Tallahassee Preparatory Academy
INTERNET SAFETY POLICY

1. Purpose. Tallahassee Preparatory Academy (the "School") recognizes the value of electronic devices and the internet to improve student learning and enhance school administration and operations. However, the internet is an unregulated vehicle for communication, and information and interactions on the internet can pose certain risks to students and staff members. Therefore, the Governing Board adopts this policy governing the use of school networks to comply with Florida law and State Board of Education rules, and to provide rules for students and employees accessing such networks.

2. General Requirements for Users. It is the policy of the School to maintain an environment that promotes ethical and responsible conduct in all online network activities by staff and students. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of the network. Users on any network operated by the School shall comply with the following requirements:

a) All use of a network must be in connection with education and research, or in the case of employees, related to the employee's job functions.
b) Users shall not access any content that is prohibited under this policy or under the law.
c) Users are prohibited from using the School's networks for any illegal or unethical purposes, including infiltrating or hacking the School's systems or any outside systems.
d) Users shall not utilize the School's networks for personal gain or personal business.
e) Users shall not install any unauthorized software or programs on any School-owned electronic device or network.
f) Users shall not destroy, delete, or modify any School-owned devices or software unless authorized to do so.
g) Users shall not utilize the School's networks to engage in harassment, discrimination, cyberstalking, cyberbullying, or obscene behavior.
h) Users will avoid clicking unknown links or accessing webpages and other content that may contain malware, spyware, ransomware, or other malicious software.
i) If any user accesses prohibited content or downloads potentially malicious software, the individual must immediately report the incident to their teacher, in the case of students, or to the Principal, in the case of staff members.

3. Requirements for Student Users. The following requirements apply to the use of the School's networks by students:

a) Student internet and technology sessions must always be supervised by a teacher or other staff member.
b) Students may only use technology or access the internet when expressly instructed by a teacher for educational purposes.

c) Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of school-provided technology or internet access shall make reasonable efforts to monitor student use to assure that it conforms to the requirements of this policy and the law.
d) Staff must make reasonable efforts to become familiar with the internet and its use so that effective monitoring, instruction, and assistance may be achieved.

4. Prohibited Uses. It is strictly forbidden for any users to access online content that is lewd, pornographic, scandalous, obscene, illegal, hateful, objectionable, inappropriate, or that otherwise does not comply with the requirements of this policy.

5. Social Media Platforms. As a general rule, the School's networks may not be used by any person to access social media platforms. In limited circumstances, students may be permitted to access social media platforms when expressly directed by a teacher to do so and solely for educational purposes. Staff members may also access social media accounts that are maintained on behalf of the School and related to the staff member's job duties. Prior to requiring students to use online content, staff must confirm that the content is not blocked by the student internet filter. Staff may make a request to their supervisor that blocked content or social media platforms be reviewed and temporarily unblocked for educational purposes. Notwithstanding the foregoing, under no circumstances may any employee or student access TikTok or any other platforms prohibited by Florida's Department of Management Services while on school grounds or participating in a school activity. Additionally, the use of TikTok to communicate or promote the School, a School-sponsored club, extracurricular organization, or athletic team is prohibited.

6. Online Messaging Platforms. Students are only permitted to utilize sanctioned email, chatrooms, and online messaging platforms while at the School or as part of School activities and only when permitted by a staff member as part of the educational program. Students should be made aware of the potential dangers posed by communicating with unknown individuals on the internet and such communications are strictly prohibited.

7. School's Responsibilities. In order to ensure network safety and enforce the provisions of this policy, the School's administration will implement the following measures:

a) Provide internal and external controls as appropriate and feasible that restrict access to content, including implementing a network filtering system that is designed to block access to prohibited or restricted content on the School's networks and on any School-issued device. Access to content should be limited to age-appropriate subject matter and materials. Access to websites, web or mobile applications, or software that does not protect against the disclosure, use, or dissemination of students' personal information in accordance with Rule 6A-1.0955, F.A.C., will be prevented.
b) Monitor the use of online activities and electronic devices. This may include real-time monitoring of network activity and/or maintaining a log of internet activity for later review.
c) Remove or revoke privileges for any user that poses a threat to the safety and security of the network or to any person.

d) Retain the ability to remotely remove any prohibited application from any School-issued device.
e) Restrict access to social media platforms, applications prohibited by the Department of Management Services, and any other destination that does not adequality protect student information.
f) Make reasonable efforts to train staff and students in acceptable use and policies governing use of the School's networks and devices.
g) Contract only with service providers and operators of websites, online services, or online applications that comply with all state and federal laws governing the disclosure of confidential student information.

8. Violations. Use of electronic devices and networks provided by the School is a privilege. To maintain the privilege, all users agree to learn and comply with the provisions of this policy. Violations of this policy may result in revocation of network access rights and further disciplinary action. Students that violate this policy will be disciplined in accordance with the Code of Student Conduct. Staff members that violate this policy will be subject to disciplinary action up to and including termination. Any criminal activity will be reported to law enforcement.

9. Parental Notification. A copy of this policy shall be made available on the School's website and incorporated into the School's Parent & Student Handbook to fully inform parents.