BPA INTERNET ACCEPTABLE USE POLICY

As part of our School Technology Plan, Baypoint Preparatory Academy (“BPA ”) provides computer network and internet access for its students and employees. BPA teachers and students use the internet as an instructional tool, to communicate, collaborate, and to complete many of their assigned academic and professional responsibilities. Access to the internet is an integral part of the instructional program designed to help students meet the BPA Expected Schoolwide Learning Results.

Each year, students and employees must acknowledge receipt of an agreement with this Acceptable Use Policy (“AUP” or the “Policy”). Students who are under 18 must also have a parent or guardian sign this policy. By signing the Parent-Student Handbook agreement, the student, employee, and parent or guardian agree to follow the rules set forth in this Policy and to report any misuse of the computer network or the internet to a teacher or administrative director. Parties agreeing to this Policy also understand that BPA may revise the AUP, as it deems necessary. Any such changes will be posted on the BPA website. http://www.baypoint.academy

Acceptable Use Policy for the Internet

Access to the BPA computer network (including, but not limited to: host computers, file servers, application servers, laptops, network hardware, printers, hand-held internet accessible devices, software, applications, data files, email systems, and all internal and external computer and communications networks and peripherals) and the internet is an integral part of the instructional program. Failure to use the BPA computer network, internet access, and student and employee accounts for exclusively educational or professional purposes may result in disciplinary action.

Students and employees may have several user accounts authorized by BPA , including, but not limited to: network access, email, calendars, file storage, applications (apps), instructional and professional resources. User accounts refer to any account created for educational or professional use while using the BPA network. All accounts created for use while at BPA should use the user’s BPA email account for registration. BPA accounts should not be used for personal purposes.

User accounts may only be used during the time the User is a student or employee of BPA . Each account owner is responsible for using it properly. The student or employee may be required to change the password the first time he or she uses the user account and routinely thereafter. Use of passwords to gain access to the BPA network does not imply that the User has an expectation of security or privacy.

If a User is uncertain about whether a particular use of the computer network, website, application, or email is appropriate, he or she should consult a teacher or administrative director.

Unacceptable Uses of the Computer Network, Email or Internet

1. Uses that violate any state or federal law, municipal ordinance, or BPA Policy are unacceptable. Unacceptable uses include, but are not limited to:

    a. Selling or purchasing any illegal substance;
    b. Accessing, transmitting, or downloading child pornography, obscene depictions, harmful materials, or materials that encourage others to violate the law; or
    c. Transmitting or downloading confidential information or copyrighted materials.
2. Uses that involve accessing, transmitting or downloading inappropriate materials on the internet, as determined by the BPA Governing Board or any related authority.
3. Uses that involve obtaining and/or using anonymous email sites.
4. Uses that involve circumventing the BPA network, filtering and/or firewall
5. Uses that cause harm to others or damage to their property are unacceptable.

Unacceptable uses include, but are not limited to the following when done while using a BPA device or the BPA network:

1. Engaging in an act of bullying, including, but not limited to, bullying committed by means of an electronic act.
2. Deleting, copying, modifying, or forging other User's emails, files, or data.
3. Installing or using encryption software on any BPA device or the BPA network.
4. Accessing another User's account for any purpose, even with consent.
5. Damaging computer equipment, files, data or the network.
6. Using profane, abusive, or impolite language.
7. Disguising one's identity, impersonating other Users, or sending anonymous messages.
8. Threatening, harassing, or making defamatory or false statements about others.
9. Accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
10. Accessing, transmitting, or downloading computer viruses or other harmful files or programs, or in any way degrading or disrupting any computer system performance including, but not limited to "email bombs."
11. Accessing, transmitting, or downloading large files, including "chain letters" or any type of "pyramid schemes."
12. Using any BPA computer to undertake "hacking," "phishing" or "spamming" internal or external to BPA , or attempting to access information that is protected by privacy laws.
13. Access and Interference: Using any robot, spider, other automatic device, or manual process to monitor or copy BPA web pages or the content contained thereon or for any other unauthorized purpose; or, using any device, software or routine to interfere or attempt to interfere with the proper working of the BPA website and/or network.
14. Abusing BPA network resources such as emailing mass mailings and chain letters, engaging in spam, subscribing to a non-work or non-school related listserv or group, spending excessive time on the internet for personal reasons, playing games, streaming music or videos, engaging in non-BPA related online chat groups, printing multiple copies of documents or otherwise creating unnecessary network traffic (intentionally or unintentionally).

- Uses that jeopardize access or lead to unauthorized access into Accounts or other networks are unacceptable. Unacceptable uses include, but are not limited to the following:
    1. Using others' User Account passwords or identifiers.
    2. Disclosing one's Account password to other Users or allowing other Users to use one's Account.
    3. Gaining unauthorized access into others' User Accounts or other computer networks.
    4. Interfering with other Users' ability to access their Accounts.
- Commercial uses are unacceptable. Unacceptable uses include, but are not limited to the following:

1. Selling or buying anything over the internet for non-BPA related personal or financial gain.
2. Using the internet for non-BPA related advertising, promotion, or financial gain.
3. Conducting for-profit business activities and engaging in non-governmental related fundraising or public relations activities such as solicitation for religious purposes, lobbying for political purposes, or soliciting votes.
4. Sending any email that is deceptive, misleading, or violates any state or federal statute or regulation including, but not limited to, the CAN-SPAM Act of 2003, or any state email or deceptive practice statute.

Plagiarism Policy

Researching information on the internet and incorporating that information into a student's work is an acceptable educational use, but students have an obligation to credit and acknowledge the source of information. Accordingly, the student acknowledges that plagiarism is inappropriate and unacceptable. Any student that is determined to have plagiarized will be referred to the Director of Education.

Copyright Policy

Baypoint Preparatory Academy prohibits the lawful and unlawful use of BPA equipment or network resources to download or share music, video, pictures, text or any content or media for the purpose of selling or giving access to the files to others, unless specifically authorized by the BPA .

Internet Safety

- In compliance with the Children's Internet Protection Act ("CIPA"), BPA implements firewall filtering/blocking software and hardware to restrict access to internet sites containing child pornography, obscene depictions or other materials harmful to minors under 18 years of age. Although BPA takes every precaution to ensure that such materials are not accessed through the computer network, there is still a risk an internet User may be exposed to a site containing such materials. A User who connects to such a site must immediately disconnect from the site and notify a teacher or administrative director. If a User sees another User accessing inappropriate sites, he or she should notify a teacher or administrative director immediately.
- In compliance with CIPA, BPA and its representatives monitor all minors' online activities while on the BPA network or BPA devices, including website browsing, email use, video and text chat, instant messaging, social media, blog participation and other forms of electronic communication. Such monitoring may lead to a discovery that a User has violated or may be violating this Policy, the appropriate disciplinary policy or the law. Monitoring is aimed to protect minors from accessing inappropriate material, as well as to help enforce this Policy as determined necessary by the BPA Governing Board or other related authority. BPA also monitors other Users' (e.g. employees, students 18 years or older) online activities while on the BPA network or BPA devices and may access, review, copy, store or delete any electronic communication or files and disclose them to others as it deems necessary.
- If a student under the age of 18 accesses his/her BPA Account or the internet outside of school, a parent or legal guardian must supervise the student's use of the Account or internet at all times and is completely responsible for monitoring the student's use thereof. Filtering and/or blocking software will be employed to monitor home access to the internet. Parents and legal guardians should inquire at BPA if they desire more detailed information about the software.
- Student information shall not be posted online unless it is necessary to receive information for instructional purposes and only if the student's teacher and parent or guardian has granted permission in advance.

- Safety and Identify Theft: Users shall not reveal on the internet personal information about themselves or about other persons. For example, Users should not reveal their full name, home address, telephone number, school address, social security number, credit card number, photograph, parents/guardians' name or any other information that could identify them to anyone except BPA staff. It is illegal to post other employees' personal information online without their prior consent.
- BPA has the authority to suspend or expel students for bullying fellow students over the internet, in text-messaging or image by means of an electronic device including but not limited to a telephone, mobile phone or any other wireless communication device, computer, offline or online communication device.
- Users shall not meet in person anyone they have met on the internet in a secluded place or a private setting. Users who are under the age of 18 shall not meet in person anyone they have met on the internet without his/her parents/guardians' permission.
- Users will abide by all BPA security policies and by CIPA.

Privacy Policy
No Expectation of Privacy: BPA has the authority to monitor all Accounts, including email, files, documents, internet activity, and other materials transmitted, received, or created by the User. Users cannot expect that anything created, stored, sent or received using the BPA network will be private. Files and email are continuously archived by BPA; therefore, their contents will still be available even though the User has deleted them. Files, email and/or the history of websites a User has visited may be read by BPA at any time, including if it is believed that the User violated the AUP, the school discipline policy, the school ethics policy, the school academic integrity policy, or the law. All such materials are the property of BPA . Users do not have any right or expectation of privacy regarding such materials.

Restriction of Free Speech: The BPA network is not a public access service or a public forum. BPA has the right and responsibility to restrict material including text, graphics and all other forms of expression accessed, posted or stored on the system.

Waiver of Privacy Rights
Students expressly waive any right of privacy, as to BPA , in anything they create, store, send, or receive using the BPA network. They understand and consent to BPA ' use of human and/or automated means to monitor the use of the BPA network and devices, including email and internet access.

Penalties for Improper Use of the Internet
Access to the internet and the use of a computer (or other BPA provided devices) is an integral part of the instructional program. Inappropriate use may lead to disciplinary and/or legal action including but not limited to suspension or expulsion for students, or dismissal from employment from BPA , or criminal prosecution by government authorities. BPA will tailor any disciplinary action to meet the specific concerns related to each violation.

Student and Employee Owned Devices
Neither students nor employees are permitted to connect personal devices to the BPA network without the specific permission of BPA administration or IT department.

Disclaimer

- BPA makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs or other obligations arising from the unauthorized use of the Accounts. BPA also denies any responsibility for the accuracy or quality of the information obtained through the Account. An internet search may automatically produce search results that reference or link to third party sites throughout the internet. BPA has no control over these sites or the content within them. BPA cannot guarantee, represent or warrant the content of any third party site is accurate, legal and/or inoffensive. BPA does not endorse the content of any third party site, nor do we warrant that the site will not contain viruses or otherwise impact an internal or external computer.

- Any statement accessible on the BPA computer network or the internet is understood to be the author’s individual point of view and not that of BPA , its affiliates, or employees.
- Users are responsible for any losses sustained by BPA or its affiliates resulting from the User’s intentional misuse of any Account.

By agreeing to this AUP, students, parents and employees help to ensure a safe learning environment for everyone. For additional information about this Policy, contact the Director of Operations, Director of Education or the Information Technology Manager.

Additional Use of Technology by Students

Additional devices such as audio-visual equipment and other devices are utilized in selected classes and may be checked out to selected students. The school Acceptable Use Policy and Restitution of Monies policy are applicable to the issuance of any school equipment to students.