



5.381 Student Social Media Guidelines

The Sarasota County School District allows schools and the District Communications and Community Relations Department to use online social media to improve communication among the District, families, students, staff and other members of the Sarasota County Schools community. This document contains guidelines to ensure that participants in social media communications understand and follow procedures that will make the use of online social media a positive, legal, and productive experience for everyone involved.

A. Definitions

“Social media” include various Internet sites and technological tools that enable users to share information and resources easily. Social media can include text, audio, video, images, podcasts, and other electronically transmitted communications. These media provide information from various published sources and allow for interaction through user-generated content.

“Technology” includes the Internet and any device, regardless of whether it is District-owned or personally-owned, that is used to access it or otherwise share information electronically, including, but not limited to, computers, notebooks, telephones, cell phones, personal digital assistants, pagers, MP3 players such as iPods, USB drives, communication networks, platforms, and servers, wireless routers, or other wireless communication devices.

“District technology” is technology owned or provided by the Sarasota County School District. “Personal technology” is any device that is owned by the user or provided by a third party other than the District.

B. Representative Social Media Sites

These guidelines pertain primarily to social networking sites and their corresponding Apps.

Some examples include, but are not limited to the following:

- Facebook (<http://www.facebook.com>)
- Twitter (<http://www.twitter.com>)
- YouTube (<http://www.youtube.com>)
- Instagram (<http://www.instagram.com>)
- Flickr (<http://www.flickr.com>)
- Snapchat (<http://www.snapchat.com>)
- TikTok (<http://www.tiktok.com>)

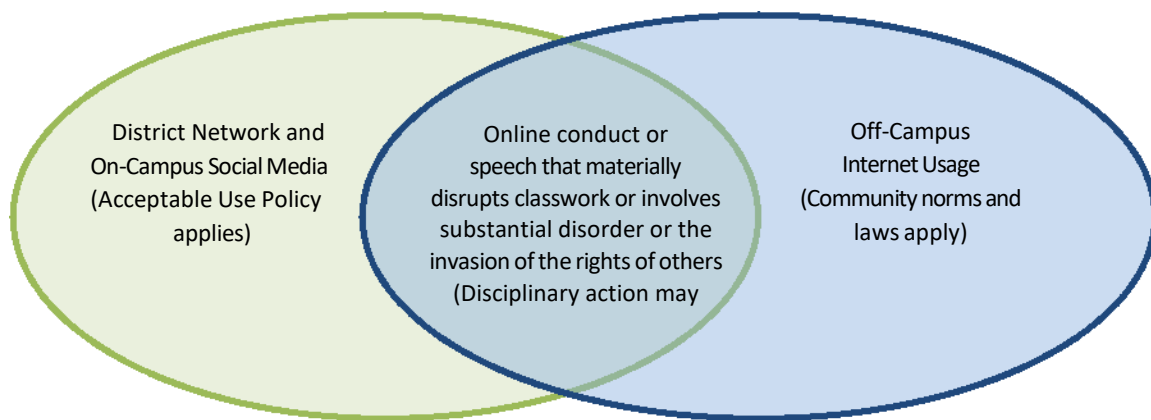
- Blogs (Web Logs)
- Any District-related social media account or page

C. Social Media and Internet Use Guidelines

Although students enjoy free speech rights guaranteed by the First Amendment to the US Constitution, those rights are subject to certain limitations. Access to District technology is a privilege, not a right. The guidelines in this document are intended to present students and families with direction for responsible, safe, ethical, legal, and effective use of social media.

Student use of District technology for electronic communication is governed by the District Acceptable Use Policy and the Code of Student Conduct, which describe consequences for violations, if the online conduct or speech materially disrupts the classroom or involves substantial disorder or the invasion of the rights of other. Students should not expect privacy in the content of their personal files on the District Internet system or other District technology, including email. District technology may be used for educational purposes only. Use for entertainment purposes such as personal blogging, instant messaging, on-line shopping, or gaming is not allowed.

Use of personal technology may also violate the District's Acceptable Use Policy or Code of Student Conduct if the online conduct or speech materially disrupts the classroom or involves substantial disorder or the invasion of the rights of others. This is so whether it occurs on or off campus.



Although the use of District technology or personal technology while off campus or not engaged in a school-related activity is often unrelated to school, in some circumstances courts have held that the off-campus electronic communications may be connected enough to school or District interests to result in either student or staff-member discipline. The figure above illustrates the potential overlap in the use of District and personal technology. When evaluating whether student such off campus or non- school related speech or conduct is permissible, the District must evaluate whether it tends to materially disrupt the educational process or cause substantial disorder or invades on the rights of others. When making this determination, context matters and the individual circumstances should be evaluated on a case-by-case basis. Factors for consideration include: the age of the student, the nature of the speech or conduct, the actual or likely impact on the school environment, and the actual or likely impact on the rights of others. Consideration must also be given to the First Amendment rights that students possess to engage in off campus speech that does not tend to materially impact the school as well as the District's diminished ability to regulate off campus speech and conduct compared to its ability to so regulate the same speech or conduct that occurs on campus, during school, or during participation of school-related activities.

D. Student Use of Technology

Control of Personal Information – Students should always protect personal information that would allow a recipient to locate the student, including his or her family name, home address or location, school address or location, work address or location, or phone number.

When using District technology, students shall not disclose their personal contact information or the personal contact information of others. Students are encouraged to follow these rules in their use of personal technology as well. If student use of personal technology materially disrupts classwork or tends to cause substantial disorder or the invasion of the rights of others, the student may be disciplined. In order for disciplined to be imposed regarding a particular opinion, the District must establish that the discipline was supported by something more than a desire to avoid the discomfort and unpleasantness that always accompanies unpopular viewpoints.

Cell Phone Use – Students may possess electronic devices such as cell phones, smart phones, laptops, electronic tablets, e-readers and other devices designed to receive and send an electronic signal or store digital data in school, on school property, at after-school activities and at school-related functions, provided that during the student day the electronic devices remain powered off and concealed from view.

Students may not use electronic devices during school, while on school property or vehicles or at or while engaged in a school-sponsored activity to access or view Internet websites that are otherwise blocked to students at school or in a manner prohibit by District policy or law, without explicit authorization. In special circumstances with

permission from a supervising District employee, a student may so use an electronic device. The requirement that electronic devices must be turned off will not apply when the electronic device is being used for an educational or instructional purpose with the teacher's permission and supervision.

Students may not possess District technology, personal technology at their desks, clipped to their belt, in their pocket, or anywhere within reach during testing, without express authorization, even if the device is turned off or the student is not using it. If a student is found to be in possession of any District technology or personal technology in a manner not authorized or otherwise in violation of District policy or the law during testing, his or her test may be invalidated and discipline may result.

Possession of District technology or personal technology by a student is a privilege that may be forfeited if the student fails to abide by the terms of District policy or law, or otherwise engages in misuse of this privilege. Violations of this or other District policies or law may result in disciplinary action and/or confiscation of the technology or device. If the technology or device is confiscated, it will be returned to the student's parent or guardian as defined by Florida statute. The District is under no obligation to return seized District technology unless required by law.

The student who possesses District technology or a device is responsible for its care and security. The District is not responsible for preventing or investigating the theft, loss, damage, or vandalism to District or personal technology or devices brought on to District property.

Inappropriate and/or Illegal Uses of Technology

Unless otherwise noted, the following activities are prohibited uses of: (1) District technology, including computers and other hardware, software and the District network (2) personal technology while on campus or District vehicles, during school, during participation in school related activities or while off campus but when the use in question materially disrupts the classroom or that involves substantial disorder or invasion of the rights of others:

- Taking or posting photographs of individuals without their knowledge or consent;
- Using a computer, video recorder, camera, technology, or program in any manner other than for appropriate educational purposes;
- Accessing, copying, transmitting or distributing threatening, offensive, inflammatory, pornographic, obscene, or otherwise inappropriate images, language or materials, including screen savers, backdrops, or pictures on school District-owned technology or on any other electronic device;
- Transmitting or copying material in violation of federal, state, or local law, School Board policy or regulation, or Code of Student Conduct, including, but not limited to, copyrighted material; test questions or answers; unauthorized student work products; trade secrets; or computer viruses, "worms" or "trojans" at any time and

- regardless of device ownership;
- The use of TikTok or, any successor platform, or any other platform on the prohibited list as stated by the Florida Department of Management Services while connected to district- or school-provided internet;
 - Committing plagiarism; cheating; or reproducing tests, textbooks, teaching materials, or other intellectual property without expressed written permission at any time and regardless of device ownership;
 - Using technology for commercial activities unless explicitly permitted by the School Board;
 - Conducting private business or illegal activity;
 - Using email, instant messaging, web pages, or other technology to threaten, disrupt, or interfere with the safety and welfare of the school community;
 - Using technology to threaten, harass, or bully other students or staff;
 - Using profanity, obscenity, epithets, or other language that violates generally accepted norms of appropriate public discourse;
 - Accessing online telecommunication systems other than those authorized and assigned as student educational systems;
 - Downloading or printing music, games, videos or inappropriate files;
 - Gaining or attempting to gain unauthorized access to the District's network, computer servers, or data files at any time and regardless of device ownership;
 - "Hacking" into the school's computer systems or modifying computer settings without permission at any time and regardless of device ownership;
 - Attempting to log on to the District's network using another person's identity at any time and regardless of device ownership;
 - Bypassing or attempting to bypass the District's filtering software at any time and regardless of device ownership;
 - Modifying the District's original pre-set software or hardware, including, but not limited to, loading software applications not authorized by the District; changing the computer name; changing or removing operating system and extensions; altering security/filtering software; altering the pre-loaded operating system or application; dismantling the computer for access to internal parts; or accessing or altering passwords at any time and regardless of device ownership;
 - Vandalizing data;
 - Using network access to destroy information that belongs to others; and
 - Using technology in any other manner not listed above but determined to be inappropriate by staff or administrators.

Violations will result in serious disciplinary actions and may include arrest and prosecution if a criminal law is broken. Examples of such criminal violations would be computer hacking or trespass, harassment or threats via computer, or computer fraud.

System Security – Students are responsible for their individual District account and should take all reasonable precautions to prevent others from using their account. Under no circumstances should a student provide his or her password to another person. Students

shall immediately notify a teacher or administrator if they identify a security problem.

Resource Limits – Students shall not download large files without permission of a teacher or administrator. Students shall not misuse District or school distribution lists or discussion groups by sending irrelevant or non-school related messages.

Because online content can be spread in mere seconds to a mass audience, the District encourages students to ask themselves before posting any information online to ponder whether doing so is within the student’s best interests.

References

This document was developed by the Sarasota County Schools Communications Department in collaboration with the Sarasota County Schools Information Technology Department and the Office of the Superintendent.

The guidelines were adapted from the Student Social Media Guidelines of the San Diego Unified School District, which developed them in consultation with a consortium of legal, educational and social media experts.

Thanks to the San Diego Unified School District for their support and permission to use this document.

Policies: 532; Zero Tolerance of School-Related Crimes
5322; Prohibition Against sale or Possession of Alcohol or Drugs
5323; Bullying and Harassment
5371; Gang Control Policy
5.38; Student Use of Electronic Devices

Procedures: Parent and Student Handbook
Section 3; Behavior
Acceptable Use Policy

Revised August 2021, September 2023

P. Duggan