Computer and Systems Usage Policy

All persons using the School's computers, the School's computer systems, or personal computers on School property or over the School's systems are required to abide by the following rules. This policy also applies to the use of any personal electronic devices (computers, cameras, iPhones, iPads, smart watches, smart/cellular phones, video cameras, etc.) on School property or at a School-related event or used at or away from School for school work on a regular or intermittent basis. Failure to abide by these rules will result in appropriate disciplinary action determined by the School administration. All computers and devices should be used in a responsible, ethical and legal manner. Violations of the following guidelines may result in the revocation of access privileges and possible disciplinary responses, including expulsion for serious offenses.

Purpose: The purpose of providing access to the Internet and the School's computer systems is to support research and provide unique educational opportunities. The use of such resources should be limited to those activities that support the School's educational objectives.

Privilege: The use of the School's systems is a privilege and not a right. Inappropriate or illegal use of the School's systems or of the Internet will result in loss of the privilege and disciplinary action.

Internet Access: The School community--students, faculty, administrators and staff-- have the privilege of access to the Internet. The School encourages students and teachers to use the Internet to expand their knowledge. The Internet allows users to send and receive e-mail, to log onto remote computers, and to browse databases of information. It also lets users to send and receive files and programs contained on other computers. Files are not to be downloaded to the Schools local or network hard drives.

Internet Safety: Students should never give out personal information (address, telephone number, name of School, address of School, date of birth, Social Security Number, credit card number, etc.) over the Internet. Students also should not meet with someone that they have contacted on-line without prior parental approval. Safety is the responsibility of the parent and student. The School is not liable in any way for irresponsible acts on the part of the student.

Pirated Software: The term "pirated software" refers to the use and transfer of stolen software. Commercial software is copyrighted, and each purchaser must abide by the licensing agreement published with the software. There is no justification for the use of illegally obtained software. The School will not, in any way, be held responsible for a student's own software brought to School for personal use.

Network Access/Passwords: Accessing the accounts and files of others is prohibited. Attempting to impair the School's network, to bypass restrictions set by the

network administrator, or to create links to the School's web page is prohibited. Obtaining another's password or rights to another's directory or e-mail on the School's network is a violation of School rules as well as a form of theft. Taking advantage of a student who inadvertently leaves a computer without logging out is not appropriate. Using someone else's password or posting a message using another's log-in name is a form of dishonesty, just as is plagiarism or lying, and will be treated as a violation. **Guard your password. You will be responsible for any activity done on the School's system under your password.**

School's Right To Inspect: The School reserves the right to inspect user directories for inappropriate files and to remove them if found and to take other appropriate action if deemed necessary, including notification of parents. The School also reserves the right to inspect any personal electronic devices brought onto campus to a School-related event or used at or away from School for school work on a regular or intermittent basis. In such case, the School reserves the right to inspect the device, including all contents. Students must provide any and all passwords to inspect the device and its contents upon request by a school administrator. Students and their parents consent to the School logging into the device and its contents and applications, as well as accessing all communications, including, without limitation, stored communications. Do not assume that any messages or materials on your computer/electronic device or the School's systems are private.

Electronic Communication: Students are expected to use their school provided email/Google Classroom account for all school related work and communication. Students are expected to check their email/Google Classroom daily. Electronic communication, such as e-mail and text messaging, may not be used to harass or threaten others. The School reserves the right to randomly check electronic communication. Electronic communication must not include personal attacks and should follow the normal rules of appropriate public language. They should not contain any language or content, which the author would not be willing to share from the podium at a School meeting. Students should be made aware that deleted e-mails can be retrieved.

Any person who believes that they have been harassed or threatened by any electronic communication should immediately report the concern in accordance with the School's No Harassment/No Bullying policy.

Viruses: Every effort is made by the School to keep our system virus-free. Even with the best techniques, however, computer viruses can be transmitted to and from any computer, including those in the computer center. The School is not responsible for the transmission of any virus or for damage suffered from a virus.

Care of School Computers: Members of the School community will not abuse, tamper with, or willfully damage any computer or other technology-related

equipment, use the computer or other technology-related equipment for other than appropriate work, or bring food or drink into any computer area. Any intentional acts of vandalism will result in discipline and students will be held responsible for replacement or repairs.

Reporting Requirements/Discipline: Any student who accesses inappropriate material on the Internet, receives harassing, threatening, or inappropriate materials via e-mail, text, or on the Internet, must immediately report the concern to the teacher who is supervising the activity or to the School Principal so that the situation can be investigated and addressed appropriately. Students who violate any aspect of this Computer and Systems Usage Policy will be subject to appropriate discipline and loss of computer or Internet privileges.

Social Media and Social Networking Policies and Procedures

Social media encompasses a broad array of online activity including social networks/media such as Twitter, Flickr, Instagram, Facebook, GroupMe, and Snapchat, blogs, and other similar online or Internet communications. Because this form of communication is vast and growing, we feel it is important to communicate to you the School's position regarding a student's use of social media or networking.

Use at School or a School-Related Event: We do not permit students to access social media and/or social networking sites while on School property or at a School-related event, unless such use is on a School social media platform or School sanctioned site **and** the use is for school related work. We have taken steps to block many of the social media/networking sites on our network, but technology will undoubtedly work faster than our IT administrators. Therefore, even if you are able to access such sites on School property or at a School-related event, you should understand that your activities are in violation of School policy and may result in disciplinary action.

Use Away from School Property: It is not our goal to regulate a student's personal online activities when not on School property or at a School-related event. Please understand, however, that certain activities might impact a student's relationships with other students or school employees or School rights that we do reserve the right to regulate. All students should ensure that they are familiar with School's conduct policies to avoid any online communications that might violate those policies.

Guidelines: You should ensure that your online activities do not violate a School policy regarding bullying or harassment, or other similar policies pertaining to how students interact with each other. If you post or say something online that makes another student feel uncomfortable, your activity may result in an investigation and possible discipline.

Students should also be aware that teachers and administrators periodically check such sites and may determine that off campus behavior violates the School conduct code by making disparaging or negative comments about the School, administration, or faculty members in a manner that is disruptive to the School's educational mission or activities.

Students should not "follow" or be "friends" with any faculty member or other adult member of our community (other than the student's parent) on any of these social networking sites. Any violation of this prohibition must be reported to the Administration immediately.

In addition, postings on social networking or other Internet sites of students engaging in inappropriate behavior (such as drinking, smoking, vaping, sexual actions, etc.) is prohibited.

Students are not permitted to use the School's name, logo, trademark, or service mark in online activities. Students are not permitted to post photographs of the School, its locations, activities, students, parents, or employee-related activities online. Students are not permitted to create websites or social networking profiles to rate teachers, discuss aspects of the School, or otherwise disclose information online that the School would find offensive or inappropriate if posted in the School's newspaper. Finally, students are not permitted to disclose any confidential information of the School, employees, students, parents, or activities online.

Your Identity Online: You are responsible for any of your online activity conducted with a School email address, and/or which can be traced back to the School's domain, and/or which uses School assets.

What you publish on such personal online sites should never be attributed to the School and should not appear to be endorsed by or originated from the School.

School's Right to Inspect: The School reserves the right to inspect all electronic data and usage occurring over the School's network or on School property without prior notice. We also reserve the right to assess information in the public domain on the Internet and to discipline students for any violation of these guidelines.

Online Learning Management Systems and COPPA Information

We are committed to high quality teaching and learning. We realize that part of 21st century learning is adapting to the changing methods of communication and providing rich and varied contents and experiences for our students. The importance of teachers and students engaging, collaborating, learning, and sharing in digital environments is a part of 21st century learning and provides students the opportunity to develop as literate and technologically competent individuals. Educational standards are now requiring the use of online education tools and our School uses several computer software applications and web-based/cloud-based education technology services operated not by the School, but by third parties. These applications include, but may not be limited to, Google Classroom, Google Drive, Discovery Education, Schoology, Explain Everything, See Saw, Scratch, Kodable, Zoom, Canvas, Code Monkey, and other similar educational programs. A complete list of the programs may be obtained from the School administration.

In order for our students to use these programs and services, certain personal identifying information—generally the student's name and school email address—must be provided to the website operator. Please note that any personal information provided by the School is for educational purposes only and is used by the School solely to communicate with the service provider. Students will receive a school email address to participate in certain of these computer software applications and web-based/cloud-based services. Under federal law entitled the Children's Online Privacy Protection Act (COPPA), certain website providers must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. For more information on COPPA, please visit https://www.ftc.gov/tips-advice/businesscenter/guidance/complying-coppa-frequently-asked-questions.

COPPA permits schools such as ours to consent to the collection of personal information on behalf of its students, thereby eliminating the need for individual parental consent to be given directly to the website operator. Your signature on this Handbook will reflect and constitute your consent for our School to provide personally identifying information for your child consisting of first name, last name, an email address, username, and school-related information, such as school name, class, and teacher name. Your signature will also reflect and constitute your consent for your child to participate in video conferencing, podcasts, and live chats, which means that their identity will be revealed, their voice will be heard, and their image displayed to others and both may be recorded. If you do not want your student to participate in these programs, please notify School Administration.

Distance Learning Addendum Policy

All persons using the School's computers, the School's computer systems, or personal computers for distance learning courses are required to abide by the rules set forth in the Student Handbook and the following rules. All computers and devices while participating in distance learning courses should be used in a responsible, ethical and legal manner. Failure to abide by these rules will result in appropriate disciplinary action up to and including expulsion.

Purpose: The purpose of providing access to distance learning is to support the School's educational objectives while addressing the challenges that arise out of the COVID-19 pandemic. Participating in the School's distance learning program is a privilege and not a right. Inappropriate or illegal use of the School's distance learning program will result in loss of the privilege and disciplinary action.

Expectations: Our expectations of our students are as though they were on campus in their classrooms. Students are expected to fully engage in all courses, complete all course-work, and submit all course-work, including homework as instructed. Students are held to the same academic standards, as in face-to-face instruction, and subject to the School policies on plagiarism and cheating, dishonesty, and all other conduct policies.

Absences: Students are expected to log-in to the School's System every school day. Parents must report a student's absence (regardless of student's age) in accordance with the School's Absenteeism policy. See, also the School's policies on excused and unexcused absences and make-up work.

Live and Recorded Sessions: Distance learning courses will have both live sessions (which will be recorded) and pre-recorded sessions. Students are responsible for attending live courses as scheduled and reviewing pre-recorded sessions as directed by the teacher. Only enrolled students, their parent/guardians, and approved staff will be allowed to enter and participate and to review the recordings (live and pre-recorded). Students are prohibited from sharing course passwords or links with others.

For all live sessions, it is the parents' responsibility to ensure that the student participating in the course is participating in an appropriate environment, is appropriately dressed, and that the computer and camera that the student is using does not show anything inappropriate. Virtual backgrounds or blurred backgrounds are allowed only if they are appropriate. Students are encouraged to place their computer on a stable surface like a table, rather than a soft surface (like a couch or bed).

The live sessions will be recorded. Students might be asked to participate in video conferencing, podcasts, and live chats, which means that their identity will be

revealed, their voice will be heard, and their image displayed to others participating in the course, all of which may be recorded. If the parents do not want the student to be recorded, it is the parent's responsibility to: (1) cover the webcam on the student's computer or turn off the video button; (2) tell the student not to respond to questions posed by the teacher; and (3) email the teacher at least 5 days before the class is set to start to advise him/her that the student will not be speaking up during the session so their voice and image are not recorded.

Internet Safety: The School will provide strict security protocols while participating in live distance learning sessions, but online security for the student will be the responsibility of the parents and students. The School is not liable in any way for irresponsible acts on the part of the student while participating in distance learning courses. Students should never access or share any material that is pornographic, violent in nature, or otherwise harassing. Students also should never give out personal information (address, telephone number, name of School, address of School, date of birth, Social Security Number, credit card number, etc.) over the Internet.

Equipment: Families may sign-out a Chromebook for their student to use during distance learning. It is the parents' responsibility to provide any additional equipment needed for distance learning, such as headset, earphones, microphone, digital camera, supply kits, etc. Any damage to said equipment will be the sole responsibility of the students and the parents.

Appropriate Interactions and Communications: Appropriate behavior for students is expected. Standard handbook policies apply. Any student who believes that they have been bullied, threatened, harassed, or received any inappropriate remarks or comments should immediately contact PBIS leaders.

Bullying, including cyberbullying, threats, and harassment during a session or outside of a session is not appropriate. All students should always use respectful language and never use profanity or threatening, aggressive, or abusive language. No one should ever make sexual, racial, ethnic, or other inappropriate remarks or jokes.

There may be some situations in which students will want additional information from a teacher. That communication may be by email or contact through school communication platforms including ClassDojo or Google Classroom during the teacher's scheduled office hours.

In all communications and interactions, all parties will continue to respect appropriate boundary guidelines. If a student or a parent becomes aware that any adult's communications are inappropriate, such information should be immediately reported to School Leader.

Personal Information: The distance learning program requires the use of several computer software applications and web-based/cloud-based education technology services operated not by the School, but rather by third parties. These applications include, but may not be limited to, Google Classroom, ClassDojo, Google Drive, Discovery Education, Schoology, Explain Everything, See Saw, Scratch, Kodable, Zoom, Canvas, Code Monkey, and other similar educational programs. In order for students to use these programs and services, certain personal identifying information—generally the student's name and email address provided by the School—must be provided to the website operator. A complete list of the programs with the privacy policy for each can be found on our School website. Please note that any personal information provided by the School is for educational purposes only and is used by the School solely to communicate with the service provider. Under federal law entitled the Children's Online Privacy Protection Act (COPPA), certain website providers must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. For more information on COPPA, please visit https://www.ftc.gov/tips-advice/businesscenter/guidance/complying-coppa-frequently-asked-questions. COPPA permits the School to consent to the collection of personal information on behalf of its students, thereby eliminating thereby eliminating the need for individual parental consent to be given directly to the website operator. Therefore, by allowing the student to participate in the School's distance learning courses, the parents/guardians acknowledge their consent for the School to provide personally identifying information for the student consisting of first name, last name, an email address, username, and school-related information, such as school name, class, and teacher name.

Photographs/Recordings: Parents and students are not allowed to take, and shall not take any photographs, video, or other recordings of other students, other children, or other parents/guardians without their express consent, and are not allowed to transmit, upload, or post such content online or electronically including on any social media or similar site, or use or publish such content in any non-personal media such as a book, video, film, television program or publicly viewable website. Upon the School's request, parents and students shall immediately delete and/or remove such content from any device, site, platform, or other media.