Instruction

District 27's computer and network resources are solely for the use of authorized District 27 students, staff, adult education students and other specifically designated users.

This Policy governs all use of District 27 technologies and technological resources while on or away from District property, including accessing the District 27 network resources via a personally owned device. District 27 technologies and technological resources (including, but not limited to, the District's school-issued computers and access to the Internet through the District's network) are collectively referred to in this policy as the District's "Technology Network."

Access to Electronic Networks

Electronic networks are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication.

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

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

The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social

networking websites and in chat rooms, and (2) cyberbullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Users of the District electronic networks have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks. Yet, no Personal Identifiable Information will be shared that would be in violation of FERPA or SOPPA. General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, Acceptable Use of the District's Electronic Networks, contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the *Authorization for Access to the District's Electronic Networks* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use.

Confidentiality

All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

Violations

The failure of any user to follow the terms of the District's administrative procedure, *Acceptable Use of the District's Electronic Networks,* or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Permissible Use of Technology in the District and Via Remote Learning Platforms

The Technology Network is to be used primarily for academic and administrative purposes and not as a public forum for general use. Access to the District's Technology Network is a privilege, not a right. By using or accepting any portion of District 27's Technology Network and signing the attached authorization form, the user hereby agrees to the following terms and conditions. Any violation of which may result in the loss of privileges, disciplinary action, including suspension and expulsion, and / or appropriate legal action.

Acceptable Uses:

a. Curricular and instructional activities that are consistent with the educational objectives of District 27;
b. Research consistent with the educational objectives of District 27;
c. Communications between students, faculty, staff, and the local and global communities pertaining to curricular and instructional activities;
d. Usage of video conferencing and other tools for instruction. Examples include ZOOM, Google Hangouts Meet, GoGuardian, and others.
e. Development and implementation of the curricula;
f. Professional development of staff members;
g. Administrative or managerial record-keeping, or reporting data access; and
h. Electronic communication between staff and students must conform to District 27's requirements with respect to the content of the communication and the method of communication.
    1. As for the content of electronic communication between staff and students, it must be professional and transparent as set forth below:
        a. All electronic communication between staff and students must be written using a professional and businesslike tone, and strictly pertain to District 27 educational objectives or activities.
        b. All electronic communication between staff and students should be presumed to be a matter of public record.
    2. All electronic communication between staff and students should be made via a District 27 e-mail account or District 27-sponsored website or other appropriate venues.

Unacceptable Methods and Uses: (This list is meant to be illustrative and non-exhaustive)

Using any technology, either District owned or personal, to engage in inappropriate contact with a student or students;

a. Performing any activity that materially and substantially disrupts the proper and orderly operation and discipline of District 27's schools;
b. Performing any illegal activity including, but not limited to, violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law or regulation;
c. Engaging in online gaming and associated websites to communicate or interact with students;

d. Utilizing personal social networking forms of electronic communication (e.g. Facebook, Twitter) to communicate with students;

e. Utilizing personal, non-district approved, text-messaging to communicate with individual students;

f. Unauthorized downloading, uploading, modification or installation of software, regardless of whether it is copyrighted or free of viruses;

g. Downloading copyrighted material for other than permissible use;

h. Using the network for private financial or commercial gain;

i. Wastefully using resources, such as file space;

j. Creating or forwarding chain letters, "spam," or other unsolicited or unwanted messages;

k. Creating or sending e-mail or other communications which purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;

l. Accessing, using or possessing any material in a manner that constitutes or furthers fraud (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright or other intellectual property right;

m. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the District's Technology Network or on any external computer, computer system, or computer account;

n. Taking any steps which threaten, or which may reasonably appear to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat;

o. Engaging in cyberbullying, as set forth in the Cyberbullying section of this policy;

p. Engaging in any type of sexual discrimination and/or sexual harassment, as set forth in District's 27 Sexual Harassment Policy;

q. Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information;

r. Using another user's account or password;

s. Posting anonymous messages;

t. Posting material authorized or created by another without his/her consent;

u. Failure to comply with computer software licensing agreements held by the District;

v. Deliberately accessing, transmitting, submitting, posting, publishing, or displaying any defamatory, abusive, obscene, profane, sexually oriented, threatening, offensive, harassing, or illegal material;

w. Using the network while access privileges are suspended or revoked;

x. Using the Technology Network to participate in acts constituting "prohibited political activities" under the *State Officials and Employees Ethics Act* or "election interference" under the *Election Code* or to participate in any political activities that create an appearance of impropriety under those laws or under any ethics policy of the District relating to political activities of the District's employees;

y. Using the Technology Network in a way that threatens the integrity or efficient operation of District 27's or any other public or private entity's Technology Network.

z. Attempting to commit any action which would constitute an unacceptable use if accomplished successfully; and,

aa. Using the Technology Network to violate any other District policy.

bb. Only Northbrook School District 27 employees are authorized to distribute screenshots, photos, audio/video recordings and distribution of any virtual educational experiences. This is in order to protect privacy, prevent cyberbullying and reduce distribution of content from virtual educational experiences.

cc. Parents/guardians and other household members who normally are not privy to day-to-day classroom activities, agree to respect and keep confidential any personal or private information (e.g. disability status) inadvertently discovered about other students due to proximity to virtual education.

Video Conferencing Etiquette for Presenters and Attendees

- During video conferencing, students and adults are expected to follow appropriate network etiquette, wear appropriate clothing, and use appropriate pictures, emojis, and/or avatars. All inappropriate behavior as judged by the building and District administration will be subject to discipline.

Network Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite and non-abusive in messages.

b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.

c. Do not reveal the address, telephone number, or personal information of students or staff members without their permission.

d. Recognize that electronic mail (E-mail) is not private and may be monitored. 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.

Student Safety

As a precaution to maintain personal safety:

a. Students should not give out such personal information as their full name, age, home address, telephone number(s), photograph, their parents' or guardians' work address or telephone number, or the name or location of the school over the Internet or through email. Students should not give out such personal information about other individuals over the Internet or through email.

b. Students should immediately inform their parents, guardians, or a member of District staff if they come across any information on the Internet or in an email that makes them feel uncomfortable. Students should not respond to any e-mail or other message which makes them feel uncomfortable.

c. Students should never agree to meet someone in person whom they have "met" online without parental knowledge, permission, and supervision.

d. Students should never agree to send or accept any item to or from a person whom they have "met" online without parental knowledge, permission, and supervision.

Cyberbullying

Cyberbullying includes, but is not limited to, harassing, sexually harassing, teasing, impersonating, intimidating, stalking, threatening or terrorizing any person or group of persons by sending or posting inappropriate and / or harmful e-mail messages, instant messages, text messages, digital pictures, images or video, or web site postings because of actual or perceived race, color, religion, sex, national origin, ancestry, age, marital status, physical or mental disability, military status, sexual orientation, gender-related identity or expression, association with a person or group with one or more of the aforementioned actual or perceived characteristics, or any other distinguishing characteristic or reason.

Students and staff are expected to treat each other respectfully at all times, including through the use of technology as a form of communication. Cyberbullying should be reported to school personnel (who in turn will report to school administration). Investigation and disciplinary consequences for cyberbullying shall be in accordance with District policy, including District discipline policies. Discipline may include, but is not limited to, the loss of computer privileges, detention, suspension, or expulsion. Students and staff may be disciplined for cyberbullying that occurs on school property or through the use of District 27's Technology Network, including off-campus use of a school-issued computer. In addition, students and staff may be disciplined for cyberbullying that occurs off-campus on a personal computer if the personal technology use causes a material and substantial disruption to school operations, or otherwise has a clear nexus to school.

No Warranties

The District makes no warranties of any kind, whether expressed or implied, for the services it is providing. The District shall not be responsible for any of the following in connection with the use of the District's Technology Network, including but not limited to the following:

a. Loss, damage, alteration, or unavailability of data.
b. Physical or psychological damages incurred by the user.
c. Accuracy or quality of information obtained.
d. Connecting to the Internet.

Indemnification

Use of District 27's Technology Network constitutes agreement by the user to indemnify District 27, its Board, employees, and agents for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this policy.

Privacy/Monitoring

Any electronic communications or files created on, stored on, or sent to, from, or via the Technology Network are the property of the District. As a result, there is no expectation of privacy with respect to the use of District 27's Technology Network. Messages and files can be recovered even after they have been deleted from a user's individual account.

Administration and authorized staff may access, monitor, and review such messages and files without prior notice or permission from the account's user. The District reserves the right to intercept, access, and disclose to appropriate authorities all information created with, sent to, received by, or stored on the Technology Network at any time, with or without user notification. Use of the District's Technology Network constitutes consent by the user for the District to access and review such files consistent with this paragraph.

Security

If a security problem on the Technology Network is identified, the user shall notify the instructor, system administrator(s) or building principal and not divulge this problem to other users. Account and password information shall be kept confidential except users must provide account and password information to the system administrator(s) as appropriate.

Enforcement

Technology Network privileges may be suspended or revoked by the Superintendent or Building Principal. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies. Suspected criminal conduct may be referred to law enforcement authorities.

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. The user (or parent/guardian of a minor user) assumes full responsibility for any unauthorized charges or fees incurred by such user, including, but not limited to, telephone charges, long distance charges, per minute surcharges, and/or equipment or line costs.

Bring Your Own Technology (BYOT)

The District provides a primary device for students to engage in the academic program. The District does not support a BYOT program for students. The District provides a primary device for staff to engage in their work. If staff chose to bring their own privately owned device to work, all aspects of the Acceptable Use Policy are in effect. Moreover, the District Technology Department will not be responsible for providing support for the use of this privately owned device. In the event that a privately owned device is lost, stolen, or damaged, District 27 is not responsible for any financial or data loss.

Northbrook School District 27
Authorization for Internet Access
Grades K-8

Authorization for Internet Access

STUDENT NAME: _____GRADE _____SCHOOL/TEAM_____
(Please print)

I understand and will abide by District 27's PERMISSIBLE USE OF DISTRICT TECHNOLOGY NETWORK policy. I further understand that should I commit any violation of this policy, my privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District

Technology Network and having access to public networks, I hereby release District 27 and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use, the District Technology Network.

DATE _____

_____

PARENT/GUARDIAN NAME (Please Print):

Signature: _____

Student Signature: _____

Northbrook School District 27
Authorization for Internet Access
Staff Members

Authorization for Internet Access

NAME: _____

SCHOOL/TEAM: _____

(Please print)

I understand and will abide by District 27's Policy 6:235. I further understand that should I commit any violation of this policy, my privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District

Technology Network and having access to public networks, I hereby release District 27 and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use, the District Technology Network.

I further understand that it is my responsibility to be familiar with the content of Policy JFCB as it is currently written or as it may be revised by the Board of Education.

DATE _____

Signature: _____

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.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
115 ILCS 5/14(c-5), Ill. Educational Labor Relations Act.
720 ILCS 5/26.5.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:220 (Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

REVIEW HIS: 1996, 2007, 2010, 2017, 2020, December 2021