CENTRAL HIGH SCHOOL DISTRICT NO. 71 BOARD POLICY MANUAL

5.61 USE OF TECHNOLOGY POLICY - INSTRUCTION

Section 1: Purpose

Central Community High School District #71, through its Superintendent or designee, may authorize staff, students and other individuals to use or otherwise access District Technology, as defined below, for professional, educational or other uses that further the District's interests. The sole purpose of such use or access is to improve the education of District students and the educational environment of which they are a part. This policy and related administrative procedure shall outline the responsibilities, requirements and other restrictions that govern use of and access to District Technology.

Section 2: Definitions

For purposes of this policy and any related administrative procedure, the following definitions shall apply:

"District Technology" - Any computers, electronic devices, systems, software or network owned, operated or provided by the District, including but not limited to servers, desktop and laptop computers, mobile phones, smartphone devices, IP telephone devices, devices that provide internet and/or network connectivity, e-mail and messaging systems and accounts owned or operated by or on behalf of the District, web pages published on the District's web servers and/or under its domain and any other personal communications devices or software that run on any of the above. For purposes of this definition, a network is a collection or collections of computers, electronic devices, systems and/or software that are interconnected by communications systems to facilitate sharing of information, data and/or electronic resources or to otherwise communicate electronically with others.

"Authorized User" - Staff, students and/or other individuals who the Superintendent or designee has explicitly authorized to use or access District Technology for professional, educational and/or other uses that further the District's interests.

Section 3: Applicability

An individual acknowledges this policy and related procedures and is subject to its terms by using or accessing District Technology. A user need not sign and return an acknowledgement form to be subject to this policy and related procedures.

Section 4: Acceptable Use

Only Authorized Users may use or access District Technology. Authorized Users are expected to use or access District Technology for professional, educational or other uses that further the District's interests, which include but are not limited to research, professional communications and other administrative and educationally relevant activities. Authorized Users are also expected to maintain the highest standards of

ethical behavior and to assume personal responsibility for their use. Other uses (including personal uses) must be minimal *(de minimis)* and must not interfere with the purposes of this policy or the District's interests.

In addition to complying with this policy, Authorized Users must comply with State and federal laws and regulations, the terms of administrative procedures implementing this policy and the terms of any other related policies and procedures. The Superintendent or designee may require a user (and his or her parents, if the user is a student) to sign and return an acknowledgement form (Acceptable Use Agreement) acknowledging the duty to comply with such policies, procedures, laws and regulations before becoming an Authorized User.

Section 5: Limited Rights of Use

Use of District Technology is a privilege, not a right. District Technology is not a limited public forum.

The Superintendent or designee may, when necessary in his or her sole discretion, act to protect and ensure the operability, integrity, security and reliability of District Technology, which may require denying users access in whole or in part.

Materials created by staff members in or related to the performance of their employment duties, including materials created on District Technology are property of the District. The District retains the right to review, edit and/or delete any material posted on the District's web servers or web pages or on behalf of the District on other web servers or web pages at any time.

No Expectation of Privacy - Users have no expectation of confidentiality or privacy with respect to any communication or access made through District Technology, regardless of whether that use is for District-related or personal purposes, other than as specifically provided by law. The District may, without prior notice or consent, log, supervise, access, monitor and record use or access District Technology (including reviewing files and other materials) at any time for any reason related to the operation of the District and/or for any purpose that furthers the interests of the District. By using or accessing District Technology, users agree to such access, monitoring and/or recording of their use.

Section 6: Internet Safety and Protection

The District installs and operates filtering software on District Technology to limit users' Internet access to obscene, pornographic, harmful to children, or otherwise inappropriate material as required by the Children's Internet Protection Act. The District does not and cannot guarantee the efficacy of such software. It may block access to legitimate materials, and may fail to successfully block access to all inappropriate material. The District's use of such software does not absolve users of the responsibility not to access inappropriate materials or to otherwise abide by State and federal laws and regulations, the terms of administrative procedures implementing this policy and the terms of any related policies and procedures.

Section 7: Responsibility For use and/or Misuse

No Warranties - The District is not responsible for any information that may be lost or damaged (including being rendered unavailable) by use or access of District Technology or any material or services accessed and/or transmitted thereby or thereon, including the Internet and e-mail, the District specifically denies any liability or responsibility for transmissions or other communications made by any user of District Technology.

User Responsibility - Each Authorized User must maintain the confidentiality of any username(s) and/or password(s) provided to access District Technology and is responsible for all actions taken under those username(s) and/or password(s). Each Authorized User is responsible for any loss, damage, charges or other fees resulting from use of the District Technology unless those charges are authorized by the Superintendent or designee prior to being incurred.

By using District Technology, all users agree to indemnify the District to the extent allowed by law for any losses, costs, unauthorized charges or damages, including reasonable attorney's fees, incurred by the District relating to or arising out of the violation of this policy or any related procedures, other related policies and procedures or state or federal law.

Section 8: Enforcement

Where the Superintendent or designee determines that an Authorized User has violated this policy or related procedures, any other relevant District policy or procedure, and/or State or federal law, he or she may revoke or suspend the Authorized User's access rights. All users, whether authorized or unauthorized, may also be subject to criminal liability and/or civil liability to the extent authorized by law, as well as disciplinary action up to and including suspension and dismissal (staff) or expulsion (students).

Section 9: Administrative Procedures

The Superintendent shall establish administrative procedures that implement this policy, and shall take any other action appropriate to implement this policy.

LEGAL REF.:	No Child Left Behind Act, 20 u.s.c. §6777. Children's Internet Protection Act, 47 u.s.c. §254(h) and (1). Enhancing Education Through Technology Act, 20 u.s.c §6751 et seq. 720 ILCS 135/0.01. 705 ILCS 405/3-1.
CROSS REF.:	5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Publications)

Adopted: December 19, 2016

5.61A USE OF TECHNOLOGY POLICY – ADMINISTRATIVE PROCEDURE (ACCEPTABLE USE OF ELECTRONIC NETWORKS)

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. 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 legal action.**

Terms and Conditions:

Acceptable Use - Access to the District's 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.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building Principal 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 network. 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 of 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; and

m. Using the network 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 email is not private. People who operate the system have access to all email. 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.

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 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 District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

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 violation of these procedures.

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. 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 Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

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.

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.

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.

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.

a. 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.
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 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.
d. 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 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 School District's email system constitutes consent to these regulations.

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.

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

Each District computer with Internet access 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.

The system administrator and Building Principal(s) shall monitor student Internet access.

LEGAL REF.: No Child Left Behind Act, 20 u.s.c. §6777.
Children's Internet Protection Act, 47 u.s.c. §254(h) and (1).
Enhances Education Through Technology Act of 2001,20 u.s.c §6751 et seq.
Harassing and Obscene Communications Act, 720ILCS 135/0.01.

Adopted: December 19, 2016

5.61B USE OF TECHNOLOGY POLICY – ADMINISTRATIVE PROCEDURE (USE OF TECHNOLOGY - WEBSITES)

This administrative procedure implements District Policy 5.61, *Use of Technology,* and incorporates by reference all definitions in and terms of that policy. These procedures provide some specific guidelines regarding use of both "Internal" and "External" websites which are defined as:

- *Internal Sites:* Any networked or online District resource that allows publishing of content in any format that is accessible to students, staff, or the public where accounts and access are created and maintained by the District technology department.
- *External Sites:* Any online District resource (including social networks) that allows publishing of content in any format that is accessible to students, staff, or the public where accounts and access are not created and maintained by the District technology department.

The term "Sites" in this administrative procedure refers to both Internal and External Sites and any site created by an employee, volunteer, or student that identifies the content author or contributor as an employee, volunteer, or student associated with the District, as well as any site that links back to any Internal site.

Teachers, administrators, coaches, activity sponsors, and students are authorized to create, publish, and collaborate on Sites related to educational, professional, and other purposes that further the District's interests. This is a limited authorization and does not create a limited public forum. Moreover, content published in this manner is subject to the same rules and regulations as all other District Technology activity, including the limitations on user rights.

Risks

The District cannot guarantee that the content of Sites will be error-free or completely dependable. While the District will strive to ensure that Sites created by District employees, volunteers, and students are accurate and appropriate, the District is not liable or responsible for: (1) any information that may be lost, damaged, or unavailable due to technical or other difficulties; (2) the accuracy of information on Sites; (3) breaches of confidentiality; or (4) the unauthorized use of or access to District Sites.

Subject Matter

All subject matter on Sites must relate to curriculum, instruction, school-related activities, or general information relating to the school district and its schools. Professional pages (which might include academic qualifications, credentials, and related items) are allowed and strongly encouraged. Personal Sites (those containing personal information not directly related to academics) are prohibited.

Documents may not contain objectionable material or provide links to objectionable material. "Objectionable" means offensive, obscene, abusive, profane, pornographic, lewd, vulgar, threatening, racially or sexually offensive, harassing, inflammatory, or defamatory, and is defined in the discretion of the District administration.

Quality

Anything posted on a Site must be free of spelling and grammatical errors, time-specific material must be kept up to date. All content appearing out of date (30 days or more past an event or timeline at the longest) may be removed from the Web by the Director of Technology without prior notice or consent.

Ownership

All Internal Sites are the property of the District. All External Sites created and used on District time, using District Technology, and/or for work-related purposes may be considered "work for hire." Ownership of physical and virtual products so created must be surrendered by the creator of the work to a building or District administrator upon request, including any online material created to be used with students for instructional or co-curricular purposes.

Student Protections

- Students must be identified only by first name or initials on all Sites. No other personally identifiable information will be published. Student phone numbers and home addresses shall never be published.
- Students or parents may select not to have their image (video or still) in District publications and Sites by updating the Photo Release Form.

Copyright

Electronic transmissions and posting materials on the Web are forms of copying. Users may not produce, transmit, or post unlawful copies of copyrighted materials via District Technology. Site creators and contributors will only post material that, to the best of their knowledge, is not copyrighted or trademarked, or, for material that is copyrighted or trademarked, post only with the permission of the copyright or trademark holder and include documentation verifying the granting of permission. Users should not use photographs, drawings, video clips, sound clips, or other media on a Site without permission of the person who owns the rights to them.

All links that take users to websites outside the District's pages should be identified as not being part of the District's site.

Use of Sites

The following guidelines and procedures must be followed by employees, volunteers, and students when using or authoring any Site:

- All Sites must adhere to all laws and District policies.
- Sites created by or collaborated on by employees, volunteers, or students that violate the law, are inconsistent with the District mission statement, disrupt the educational process, interfere with an employee's performance or work responsibility, are not in accord with this policy, or that damage the integrity of the District are prohibited. Such Sites will be removed upon request of the administration and may result in disciplinary action.
- Nothing will be posted on a Site that is discriminatory, confidential, threatening, libelous, disparaging, obscene, indecent, or makes slanderous comments about

the District, its employees, students, or parents. Employees, volunteers, and students are personally liable for their own commentary.
- Any Site that is found to interfere with the educational process or work performance, result in unproductive use of time, violate any District policy, or be unlawful may be blocked using the District's content filter
- Failure to follow these guidelines and procedures may result in the loss of authoring and contributing privileges or other more severe disciplinary measures including student suspension or expulsion, employee termination, or legal action.

Best Practices for Using Sites

The following should be practiced and modeled by staff and are expected of students when publishing to Sites:

- Review District policies.
- Develop and test all Sites prior to using or assigning them.
- To the best of your ability, ensure usability for all visitors and participants and check that the content reflects yourself and the District.

External Web Content and Social Networking Sites

Many External Sites may be appropriate for instructional and work related purposes. The following points must be followed when working with external Sites:

- All laws and District policies must be followed.
- An employee, volunteer, or student that posts, creates, collaborates on, or modifies content on external Sites must:
    a. Register with a District email address.
    b. Provide access to these Sites to an administrator immediately upon request.
    c. Be aware that the District may monitor these Sites and that the content on these Sites is still subject to FOIA and legal discovery.
- Teachers that require the use of external Sites in their courses must reference the Sites on their syllabi.
- Direct communication between staff and students or parents may not take place through any external Site unless the communication is automatically and completely copied to the District email system.
- Employees, volunteers, and students that use external Sites take full responsibility and liability for anything they post and will fully accept any repercussions from unacceptable use.

Adopted: December 19, 2016