District 125
Adlai E. Stevenson High School

Acceptable Use Guidelines:
Regarding Access and Use of
District Information Services Systems

Introduction

The District Information Services Systems were established to support the school curriculum, facilitate appropriate communications between the school and community, and enhance performance of the operational responsibilities of the District.

For purposes of these guidelines, “Electronic Communication” is any electronic form of communication including but not limited to chat rooms, e-mail, forums, article forwarding, instant messaging, text messaging, blogs, message boards, document forwarding from home, libraries, or other outside sources.

The Acceptable Use Guidelines are designed to:

1. Raise awareness of acceptable ways to use electronic communication tools when communicating with students and staff.

2. Raise awareness of potential outcomes that may result when using electronic communication tools with students and staff.

3. Protect District 125 information system users from inappropriate use of electronic communication systems.

Using District Information Services Systems and electronic communication appropriately can help develop academic as well as social emotional skills. However, if technology, including use of social media, is not used properly, it may not meet our public and professional standards or the Vision and Values that we set for ourselves at District 125.

These guidelines may be revised from time to time as changes in law or other circumstances dictate, and posted in revised form on the District website.

Per District 125 Board of Education Policy 6:235, the term “District Information Services Systems” or “Systems” includes all computer hardware and software owned or operated by the District, District electronic mail, District websites, District online services and bulletin board systems, and electronic information systems. “Use” of the District Information Services Systems includes use of or obtaining access to the system from any electronic device and/or computer terminal, whether or not owned or operated by the District.

District Authority

The District reserves and retains the right to regulate the content of and links to the District Information Services Systems. The Systems do not constitute a public forum. The District has the right to and does monitor use of the Information Services Systems. Except as provided by federal and state statutes protecting the confidentiality of students' records, no user of the District Information Services Systems has an expectation of privacy in connection with such use.

The District retains ownership and use rights over all information, data, and intellectual property produced through use of any and all of the district's information systems.

The District makes no warranties of any kind, express or implied, for the Information Services Systems it is providing. The District will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, viruses, or service interruptions whether caused by the District's negligence or by a user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained on the Internet through the use of the District's Systems. All users need to consider the source of any information they obtain, in evaluating the reliability of that information.

District 125 shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Many District devices come with a built-in webcam. The District does not have the ability to remotely access the webcam. At no time will the District use webcams to monitor students or employees.

Use of the Systems is a privilege, not a right. Inappropriate, unauthorized, or illegal use may result in cancellation of use privileges and in other appropriate disciplinary and legal action. The Superintendent, or their designee shall have the authority to determine inappropriate use as described in these Guidelines, and their decision is final.

Responsibility

Use of the District Information Services Systems shall be consistent with the Board of Education policy, the Acceptable Use Guidelines, and the Vision and Values adopted by District 125, as well as with the varied instructional needs, learning styles, abilities and developmental levels of students. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

When using electronic means to communicate about public business of the District, employees and officers of District 125 should use only the District Information Services Systems – not personal electronic devices – in order to ensure that communications which are public records and which are not exempt from disclosure under the Illinois Freedom of Information Act (FOIA) are available and accessible to the public if requested under FOIA, and to avoid the potential need to search personal electronic devices for records relating to public business of the District which are responsive to a FOIA request.

Students and District employees are responsible for respecting and protecting the rights of other users in the District and on the Internet.

Electronic Communication

Electronic communication should always be **T**ransparent, **A**ccessible and **P**rofessional (**TAP**) as defined below:

1. **The communication is Transparent:** As a public-school district, we are expected to conduct non-confidential communications in an open and accountable manner.

2. **The communication is Accessible:** Users of the District Information Services Systems should bear in mind that electronic communications on the Systems are potentially public records of the District, which may be accessed under the Illinois Freedom of Information Act, after content exempt under FOIA has been redacted.

3. **The communication is Professional:** All electronic communication from District employees to one another, to members of the public and to students should be written in the manner of professionals, representing District 125, word choices, tone, grammar and subject matter. Communications should be courteous, conscientious, and businesslike.

Communication Methods

1. Acceptable Methods

    a. School website - www.d125.org including school-sponsored websites
    b. District 125 email and collaboration tools
    c. Infinite Campus Student Parent Portal
    d. Canvas Learning Management System
    e. One-way messaging - Remind.com - Internet service sending text to registered individuals to receive notifications.
    f. Social Media (Social media is defined as any form of online publication of presence that allows interactive communication, including: social networks, blogs, Internet websites, Internet forums and wikis.)
    g. Two-way messaging - Not encouraged. If two-way texting is necessary, District personnel must follow TAP guidelines, and they must obtain parental permission before two-way texting. (Please see Student Activities and Athletic Department)

2. Unacceptable Methods

    a. Non-District email accounts - District 125 employees should never use personal email accounts to communicate with students about school matters. Coaches not employed by District 125 during the school day must also follow this expectation.
    b. Online games and related activities - While many people enjoy gaming systems (Wii, Xbox, etc.) and recreational websites that allow them to compete with others through the Internet, these are not acceptable activities for employees to engage in with students.

Use of Email

The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

1. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.
2. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
3. Electronic messages transmitted via the School District's Internet gateway identify the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
4. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

Remote Learning

Remote learning experiences may consist of several communication methods. When providing remote learning, it is imperative that you only use the acceptable methods as outlined in the above Acceptable Communications section.

There are additional guidelines for administering or participating in a remote learning experience. They are as follows:

1. Ensure your confidentiality and integrity (host or participant) as well as for the product(s) you create, receive, maintain, or transmit.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of the remote learning experience.
3. Protect against any unnecessary uses or disclosures of personal information, that is not permitted or required under the privacy regulations.
4. All participants must be compliant and respect the goal and activities of each session.

Access Control

1. (Host Only) Follow technical policies and procedures that maintain your electronic protected information and allow access only to authorized school personnel.
2. Establish (and implement as needed) procedures for obtaining necessary electronic user (host or participant) health information during an emergency.
3. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
4. Use the school's approved mechanism for encrypting and decrypting electronic protected user (host or participant) information.

Audit Controls:

1. Use only the school approved hardware, software, and/or procedural mechanisms to record or monitor your (host or participant) activity and your (host or participant) information.

Integrity:

1. Protect your (host or participant) information from improper alteration or destruction.

Person or Entity Authentication:

1. Verify that a person or entity (host or participant) seeking access is the one claimed.
2. (Host only) Protect the session to ensure access is protected by the approved authentication system.

Transmission Security:

1. Ensure that information (of host or participant) that is being transmitted over a network is in fact secure before sending.

Official School Organizations and Social Media Communications

All communication is required to follow TAP guidelines. Employees should obtain their supervisor's approval prior to setting up a school-related social network and register the site with the school Public Information Office online at d125.org. Review and reference the Stevenson Social Media Guidelines which are posted on our school website and Facebook page. Guidelines for use of Facebook are outlined below, as Facebook is currently the most commonly used form of social media. However, the principles reflected in these guidelines should be followed when using any form of social media.

Using Facebook

Setting up a Facebook Fan Page for student groups:

A Facebook Fan Page, as distinguished from a Facebook Group, can be appropriate as a supplemental method of communicating electronically with student groups if it is set up correctly. Unlike Facebook Groups, Fan Pages are public and visible to unregistered students and parents. District 125 guidelines must be followed when publishing content to any website. Photos of students should not be posted in conjunction with their names or other personally identifiable information. An employee should use their "@d125.org" email address to

register as a contact for the Page so that any feedback or comments are sent to the District, and not to any personal email addresses.

Setting up a Facebook Group Page:

While not the preferred method, a Facebook Group can be appropriate in certain situations. A Facebook Group may only be owned and must be monitored by a District 125 employee who has received administrative approval to set up the Group. Unlike Facebook Fan Pages, Group pages are not visible for unregistered students and parents and thus not searchable. Due to the nature of two-way messaging within a group, the District employee responsible for the Group must monitor its communications frequently. District 125 guidelines for publishing content to any website apply to Facebook Group Pages, including the prohibition on posting photos of students in conjunction with their names or other personally identifiable information. The responsible employee should use their "@d125.org" email address to register as contact for the Group, so that any feedback or comments are sent to the District, not to any personal email addresses.

If you decide to establish a fan or group page, you must notify the parents or guardians of your students in advance that you'll be using the site to communicate information to your group in addition to other methods such as websites, email, or form letters. You must also inform parents or guardians that these pages may contain commercial advertising that is not endorsed by District 125. Since not every student has a Facebook Page or access to Facebook, you must consider this when posting to your page. District 125 cannot require students to have a Facebook account. Therefore, you must make any information posted on Facebook accessible to non-Facebook users by alternate means.

Social Media Websites for Personal Purposes

Important reminders for employees who use Facebook, Twitter, LinkedIn, blogs or other social media websites. All District employees who use personal technology and social media shall always adhere to the high standards for appropriate school relationships required by policy 5:120 ("Employee Ethics; Conduct; and Conflict of Interest") regardless of the ever-changing social media and personal technology platforms available.

General Guidelines

1. Employees who use Facebook to communicate with friends, family, and their personal network should ensure their privacy settings are set to "Only Friends." Using the "Friends of Friends" or "Acquaintances" settings opens Facebook content to a much larger group of people including students and parents. Staff members should never "friend" students who are currently enrolled in District 125, or accept their "friend requests." An employee who has previously "friended" a currently enrolled District 125 student should "defriend" that student immediately. These guidelines apply to other relevant social media applications such as LinkedIn, Instagram, SnapChat, TikTok, etc.

2. The wall between the role of a public educator and personal friendships with students should always be visible and strongly communicated.

3. Employees should not publish, post pictures, or engage in a dialogue whether in social media, a blog, a discussion thread or another website that compromises their professionalism, integrity and ethics as District 125 professionals. A good question to ask is, does this communication satisfy TAP guidelines?

4. District 125 employees are expected to ensure that their online activities do not interfere with fulfilling their job requirements or their commitments to the students and community of District 125.

5. When contributing to online content, District 125 employees should:
    a. Use good judgment and common sense
    b. Post accurate information
    c. Not post defamatory, libelous, vulgar, obscene, abusive, profane, threatening, or otherwise offensive or illegal information or materials
    d. Comply with copyright laws
    e. Respect the privacy of staff members or of students

6. Employees who are not authorized to speak on behalf of District 125 in an official capacity should preface any online expression of opinions or comments about District 125 or its programs with a disclaimer clearly stating that their comments do not represent the views of District 125.

    For example: "The postings on this site are my own and do not necessarily represent the views or positions of my employer," or "My online postings/opinions are my own, not those of District 125."

7. When using the District Information Services Systems to communicate, Employees should know and comply with other existing District policies, rules, and conduct standards such as including those which pertain to harassment, anti-bullying (including cyberbullying), and students/staff relations. See Our Guide for Responding Online at d125.org.

8. Employees must maintain the confidentiality of privileged information, including student record information, personnel information, and other confidential District information.

SOPPA Student Online Personal Protection Act

The District is required to review all K-12 educational solutions that store or link to personally identifiable information or material, in any non-publicly available format. Review will be necessary where student data provided involves a K through 12 purpose. A "K through 12 purpose" is one which aids in the administration of instruction in the classroom or at home.

Review will not be necessary if the web service is not intended for school instruction, but instead serves a general audience (e.g. Google Search Engine. the Chicago Tribune website, etc.). When in doubt, employees are instructed to contact the Information Services Division. Upon review (if applicable), the District must enter into an agreement with the solution provider, which outlines what student data is stored, and what steps the provider will take in the event of a data breach.

Before a solution can be used, please consult the District database to determine if an agreement exists: https://sdpc.a4l.org/district_listing.php?districtID=6283. Or contact tech_trainers@d125.org for additional information.

Prohibitions

District students, employees, contractors, and guests are expected to act in a responsible, ethical and legal manner consistent with District policy, accepted rules of network etiquette, and federal and state law.

It is prohibited to use the District Information Services Systems:

1. To facilitate illegal activity.
2. For product advertisement or political lobbying.
3. For hate mail, discriminatory remarks, and defensive or inflammatory communication.
4. For unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials, including copyrighted software and school logo.
5. To access obscene or pornographic material.
6. For commercial or for-profit purposes.
7. To communicate with inappropriate language or profanity.
8. To transmit material likely to be offensive or objectionable to recipients.
9. To intentionally obtain or modify files, passwords, and data belonging to others.
10. To impersonate another user, or to use anonymity or pseudonyms.
11. For fraudulent copying, communications, or modification of materials in violation of copyright laws.
12. To load or use unauthorized games, programs, files, or other electronic media.
13. To disrupt the work of other users.
14. To destroy, modify, or abuse network hardware or software.
15. To quote personal communications in a public forum without the original author's or speaker's prior consent.
16. The illegal use of copyrighted software by students and District employees is prohibited.
17. To use the networks while access privileges are suspended or revoked.

Users are advised that to protect the integrity of the Information Services Systems:

1. The District has the right to and does monitor the use of the Systems.
2. Employees and students may not reveal their passwords to another individual.
3. Users must not use a computer that has been logged into using another person's name.

4. Users should not use computers to which they have not been given access by authorized personnel of the District.
5. A user who is identified as a security risk or who violates the Acceptable Use Guidelines may be denied access to the Systems.

Safety & Security

To the extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications should immediately bring them to the attention of a teacher or administrator.

Network users should not publish or reveal personal information about themselves or others on the network.

In order to maintain the security of the Systems, authorized users are prohibited from engaging in the following actions:

1. Use of unauthorized personal equipment attached, connected, and/or installed to the District's network.
2. Intentionally disrupting the use of the Systems network or technology resources for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, spreading computer viruses, engaging in "hacking" of any kind, use of proxy or filter avoidance software or devices, and/or engaging in computer tampering of any kind.
3. Disclosing the contents or existence of District computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients.
4. Downloading and/or installing and/or using unauthorized software, games, programs, files, electronic media, and/or stand-alone applications. Staff members are authorized to download or use items that are directly related to their job duties and only by following appropriate procedures.
5. Network security is a high priority. If you can identify a security problem on the network, you must notify a system administrator. Do not demonstrate the problem to other users.

Students' Personal Electronic Devices

District personnel may temporarily confiscate a student's personal electronic device when there are reasonable grounds to suspect the student is using or has used the device to violate the law or school rules, including these Acceptable Use Guidelines.

District personnel may search content stored on a student's personal electronic device when there are reasonable grounds to suspect that doing so will reveal evidence that the student has used the device to violate the law or school rules, including these *Acceptable Use Guidelines*. Except in exigent circumstances posing a significant risk of danger to members of the school community, school personnel will obtain permission of the student whose personal electronic device they wish to search, and of the parent or guardian, before conducting the search.

Except in such exigent circumstances, if the student and parent or guardian refuse permission, District personnel will seek a warrant to search the personal electronic device.

Consequences for Inappropriate Use and Other Violations of Acceptable Use Guidelines

In addition to the provisions of Board of Education Policy 6:235 (“Access to Electronic Networks”) and these Acceptable Use Guidelines promulgated as required under 6:235, and student and personnel discipline policies.

General rules for behavior and communication apply when using District Information Services Systems and the Internet. Consequences for inappropriate use may include, but are not limited to, loss of access and other disciplinary measures. These may include temporarily confiscating and retaining electronic devices when such devices are used to access and improperly use the District Information Services Systems.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or other networks, including by uploading or creating computer viruses or making or attempting to make equipment or networks unstable.

Illegal use of the District Information Services Systems, intentional deletion of or damage to files or data belonging to others, or theft of services will be reported to law enforcement authorities for possible prosecution.