by BRIDGES personnel may result in the employee being subject to disciplinary action in accordance with Board disciplinary policy and administrative regulations.

**GOVERNANCE:**
BRIDGES staff shall enforce the Acceptable Use and Internet Safety Policy fairly and consistently among all students. Sections of this Policy will be printed and distributed as part of the annual back to school packet and must be signed by Student and Parent/Guardian prior to use of any technology on the BRIDGES campus.

**REVISION HISTORY:**