INTERNET SAFETY POLICY

PURPOSE

Lake Wales Charter Schools, Local Educational Agency (the "LEA") recognizes the value of electronic devices and the internet to improve student learning and enhance school administration and operations. Therefore, the Governing Board adopts this policy governing the use of LEA networks to comply with Florida law and State Board of Education rules, and to provide rules for students and employees accessing such networks.

On July 19, 2023, the State Board of Education adopted Rule 6A-1.0957, Florida Administrative Code (F.A.C.), Internet Safety Policy. The purpose of this rule is to set forth requirements for internet safety policies that must be adopted by school districts and charter school governing boards.

By September 1 of each year, each district school board and charter school governing board must adopt an internet safety policy for student internet use that applies to all devices owned or provided by a district or school, or any device (including privately owned) connected to district- or school-provided internet. This policy must be reviewed and approved annually by the school board or governing board. In developing a student internet safety policy, district school boards, and governing boards must review whether the Children's Internet Protection Act, 47 C.F.R. § 54.520, applies and, if so, ensures compliance with CIPA.

STUDENT INTERNET SAFETY REQUIREMENTS

Student internet safety policies must, at a minimum:

- Require the use of technology protection measures to filter or block access to material that is not appropriate for students, taking into consideration the subject matter and the age of the students served at each school;
- Protect the safety and security of students when using email, chat rooms, and other forms of direct electronic communications;
- Require the use of technology protection measures to prevent hacking or unauthorized access by students to data or information that they should not have access to and to prohibit other unlawful online activities by students;
- Prevents access to websites, web or mobile applications, or software that do not protect against the disclosure, use, or dissemination of students' personal information in accordance with rule 6A-1.0955, F.A.C.;
- Prohibits students from accessing social media platforms, except when expressly directed by a teacher for an educational purpose.
- Prevent unauthorized online disclosure, use, or dissemination of student Personally Identifiable Information (PII).
- Prevent access to websites, web or mobile applications or software that do not protect against the disclosure, use or dissemination of student PII in accordance with Rule 6A-1.0957 F.A.C.

TIKTOK

School districts and charter school governing boards must:

- Prohibit the use of TikTok, and any successor platforms, on all district- or school-owned devices, or any device (including privately owned) connected to district- or school-provided internet;
- Prohibit the use of TikTok, or any successor platforms, to be used to communicate or promote any school district, school, school-sponsored club, extracurricular organization, or athletic team.

GENERAL REQUIREMENTS FOR USERS

The LEA's policy is 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 LEA shall comply with the following requirements:

- All use of a network must be in connection with education and research, or the case of employees, related to the employee's job functions.
- Users shall not access any content prohibited under this policy or the law.
- Users are prohibited from using the school's networks for illegal or unethical purposes, including infiltrating or hacking the school's systems or any outside systems.
- Users shall not utilize the school's networks for personal gain or personal business.
- Users shall not install any unauthorized software or programs on any LEA-owned electronic device or network.
- Users shall not destroy, delete, or modify any LEA-owned devices or software unless authorized to do so.
- Users shall not utilize the school's networks to engage in harassment, discrimination, cyberstalking, cyberbullying, or obscene behavior.
- Users will avoid clicking unknown links or accessing webpages and other content that may contain malware, spyware, ransomware, or other malicious software.
- 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.

REQUIREMENTS FOR STUDENT USERS

The following requirements apply to the use of the school's networks by students:

- Student internet and technology sessions must always be supervised by a teacher or other staff member.
- Students may only use technology or access the internet when expressly instructed by a teacher for educational purposes.
- Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of LEA-provided technology or internet access shall make reasonable efforts to monitor student use to ensure that it conforms to the requirements of this policy and the law.
- Staff must make reasonable efforts to become familiar with the internet and its use so that effective monitoring, instruction, and assistance may be achieved.

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.

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 LEA 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's 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 Education while on school grounds or participating in a school activity. Additionally, the use of TikTok to communicate or promote the LEA, a School-sponsored club, extracurricular organization, or athletic team is prohibited.

ONLINE MESSAGING PLATFORMS

Students are only permitted to utilize sanctioned email, chatrooms, and online messaging platforms while at the LEA or as part of LEA 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.

SOCIAL MEDIA SAFETY INSTRUCTION (F.S. § 1003.42)

For students in grades 6 through 12, the LEA shall provide age-appropriate instruction regarding the social, emotional, and physical effects of social media. The curriculum shall include:

- The negative effects of social media on mental health, including its addictive nature.
- Safety protocols for maintaining personal security and identifying cyberbullying, predatory behavior, and human trafficking.
- The permanence of digital content and the long-term impact of misinformation.

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:

- 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 LEA-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-1.0957, F.A.C., will be prevented.
- 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.
- Remove or revoke privileges for any user that poses a threat to the safety and security of the network or to any person.
- Retain the ability to remotely remove any prohibited application from any LEA-issued device.
- Restrict access to social media platforms, applications prohibited by the Department of Management Services, and any other destination that does not adequately protect student information.
- Make reasonable efforts to train staff and students in acceptable use and policies governing the use of the school's networks and devices.
- 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.
- Instructional personnel may designate specific areas or times where wireless communication devices are prohibited during instructional time (F.S. § 1006.07).
- Prior to requiring students to use online content, policies must require staff to confirm that the content is not blocked by the student internet filter.
- Policies must provide a process for staff to request that blocked content or social media platforms be reviewed and unblocked for educational purposes.

VIOLATIONS

Use of electronic devices and networks provided by the LEA 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.

PARENTAL NOTIFICATION

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

Changes:

Update Category	Change	Statutory Basis
Curriculum Mandate	Added Section 9: Mandatory age-appropriate instruction for grades 6-12 on the social, emotional, and physical effects of social media (including its addictive nature).	F.S. § 1003.42(2)(u)
Classroom Management	Added to Section 10: Formally empowers teachers/personnel to designate specific times or areas where wireless communication devices are prohibited during instructional time.	F.S. § 1006.07
TikTok Ban	Added TikTok Ban as mandated by CS/HB 379 and State Board of Education.	Rule 6A-1.0957
Regulatory Consistency	Incorporated updated references to Rule 6A-1.0955, F.A.C. regarding student data privacy and PII protection within filtering mandates.	Rule 6A-1.0955, F.A.C.

Board Approved Date: Aug 17, 2026