STAFF DUNLAP CUSD#323 INTERNET & ELECTRONIC NETWORK USE PROCEDURE

All use of Dunlap CUSD# 323's electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. It is essential for all students to have access to electronic devices and networks as part of the District curriculum. These procedures do not attempt to state all required or proscribed 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 appropriate legal action.

A. Risk

With access to computers and people all over the world also come the availability of material that may not be considered appropriate for student use. Sites accessible via the Internet may contain material that is illegal, defamatory, obscene, inaccurate or controversial. District 323 has taken precautions to restrict access to controversial materials. Each computer in the District 323 capable of accessing the Internet has installed on it a software package designed to block out objectionable web sites. An additional software package that blocks objectionable sites is also installed on District servers that connect to the Internet. However, no manufacturer of such software will offer a 100% guarantee that their product will eliminate all objectionable sites. The technology available today is not capable of achieving this goal.

Technology can still be supplemented by human resources, however, and District 323 believes that supervision is still the most effective way to discourage students from accessing inappropriate information on the Internet. Every effort will be made to ensure that adult supervision is present while students are accessing the Internet. While the District is making every effort to prevent students from directly or indirectly accessing objectionable web sites, it must be understood that at this time no system will ensure complete security.

B. Terms and Conditions

Privileges - The use of the District's Internet and electronic network is necessary for your position, and personal inappropriate use will result in disciplinary action. The Superintendent or designee will make all decisions regarding whether or not a user has violated this **Authorization** and may deny, revoke, or suspend access at any time.

Acceptable Use - Access to the District's technology and electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use. The user is expected to abide by the generally accepted rules of network etiquette, whether accessing the network form a District-owned or personal device. These include, but are not limited to the following:

a. Be polite. Do not become abusive in your 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 electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be private property.

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

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
c. Downloading copyrighted material for other than personal use;
d. Using the network for private financial or commercial gain;
e. Wastefully using resources, such as file space;
f. Hacking or gaining unauthorized access to files, resources or entities;
g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
h. Using another user's account or password;

i. Posting material authored or created by another without his/her consent;
j. Posting anonymous messages;
k. Using the network for commercial or private advertising;
l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; (Unintentional accessing such shall be immediately made known to the System Administrator and Superintendent.)
m. Using the network while access privileges are suspended or revoked.
n. Removing hardware/software, networks, information, or communication devices from the District or other network; and
o. Installing client VPN's or configuring proxy servers on district devices or using such tools to circumvent content filtering or other network restrictions.

C. Internet Safety

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

Each District computer with internet access and any personal device accessing our network, has a filtering device 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 Superintendent or designee.

D. Privacy

Electronic communications are not private and staff members have no rights, ownership or expectation of privacy in any material that is stored, transmitted, or received via the District's network or electronic devices. The District reserves the right to access all electronic communications transmitted on its networks, including those deleted from a user's account but not erased. Electronic communications relating to or in support of illegal activities may be reported to the authorities.

E. Personal Technology and Social Media

All District employees who use personal technology and social media shall:

a. Adhere to the high standards for appropriate school relationships required by policy 5:120, Ethics and Conduct, at all times, regardless of the ever-changing social media and personal technology platforms available. This includes District employees posting images or private information about themselves or others in a manner readily accessible to students and other employees that is inappropriate as defined by policy 5:20, Workplace Harassment Prohibited; 5:100, Staff Development Program; 5:120, Ethics and Conduct; 6:235, Access to Electronic Networks; 7:20, Harassment of Students Prohibited; and the Ill. Code of Educator Ethics, 23 Ill. Admin. Code §22.20.
b. Choose a District-provided or supported method whenever possible to communicate with students and their parents/guardians.
c. Not interfere with or disrupt the educational or working environment, or the delivery of education or educational support services.
d. Comply with policy 5:130, Responsibilities Concerning Internal Information. This means that personal technology and social media may not be used to share, publish, or transmit information about or images of students and/or District employees without proper approval. For District employees, proper approval may include implied consent under the circumstances.
e. Refrain from using the District's logos without permission and follow Board policy 5:170, Copyright, and all District copyright compliance procedures.
f. Use personal technology and social media for personal purposes only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.
g. Assume all risks associated with the use of personal technology and social media at school or school sponsored activities, including students' viewing of inappropriate Internet materials through the District employee's personal technology or social media. The Board expressly disclaims any responsibility for imposing content filters, blocking lists, or monitoring of its employees' personal technology and social media.
h. Be subject to remedial and any other appropriate disciplinary action for violations of this policy ranging from prohibiting the employee from possessing or using any personal technology or social media at school

F. Use of E-mail

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.

a. 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.

b. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached or any internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

c. 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.

d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies 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.

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

G. Google Apps for Education.

In partnership with Google, the District will offer staff members access to Google Apps for Education, which is a collection of free online cloud-based Google applications tailored specifically for educational institutions. Each staff member will be given a Google account with access to various Google Apps, including Google Drive, Google Docs, Google Sheets, Google Slides, Google Calendar, and Google Gmail. These Google Apps may be accessed at school or at home via your log-in information.

Use of Google Apps for Education shall be in accordance with the terms and conditions set forth in this **Authorization**. The Google Apps for Education accounts are property of the District and staff members have no rights, ownership or expectation of privacy in any material that is stored, transmitted, or received via their Google account. Monitoring software is linked to the Google accounts and Google account activity may be monitored, accessed, and searched by the Director of Technology, Building Principal or designees, regardless of whether the Google Account is accessed or used at school, or at home.

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

I. Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers 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.

J. No Warranties

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer or cause. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services including accuracy or quality, obtained or transmitted through use of the Internet. Further, the District denies responsibility for any information that may be lost, damaged, altered, or unavailable when using the Internet.

K. Indemnification –

The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this **Authorization.**

L. Security - Network security is a high priority. If you can identify a security problem on the Network, you must notify your administrator or program director. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the electronic network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to network.

M. 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 computer viruses.

N. Consequences of Policy Violation

An attempt to violate the provisions of this policy may result in revocation of the user's Internet access privileges regardless of the success or failure of the attempt. Further disciplinary action, as outlined in District 323 policy, including notification to state and federal authorities, may also be taken.