Bridges Charter School	Board Policy- Acceptable Use & Internet Safety	
Policy Number: AR 6163.4	Adopted: 8-21-17	Revised:

Bridges Charter School is pleased to provide computer and network services to support its instructional program and to further student learning. Students, faculty, staff and administration will have the opportunity to access educational resources, to present information, and to work collaboratively with peers and experts internationally. The computer and network facilities are to be used in a responsible, efficient, ethical, and legal manner. **Students and parents are required to review this document**, as well as sign the accompanying agreement to insure best practices and professional conduct regarding computer and network usage.

This Acceptable Use Policy and Agreement outlines the guidelines and behaviors that users must follow when using school technologies or when using personally-owned devices on the school campus.

Technologies Covered

Bridges Charter School may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, Bridges will attempt to provide appropriate educational access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't attempt to get around technological protection measures; use good common sense; and ask if you don't know. All activity over the network or using district technologies may be monitored and retained. No use of the network or equipment provided by Bridges Charter School is private.

Web Access

Bridges Charter School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. Users are expected to respect that any web filter is a safety precaution, and shall not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should alert a staff member or submit the site for review.

Email

Bridges Charter School may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from an unknown or untrusted origin; should use appropriate language; and should only communicate with

other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Collaborative Content

Recognizing the benefits collaboration brings to education, Bridges Charter School may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online. Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see.

Devices Policy

Bridges Charter School may provide users with mobile computers or other devices to promote learning inside and outside of the classroom. Bridges Charter School makes every effort to keep all functions of these devices working properly, but does not guarantee that every function not critical for educational purposes will always work. Users are expected to abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution. Users shall report any loss, damage, or malfunction to school staff immediately. Users will be financially accountable for any damage resulting from loss, negligence or misuse, as noted in the "Parent/Student Financial Liability" section of this document. Use of school-issued mobile devices off the school network may be monitored.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown origin. If a student believes a computer or mobile device might be infected with a virus, please alert school staff. Students shall not attempt to remove the virus or download any programs to help remove the virus.

Students shall not:

1. Attempt to disable account limitations or circumvent content protection measures

2. Attempt to access anything with accounts that do not belong to them

3. Create wireless access "hot spots" with personally owned devices

4. Attempt to disrupt, damage or hack network or server operations

5. Download or attempt to download or install programs over the school network or onto school resources without express permission from school staff

Disciplinary action and/or significant financial liability will result.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Copyright Infringement

Students shall not engage in copyright infringement of any type. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner. These rights include the right to reproduce or distribute a copyrighted work. In the file

sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without teacher or parent permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission. If a student sees a message, comment, image, or anything else online that causes concern for personal safety, they should bring it to the attention of a school staff member and/or parent immediately.

Cyberbullying

Cyberbullying includes the transmission of harassing communications, direct threats, or other harmful texts, sounds, or images on the Internet, social media, or other technologies using a telephone, computer, or any wireless communication device. Cyberbullying also includes breaking into another person's electronic account and assuming that person's identity in order to damage that person's reputation. Cyberbullying will not be tolerated. Cyberbullying can potentially result in disciplinary action even if it does not occur at school.

Privacy

Any device with camera, video, or voice recording function shall not be used in any manner which infringes on the privacy rights of any other person. Students shall not take photographs; make audio recordings or video recordings of staff or students without their knowledge and permission.

Examples of Acceptable Use

Students will:

1. Use school technologies for school-related activities

2. Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline

3. Treat school resources carefully, and alert staff if there is any problem with their operation

4. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies

5. Alert a teacher or other staff member should any threatening, inappropriate, or harmful content (images, messages, posts) are seen online

6. Use school technologies at appropriate times, in approved places, for educational pursuits

7. Cite sources when using online sites and resources for research

8. Recognize that use of school technologies is a privilege and treat it as such

9. Be cautious to protect the safety of themselves and others

10. Help to protect the security of school resources

Examples of Unacceptable Use

Students will not:

1. Use school technologies in a way that could be personally or physically harmful

2. Attempt to find inappropriate images or content

3. Engage in cyberbullying, harassment, or disrespectful conduct toward others

4. Try to find ways to circumvent the school's safety measures and filtering tools

5. Plagiarize content found online

6. Post personally-identifying information, about themselves or others

7. Agree to meet someone I meet online in real life

8. Use language online that would be unacceptable in the classroom

9. Use school technologies for illegal activities or to pursue information on such activities

10. Attempt to hack or access sites, servers, or content that isn't intended for my use

***These are not intended to be exhaustive lists. Students should exercise good judgment when using technologies.**

Limitation of Liability

Bridges Charter School makes no warranties of any kind, whether expressed or implied, for the services it is providing. By use of district technology resources, students and parents agree the district will not be held responsible for:

1. Damage or harm to persons, files, data, or hardware

2. The failure of any technology protection measures, violations or copyright restrictions, or user's mistakes or negligence

3. Any damages or costs arising out of or related to the student's use of the District's technology.

4. Unauthorized transactions conducted over the school network

5. The effectiveness of filtering and other safety and security mechanisms

Violations of this Acceptable Use Policy

Students will receive instruction on this policy. Violations of this policy may have disciplinary repercussions, including:

1. Suspension of network, technology, or computer privileges
2. Notification to parents and restorative intervention
3. Detention, suspension or expulsion from school and/or school-related activities
4. Financial Liability
5. Legal action and/or prosecution

Parent/Student Financial Liability

This agreement informs Bridges students and families of their legal responsibility with regard to the Device, cases and cables, which Bridges Charter School is making available to your child. Parent(s) will be held responsible for ALL willful damage to their child's device including, but not limited to: broken screens, damaged metal casing, cracked plastic pieces, inoperability, etc. Should the cost to repair the device exceed the cost of purchasing a new device, the student's parent or guardian will pay for full replacement value. Lost devices and accompanying equipment (cases, cables, etc.) will incur the full replacement cost of the device or, when applicable, an insurance deductible.

California Education Code section 48904 states, in pertinent part, that the parent or guardian of any minor who willfully cuts, defaces, or otherwise injures any real or personal property of Bridges or its employees, or fails to return same upon demand of the Bridges , shall be liable for all damages caused by the minor. Bridges property includes the device and device case. Students should report any damage to the immediate teacher for further evaluation. Responsibility will be determined after the device is sent for repair.

Bridges Student Acceptable Use Policy

Bridges Charter Board Policy: 6163.4

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

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.

5. Abusive or threatening e-mail messages may be turned over to law enforcement. 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

Return last page only

Student Name _____ Grade _____

Homeroom Teacher _____

_____ _____

Parent Signature - Acknowledgment of Acceptable Use Policy Date