Instruction

Administrative Procedure - Acceptable Use of the Cooperative's Electronic Networks

All use of the Cooperative's electronic networks shall be consistent with the Cooperative's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions

The term *electronic networks* includes all of the Cooperative's technology resources, including, but not limited to:

1. The Cooperative's local-area and wide-area networks, including wireless networks (Wi-Fi), Cooperative-issued Wi-Fi hotspots, and any Cooperative servers or other networking infrastructure;
2. Access to the Internet or other online resources via the Cooperative's networks or to any Cooperative-issued online account from any computer or device, regardless of location;
3. Cooperative-owned or Cooperative-issued computers, laptops, tablets, phones, or similar devices.

Acceptable Use - Access to the Cooperative's electronic network must be: (a) for the purpose of education or research, and be consistent with the Cooperative's educational objectives, or (b) for legitimate business use.

Privileges - Use of the Cooperative's electronic networks is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. The Executive Director, in consultation with Cooperative administrators and the Technology Coordinator, will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the networks. Some examples of unacceptable uses are:

a. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;
b. Using the electronic networks to engage in conduct prohibited by board policy.
c. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;
d. Unauthorized use of personal removable media devices (such as flash or thumb drives);
e. Downloading of copyrighted material for other than personal use;
f. Using the electronic networks for private financial or commercial gain;
g. Wastefully using resources, such as file space;
h. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;
i. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;
j. Using another user's account or password;
k. Disclosing any network or account password (including your own) to any other person, unless requested by the Technology Coordinator;
l. Posting or sending material authored or created by another without his/her consent;

m. Posting or sending anonymous messages;
n. Creating or forwarding chain letters, spam, or other unsolicited messages;
o. Using the electronic networks for commercial or private advertising;
p. Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;
q. Misrepresenting the user's identity or the identity of others; and
r. Using the electronic networks while access privileges are suspended or revoked.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
d. Recognize that the Cooperative's electronic networks are not private. People who operate Cooperative technology have access to all email and other data. Messages or other evidence relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the networks in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the electronic networks to be private property.

No Warranties - The Cooperative makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Cooperative will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The Cooperative specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - By using the Cooperative's electronic networks, the user agrees to indemnify the Cooperative for any losses, costs, or damages, including reasonable attorney fees, incurred by the Cooperative relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify or suspects a security problem on the network, the user must promptly notify the Technology Coordinator or Program Administrator. Do not demonstrate the problem to other users. Keep your user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as the Technology Coordinator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Telephone Charges - The Cooperative assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and Cooperative policy prohibit the re-publishing of text or graphics found on the Internet or on Cooperative website or file servers/cloud storage without explicit written permission.

a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.

b. Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of *public domain* documents must be provided.

c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The Cooperative's email system, and its constituent software, hardware, and data files, are owned and controlled by the Cooperative. The Cooperative provides email to aid staff members in fulfilling their duties and responsibilities.

a. The Cooperative 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.

b. 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.

c. Electronic messages transmitted via the Cooperative's Internet gateway carry with them an identification of the user's Internet *domain*. This domain name is a registered domain name and identifies the author as being with the Cooperative. 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 Cooperative. Users will be held personally responsible for the content of any and all electronic email messages transmitted to external recipients.

d. Any message received from an unknown sender via the Internet, such as spam or potential phishing emails, should either be immediately deleted or forwarded to the Technology Coordinator. 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.

e. Use of the Cooperative's email system constitutes consent to these regulations.

<u>Privacy Issues</u>

a) All incoming and outgoing email is stored by the Cooperative, even if you delete it from your inbox.

b) Keep in mind that any email regarding Cooperative business may be a *public record* and released to the public under a Freedom of Information Act request.

c) Any email concerning a student in which the student is individually identified (by name or other identifier) is part of their official record and can be accessed by the student, parent, or guardian.

d) Choose your words carefully. Avoid sending an email if you are upset. When in doubt, call or visit someone in person rather than sending an email that can never be completely deleted.

<u>Professional vs. Private</u>

a) **Your personal email address should never be used for Cooperative business.** Do not forward @ndsec.org emails to your personal email account. Your personal email account could be subject to FOIA requests or subpoenas if used to conduct Cooperative business. Your personal email can not protect private info as required by HIPAA.

b) **Your NDSEC email address should be used for Cooperative business only.** You should not use your @ndsec.org email address for personal emails as you have no expectation of privacy and they may become public.

c) **Unsubscribe** from junk mail or mailing lists that are not pertinent to your job. We want to avoid these messages coming into our email server, so **unsubscribe** rather than just deleting or marking as spam.

d) Do not create or forward joke emails or chain letters using your Cooperative account.

<u>Best Practices</u>

a) Do not request a read receipt for every email you send. This can be annoying to others.

b) **Include an Auto Signature with your name, school, title, and contacting information.** To set up an Auto Signature, go to the **Gear⚙ Settings**. Scroll down to the **Signature** section. Turn on the Signature and type your message in the box. Select **SAVE CHANGES** at the bottom of the screen.

<u>Approved Electronic Communication Tools</u>

a) NDSEC Google Tools
   1. Gmail
   2. Google Classroom
   3. Google Meet

b) NDSEC Remind Account

c) Twitter

d) Zoom

<u>Prohibited Electronic Communication Tools</u>

a) Facebook

b) Personal Email

c) Personal Text Messaging Account

d) Personal Social Media Account

While Cooperative-provided tools such as email or Google Suite are preferred methods of communication with students and their families, employees may utilize social media when the intent of the communication is related to their curricular or co-curricular position with the Cooperative. When utilizing social media to communicate, employees must:

- Utilize a professional, work only, social media/electronic communication account to communicate with parents and students.
- Adhere to the high standards for appropriate school relationships as outlined in Board policy and the Acceptable Use of the Cooperative's Electronic Networks administrative procedure.
- Maintain professional and appropriate communication and relationships with and among students while participating in communication on Cooperative and non-Cooperative hosted social networking and communication sites.
- Set social media accounts to only allow one-way communication that begins with the teacher and ends with the student.
- Keep a record of all communication with parents and students.
- Remember that electronic communication may be subject to the Freedom of Information Act (FOIA).
- Provide students and parents with official contact information (i.e., phone number, email address, social media account, etc.), and never provide them with a home or personal cell phone number, personal email address, or personal social media account name.

- Remember that the Cooperative website is the PRIMARY source of information regarding official Cooperative communication, schedules, cancellations and important announcements. Groups or programs that maintain their own websites must utilize a platform pre-approved by the Technology Coordinator to host their website.
- Utilize their Cooperative email account when communicating with students or families and only engage in email communication with students through their Cooperative-provided email address.
- Utilize Remind as a platform to provide updates to students or detailed information not designed for a more global audience.
- Utilize Twitter, if interested, as a platform to celebrate program accomplishments or disseminate information of interest to an audience larger than the employee's immediate classroom or team.

The Cooperative strongly recommends that employees:

- Adhere to the **TAP** test when posting material online.
  - Is it **T**ransparent?
    Electronic communication between staff, students, and parents should be transparent.
  - Is it **A**ccessible?
    Electronic communication between staff, students, and parents may be a matter of public record and may be accessible by others.
  - Is it **P**rofessional?
    All electronic communication from staff to students or parents should be written in a professional manner that takes word choice, tone, grammar, and subject matter into consideration. Employee electronic communication should provide students with a positive example of how to navigate the digital world.
- Ensure the privacy settings on your personal social media accounts are set to the highest possible security settings to prevent students or parents from accessing or viewing your content. If you use a personal Facebook account, you should strongly consider setting the privatization setting to "Only Friends" rather than "Friends of Friends" or "Networks and Friends" to help ensure parents and students have no way to access your content.
- Do not "friend" or "follow" current students.
- Weight carefully your decision to "friend" or "follow" former students before doing so.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is supported if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using Cooperative Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

When on school district or Cooperative property, each internet-connected device is filtered by a web content filter that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Executive Director or designee.

The Technology Coordinator and Program Administrators shall monitor student Internet access.

LEGAL REF.: 20 U.S.C. §7131, Elementary and Secondary Education Act.
47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
720 ILCS 135/, Harassing and Obscene Communications Act.

Implemented: 8/2010
Updated: 11/2012
Updated: 8/2018
Updated: 7/2019
Updated: 10/2021