BRIDGES
PREPARATORY SCHOOL

Internet and Electronic Use Policy

Bridges Preparatory School (hereafter 'BPS' or the 'school') offers access to our own electronic network. This network includes Internet access, computer services, videoconferencing, computer equipment and related equipment for educational purposes. The purpose of this network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. This document contains the rules and procedures for students' acceptable use of the Bridges Preparatory School electronic network.

- The Bridges Preparatory School electronic network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities, including homework.
- The Bridges Preparatory School's electronic network has not been established as a public access service or a public forum. Bridges Preparatory School has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Parent/guardian permission is required for all students under the age of 18. Access is a privilege — not a right.
- It is presumed that students will honor this agreement they and their parent/guardian have signed. BPS is not responsible for the actions of students who violate them beyond the clarification of standards outlined in this policy.
- The school reserves the right to monitor all activity on this electronic network. Students will indemnify the school for any damage that is caused by students' inappropriate use of the network.
- Students are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities as well as the law in the use of the Bridges Preparatory School's electronic network.

Children's Internet Protection Act

It is the policy of Bridges Preparatory School to: (a) prevent users of its computer network, access 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 47USC 254(h)].

Cyber Bullying

All forms of cyber bullying by BPS students are prohibited. Anyone who engages in cyber bullying is in violation of this Policy and shall be subject to appropriate discipline.

Students who have been cyber bullied shall promptly report such incidents to any staff member.

Complaints of bullying or cyber bullying shall be investigated promptly, and corrective action shall be taken when a complaint is verified. Neither reprisals nor retaliation shall occur as a result of the submission of a complaint.

Cyber bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or

posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or website postings (including blogs) which has the effect of:
1. Physically, emotionally or mentally harming a student;
2. Placing a student in reasonable fear of physical, emotional or mental harm;
3. Placing a student in reasonable fear of damage to or loss of personal property; or
Rev.11/7/2013
4. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.
Students are personally responsible for appropriate behavior in their use of the BPS computer system. Access to network services is a privilege and not a right. Network and computer storage systems may be reviewed by BPS to maintain system integrity and ensure responsible system use.

Students may not:

- Access, send, display, or print offensive messages or pictures
- Use obscene language
- Damage computers, systems, networks, or other technology tools
- Violate copyright laws including loading or copying copyrighted software for personal use
- Use or attempt to acquire another's password
- Trespass in another's folders, disks, work or files
- Load unauthorized software on school computers (games)
- Intentionally waste limited resources
- Use the network for illegal purposes, including "hacking" and unauthorized access to systems or information
- Disclose, use, or disseminate personal information about himself or herself to any other minor
- Violations may result in the loss of access as well as other disciplinary action.

Access to Inappropriate Material

To practical extent, technology protection measures (or Internet filters) will be used to block or filter the access to inappropriate information from Internet or other forms of electronic communications.
Specifically, as required by the Children's Internet Protection Act, blocking will be applied to visual depictions of material deemed to be obscene, or to be child pornography, or to any material deemed to be harmful to minors.
Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.
Inappropriate Network Usage
To practical extent, Steps will be taken to promote the safety and security of users of the Bridges Preparatory School's online computer network when using electronic mail, chat rooms, instant messaging and other forms of 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 Bridges Preparatory School's 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.

Teachers must report inappropriate websites being accessed on the network to IT for blocking. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Head of School or designated representatives.

General Unacceptable Behavior

While utilizing any portion of the Bridges Preparatory School's electronic network, unacceptable behaviors include, but are not limited to, the following:

Students will not play games, use IM, email, listen to music or any other activities, applications or functions during class time, unless expressly approved by a teacher for the educational goals of that particular course and during that particular class.

- Students will not post information that, if acted upon, could cause damage or danger of disruption.
- Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Students will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, they must stop.
- Students will not knowingly or recklessly post false or defamatory information about a person or organization.
- Students will not use criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Students will not use speech that is inappropriate in an educational setting or violates school rules.
- Students will not abuse network resources such as sending chain letters or "spamming.
- Students will not display, access or send offensive messages or pictures.
- Students will not use the Bridges Preparatory School's electronic network for commercial purposes. Students will not offer, provide, or purchase products or services through this network.
- Students will not use the Bridges Preparatory School's electronic network for political lobbying. Students may use the system to communicate with elected representatives and to express their opinions on political issues.
- Students will not attempt to access non-instructional school systems, such as student information systems or business systems.
- Students will not use school equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.
- Students will not use the equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Students will not tamper, alter or delete any of the software that BPS installs on the student's computer until such time as the license expires or the student received express permission to do so.

E-Mail

- Students will not establish or access web-based e-mail accounts on commercial services through the school network unless such accounts have been approved for use by the individual school.
- Students will not repost a message that was sent to them privately without the permission of the person who sent them the message.
- Students will not post private information about another person.

World Wide Web

- Access to information for students on the Web will generally be provided through prescreened sites and in a manner prescribed by BPS administration and staff.

Real-time, Interactive Communication Areas

- Students may not use chat or instant messaging unless under the direct supervision of a teacher or in a moderated environment that has been established to support educational activities and has been approved by the BPS Head of School.

Websites

- Students may be identified by their full name with parental approval. Group or individual pictures of students with student identification are permitted with parental approval.
- Material placed on student webpages are expected to meet academic standards of proper spelling, grammar and accuracy of information.
- Material (graphics, text, sound, etc.) that is the ownership of someone other than the student may not be used on websites unless formal permission has been obtained.
- All student webpages should have a link back to the homepage of the classroom, school or school, as appropriate.

Personal Safety While on the Internet

- Students will not share personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, or work address.
- Students will not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes, or without specific building administrative approval.
- Students will not agree to meet with someone they have met online.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

System Security

- Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should students provide their password to another person.
- Students must immediately notify a teacher or the system administrator if they have identified a possible security problem. Students should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Students will not attempt to gain unauthorized access to any portion of the Bridges Preparatory School's electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Users will not attempt to access Web sites blocked by school policy, including the use of proxy services, software, or Web sites.
- Users will not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

Software is available to students to be used as an educational resource. No student may install, upload or download software without permission from the school technology department. A student's account may be limited or terminated if a student intentionally misuses software on any school-owned equipment. Files stored on the network and on individual computers are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of the Bridges Preparatory School’s electronic network may lead to discovery that a student has violated this policy or the law. Students should not expect that files stored on school servers are private.

Technology Hardware

Hardware and peripherals are provided as tools for student use for educational purposes. Students are not permitted to relocate hardware (except for portable devices), install peripherals or modify settings to equipment without the consent of the school technology department.

Vandalism

Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the school's discipline code and policies will be enforced.

Plagiarism and Copyright Infringement

Students will not plagiarize works found on the Internet (Plagiarism is taking the ideas or writings of others and presenting them as if they were the students’). School policies on copyright will govern the use of material accessed and used through the school system. Copyrighted material will not be placed on any system without the author's permission. Permission may be specified in the document, on the system or must be obtained directly from the author.

Student Rights

Students' right to free speech applies to communication on the Internet. The Bridges Preparatory school’s electronic network is considered a limited forum, similar to the school newspaper, and therefore the school may restrict a student's speech for valid educational reasons. The school will not restrict a student's speech on the basis of a disagreement with the opinions that are being expressed. An individual search will be conducted if there is reasonable suspicion that a student has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

Due Process

- The school will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school network.
- In the event there is an allegation that a student has violated the school acceptable use regulation and policy, the student will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation before a neutral administrator (or student will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code).
- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.
- If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of his/her network account.

Limitation of Liability

The school makes no guarantee that the functions or the services provided by or through the school network will be error-free or without defect. The school will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service. The school is not responsible for the accuracy or quality of the information obtained through or stored on the network. The school will not be responsible for financial obligations arising through the unauthorized use of the network.

Violations of this Acceptable Use Policy

The particular consequences for violations of this policy shall be determined by the Head of School. The Head of School and the board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

Violations of this policy may result in loss of computer use, loss of access as well as other disciplinary or legal action. Students' violation of this policy shall be subject to the consequences as indicated within this policy, as well as other appropriate discipline, which includes but is not limited to;

- Use of school network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school and/or
- Legal action and prosecution by the authorities

Wi-Fi & Other Usage During Testing

Testing days, teachers must have all devices laid out on cleared desks 20 min before session begins for staggered logging on to testing sign-up. Testing Coordinator will send detailed times and instructions. The only electronic devices that should be hooked to the BPS WI-FI account are teacher laptops and test devices only.

The only electronic devices that should be hooked to the BPS Wi-Fi password-protected network are teacher laptops and testing devices. If you have a cell phone, an iPad or any other wi-fi ready electronic device, you may connect it to BPS GUEST WI-FI only if necessary or turn your personal electronic device(s) off while you are in the school building. DO NOT STREAM MEDIA (music, videos, etc.) on any devices.

BPS “Bring Your Own Device” (BYOD) Policy

Purpose

BYOD is part of a continuous effort to incorporate STEM and blended classroom best practices into our school's daily activities, increase technology access, promote engagement, intrinsic motivation to learn and to do self-directed research. In an effort to increase access to those 21st Century skills (collaboration, communication, creativity and critical thinking), BPS will allow personal devices to be brought to school and access our network for students who follow the responsibilities stated in the aforementioned Internet & Electronic Use Policy and the attached guidelines regarding BYOD. The use of personal devices by students is optional, and students who do not participate in BYOD will not be penalized.

An important component of BYOD will be education about appropriate online behaviors. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviors. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices. The use of your own technology is not a necessity but a privilege and when abused, privileges will be taken away.

Device Types

For the purpose of this program, the word “devices” will include Android or iOS platforms only. This includes laptops, netbooks, smart phones, iPods, iPads, tablets, and e-Readers. Please note that Nintendo DS and/or other gaming devices with internet access are not permissible.

Guidelines

Students/Parents/Guardians participating in BYOD must adhere to Student Code of Conduct, Student Handbook, Electronic Use Policy and Board Policies Teachers have discretion to allow/regulate use of personal devices in classroom and specific projects.

- Devices must be in silent mode while at school, unless otherwise allowed by teacher (with teacher permission, headphones may be used)
- Devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes including but not limited to making personal phone calls, text messaging, or playing games that are not academic in nature
- Students may not take pictures/video at any time nor use devices to record, transmit, or post photographic images/video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum
- Students will not have access to devices during lunch, recess, or any time during the day that electronic devices would not be used for academic purposes

Students and Parents/Guardians Acknowledge:

- The school’s network filters will be applied to device’s connection to the Internet and attempts to bypass the network filters is prohibited
- Students are prohibited from bringing a device on premises that infects the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information; processing or accessing information on school property related to “hacking”; or altering or bypassing network security policies (such as proxies)

- BPS is authorized to collect/examine any device that is suspected of causing technology problems or being the source of an attack or virus infection
- Devices are subject to be searched by school administrators and/or staff if device is suspected of a violation of any school policy (if device is locked/password protected student will be required to unlock device at request of school administration)
- Staff is expected to use the highest ethical and professional standards when inspecting a confiscated device
- Devices must be charged prior to school and run on battery power while at school (charging of devices will not be permitted)

Lost, Stolen, or Damaged Devices
Users are responsible for their own device and it is expected that use will be responsible and appropriate. While school employees will help students identify how to keep personal devices secure, students have the final responsibility for securing personal devices. BPS takes no responsibility for lost, stolen, damaged devices (including but not limited to lost/corrupted data on devices), or device mishandling of any kind. Check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss/damage.

Usage Charges
BPS is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Logging In
All 3+ grade students must log onto their Chromebooks (or applicable devices) using their individual Bridges Google accounts (a list is available in Google Drive). They may not use the Chromebooks Guest login. K-2 students may use the Guest sign-in mode. K-1 students need not bring devices to school unless their teacher requests it.

Wi-Fi Connection & Service Providers
Students must connect personal devices to the BPS-Guest Wi-Fi network ONLY. Students may not access the main password-protected BPS Wi-Fi network, nor their personal cellular service providers.

Tech Support
Requesting or declining assistance/troubleshooting from peers/staff is discretionary to the device owner, who is ultimately responsible for any adverse consequences resulting from it. Tech support is available from IT staff on an as-needed, as-available basis. Troubleshooting on BYOD devices is up to students and willing teachers. Device owners are encouraged to “Google” or “YouTube” common troubleshooting problems first, on their own. It is highly recommended to assign a classroom tech support team led by tech savvy students.

BY SIGNING BELOW, YOU CERTIFY THAT YOU HAVE READ THIS AGREEMENT, THAT YOU KNOW AND UNDERSTAND THE MEANING AND INTENT OF THIS POLICY, THAT YOU ARE ENTERING THIS AGREEMENT KNOWINGLY AND VOLUNTARILY, AND THAT YOU AGREE TO COMPLY WITH ALL THE TERMS OF THE BPS ELECTRONIC & INTERNET USAGE POLICY.

Student Name Student Signature Date

Parent/Guardian Name Parent/Guardian Signature Date

Parents/Guardians: Please return this signed page to your homeroom teacher before students are given access to electronic devices at school.

Homeroom teachers: Keep the original signed page in a secure file. Please make a copy of this signed page and place it in Ms. Blanc's mailbox for archiving. **Do not grant access to any electronic device to a student until you have this signed page.**