

Instruction

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

All use of the District's 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 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

Acceptable Use - Access to the District's electronic networks 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 - Use of the District's electronic networks 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 networks. Some examples of unacceptable uses are:

- a. Using the networks 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 networks 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 networks 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 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 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 networks in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the networks 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 Network, 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 Network as a system administrator 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 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 Principals 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 (l).
Enhances Education Through Technology Act of 2001, 20 U.S.C §6751 et seq.
Harassing and Obscene Communications Act, 720 ILCS 135/0.01.

Instruction

Exhibit - Student Authorization for Access to the District's Electronic Networks

This form accompanies Administrative Procedure 6:235-AP1, Acceptable Use of the District's Electronic Networks. It must be signed when students will have unsupervised Internet access or when supervision will be minimal. Please submit this form to the Building Principal.

Dear Parents/Guardians:

Our School District has the ability to enhance your child's education through the use of electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Students and their parents/guardians need only sign this *Authorization for Access to the District's Electronic Networks* once while the student is enrolled in the School District.

The District *filters* access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have a network account, sign the *Authorization* form below and return it to your school.

Authorization for Access to the District's Electronic Networks Form

Students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the *Acceptable Use of the District's Electronic Networks* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of the District's Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic networks, including the Internet.

Parent/Guardian Name (*please print*)

Parent/Guardian Signature

Date

Students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the *Acceptable Use of the District's Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District's electronic networks, including the Internet, my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic networks, including the Internet.

Student Name (*please print*)

Student Signature

Date

Instruction

Exhibit - Staff Authorization for Access to the District's Electronic Networks

This form accompanies Administrative Procedure 6:235-API, Acceptable Use of the District's Electronic Networks. Each staff member must sign this Authorization as a condition for using the District's Electronic Networks. Please submit this form to the Building Principal.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. Administrative Procedure 6:235-API, *Acceptable Use of the District's Electronic Networks*, does not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of *Acceptable Use of the District's Electronic Networks*, will result in the loss of privileges, disciplinary action, and/or legal action.** The signature at the end of this document is legally binding and indicates that the individual has read the terms and conditions carefully and understands their significance.

Staff members need only sign this *Authorization for Access to the District's Electronic Networks* once while employed by the School District.

I understand and will abide by the *Acceptable Use of the District's Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District's electronic networks, including the Internet, my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its School Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic networks, including the Internet.

User Name *(please print)*

User Signature

Date

Instruction

Administrative Procedure - Web Publishing Guidelines

General Requirements

All material published on the District's website must have educational value and/or support the District guidelines, goals, and policies. Material appropriate for web publishing includes information about the District and its School Board members, agendas, policies, appropriate administrative procedures, Department activities or services, schools, teachers or classes, student projects, and student extracurricular organizations.¹ Personal information, not related to education, will not be allowed on the District's website.

The District webmaster shall implement a centralized process for review and uploading of material onto the District's website to ensure that, before material is published, it complies with District policy and procedures.² The District webmaster shall supervise the efforts of all staff members responsible for web publishing at each level of District web publishing and, when appropriate, hold in-service opportunities for those staff members. The staff members responsible for web publishing are identified in these procedures in the section **Different Levels of Web Publication**. The District webmaster shall provide regular feedback and suggestions to the Superintendent regarding these Guidelines.

All content published on the District's website must:

1. Comply with all State and federal law concerning copyright, intellectual property rights, and legal uses of network computers.
2. Comply with Board policies, administrative procedures, these Guidelines, and other District guidelines provided for specific levels of publishing. This specifically includes the Board's *Access to Electronic Networks* policy and the District's procedures on *Acceptable Use of the District's Electronic Networks*.³
3. Due to limited storage space and varying network speeds, file sizes must be kept under 500 kilobytes⁴ unless the District webmaster approves otherwise.
4. Comply with the publishing expectations listed below.

Material that fails to meet these Guidelines or is in violation of Board policy and/or procedures shall not be published on the District's website. The District reserves the right to remove any material in violation of its policy or procedures. Failure to follow these Guidelines or Board policy and/or procedures may result in loss of privileges, disciplinary action, and/or appropriate legal action.

¹ IASB Policy Services provides web publishing services for board policy manuals. For information about these services and to see sample policy manuals online, visit

² A centralized process for review and uploading of material on district web pages will assist compliance with law and district policy and procedures in a consistent fashion across the district. If appropriate, replace "District webmaster" with correct title (e.g., District Network System Administrator).

³ See 6:235, *Access to Electronic Networks* and 6:235-API, Administrative Procedure - *Acceptable Use of the District's Electronic Networks*.

⁴ Customize the file size limitation to meet the district's needs.

Publishing Expectations

The following are minimum expectations for all District web pages:

1. The style and presentation of web published material should be of high quality and designed for clarity and readability. Material shall not be published in violation of the District's procedures on *Acceptable Use of the District's Electronic Networks*, including material that is defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or harassing, or material that invades the privacy of any individual. Anonymous messages are prohibited.
2. Correct grammar and spelling are expected.
3. All information must be verifiable.
4. Publications must include a statement of copyright when appropriate and indicate that permission has been secured when including copyrighted materials.
5. Publications must identify affiliation with the District, school, and/or department.
6. Widespread use of external links to non-District websites is discouraged, but if used, the external sites must contain appropriate educational materials and information as exclusively determined by the District.⁵ Every effort should be made to ensure that all links are operational. Every link to an external website must open a new browser window.⁶
7. Relevant dates are required on all publications, including the date on which the publication was placed on the District's website. Each site should contain the date the page was last updated.
8. All publications must include the District email address of the staff member responsible for the page. This provides a contact person for questions or comments. If a student is the publisher, the sponsoring staff member's email must be included as the responsible person. Only District staff members may act as student sponsors.
9. Use of the District's website for personal or financial gain is prohibited. No commercial or private accounts should be listed on any District web pages.
10. All documents should be previewed on different web browsers, especially Google Chrome, Mozilla Firefox, or Microsoft Internet Explorer, before being posted on the District's website.

For more information about these expectations or other issues related to web publishing, please contact the System Administrator.

⁵ External links have two problems: (1) schools cannot control the content of those sites but may be held responsible for directing visitors, including students, to them, and (2) widespread use may inadvertently create a public forum or raise First Amendment concerns if and when objectionable links are rejected for publication. However, with vigilant supervision and appropriate controls, these risks can be reduced. If the district wants to use external links, replace this sentence with the following:

External links to non-District websites are limited to sites containing appropriate educational materials and information as exclusively determined by the District.

⁶ Most likely, the external website must be programmed to open a new browser window. If the district believes it is too limiting to require every link to an external website to open a new browser window, remove it from these procedures as well as 6:235-E3, Exhibit - *Online Privacy Statement*.

Protecting Student and Staff Privacy

Personal information concerning students or staff members, including home addresses and telephone numbers, shall not be published on District web pages.

A student's last name, last name initial, and grade-level shall not be published on District web pages. In addition, student records shall not be disclosed.⁷ In special circumstances (e.g., where accolades are warranted), the sponsoring staff member should contact the Building Principal who may seek permission from the student's parents/guardians. Web pages shall not display student pictures with a student identified by his or her name unless written parental permission was first granted (e.g., by executing the form *Using a Photograph or Videotape of a Student*).⁸ Student email addresses, whether a personal or District account, shall not be listed on any District web page.

Submitting Material to Be Published

Everyone submitting material for publication on the District's website shall have signed an *Authorization for Access to the District's Electronic Networks*. Before material is published on the District's website, the author must authorize the District in writing to publish the material, unless the District owns the copyright. All material submitted by a teacher or other staff member for publication on the District's website is deemed "work for hire," and the copyright in those works vests in the District.⁹ All material submitted for the District's website is subject to treatment as a District-sponsored publication.

Different Levels of Web Publication

The following guidelines provide specific information regarding web publishing at different levels within the District. At each level, a staff member is identified as being responsible for web publishing at that level. This individual's web publishing efforts are supervised by the District webmaster.

District-Level

The District webmaster conducts the District-level web publishing efforts and supervises other levels of web publishing. District-level publishing includes the District's homepage as well as any publishing activities representing the District as a whole, e.g., information about Board meetings, Board policy, and schedules. The District homepage shall have a link to an Online Privacy Statement.¹⁰

Department-Level

District departments (e.g., Transportation, Personnel, or Curriculum) may publish their own web pages as part of the District's website. The department supervisor or director is ultimately responsible for his or her respective department's web pages, but may appoint a staff member as the department's webmaster to fulfill the maintenance, reviewing, and uploading tasks. The department supervisor or director shall keep the District webmaster informed of who is the department webmaster.

⁷ The requirements of the Family Educational Rights and Privacy Act as well as the Illinois School Student Records Act severely limit website publication of student information. Even obtaining parental consent is problematic because, under 105 ILCS 10/6(a)(8), the consent must identify the recipients of the student records—impossible with web publishing.

⁸ See 7:340-AP1, E2, Exhibit - *Using a Photograph or Videotape of a Student*.

⁹ See 5:170-AP1, Administrative Procedure - *Copyright Compliance*.

¹⁰ See 6:235-E3, Exhibit - *Online Privacy Statement*.

The web-published material should coincide with that department's printed material. The District webmaster should be consulted before publishing potentially sensitive material, e.g., school comparisons or student data.

The department front pages should maintain the look and feel of the District homepage – the connection to the District should be obvious. Links to the main website's "home" must be included at the bottom of main pages, and the District's logo must be included at the top of main front pages of each department.

School-Level

The Building Principal is ultimately responsible for his or her respective school's webpages, but may appoint a staff member as the school webmaster to fulfill the maintenance, reviewing, and uploading tasks. The Building Principal shall keep the District webmaster informed of who is the school webmaster. All official material originating from the school will be consistent with the District style and content guidelines. The Building Principal or school webmaster may develop guidelines for the various sections of and contributors to the school's web pages.

Staff-Level

Any teacher or other staff member wanting to create web pages for use in class activities or to provide a resource for other teachers or staff members shall notify the school webmaster of his or her desired publishing activities.

Student-Level¹¹

A student wanting to create web pages on the District's website as part of a class or school-sponsored activity should request a teacher or staff member to sponsor the student's publishing efforts. The sponsoring teacher or staff member shall notify the school webmaster of the desired publishing activities. The student's web page must include an introduction written by the sponsor that describes the intent of the student's web page and contains the sponsor's District email address. Student web pages will be removed at the end of the school year unless special arrangements are made.

Personal web pages are not allowed on the School District's web server. Likewise, student web pages may not contain commercial or advertising links, including links to games and advertisements for games.

¹¹ Student free speech rights on the Internet are not absolute. For class or school-sponsored activities, school officials may impose some limits on what appears in school-sponsored student publications. Hazelwood v. Kuhlmeier, 484 U.S. 260 (1988).

For off-campus student website activities, school officials may discipline students for conduct that has a material and substantial interference with the school's work. Legal counsel should be consulted to evaluate the extent to which the website interrupts the educational process. This is because the evaluation requires a close and thorough examination of the circumstances. The Seventh Circuit Court of Appeals upheld a student's expulsion for an article in an underground newspaper titled, "So You Want to be a Hacker." The article's instructions about hacking into the school's computers created a clear interference with the school's operations. Boucher v. School Board of the School District of Greenfield, 134 F.3d 821 (7th Cir. 1998). See also J.S. ex rel. H.S. v. Bethlehem Area School Dist., 807 A.2d 847 (Pa., 2002), (finding student's off-campus website significantly and adversely impacted the delivery of instruction because it contained derogatory and offensive material directed toward a teacher and the principal) and Wisniewski v. Board of Education of the Weedsport Central School District, 494 F.3d 34 (2nd Cir. 2007), cert. denied 128 S.Ct. 1741 (2008), (holding a student's transmission of an icon of a pistol with blood splattering and the words "Kill Mr. VanDer Molen (English teacher) crossed the boundary of protected speech and constituted student conduct that posed a reasonably foreseeable risk that the icon would come to the attention of school authorities and that it would materially and substantially disrupt the work and discipline of the school).

CROSS REF.: 6:235 (Access to Electronic Networks)

ADMIN. PROC.: 5:170-AP1 (Administrative Procedure - Copyright Compliance), 6:235-AP1 (Administrative Procedure - Acceptable Use of the District's Electronic Networks), 6:235-AP1, E1 (Exhibit - Student Authorization for Access to the District's Electronic Networks), 6:235-AP1, E2 (Exhibit - Staff Authorization for Access to the District's Electronic Networks), 6:235-E3 (Exhibit - Online Privacy Statement)

Instruction

Exhibit - Online Privacy Statement

Online Privacy Statement

The School District respects the privacy of all website visitors to the extent permitted by law. This Online Privacy Statement is intended to inform you of the ways in which this website collects information, the uses to which that information will be put, and the ways in which we will protect any information you choose to provide us.

There are four types of information that this site may collect during your visit: network traffic logs, website visit logs, cookies, and information voluntarily provided by you.

Network Traffic Logs

In the course of ensuring network security and consistent service for all users, the District employs software programs to do such things as monitor network traffic, identify unauthorized access or access to nonpublic information, detect computer viruses and other software that might damage District computers or the network, and monitor and tune the performance of the District network. In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets, and other information. Information from these activities is used only for the purpose of maintaining the security and performance of the District's networks and computer systems. Personally identifiable information from these activities is not released to external parties without your consent unless required by law.

Website Visit Logs

District websites routinely collect and store information from online visitors to help manage those sites and improve service. This information includes the pages visited on the site, the date and time of the visit, the Internet address (URL or IP address) of the referring site (often called "referrers"), the domain name and IP address from which the access occurred, the version of browser used, the capabilities of the browser, and search terms used on our search engines. This site makes no attempt to identify individual visitors from this information; any personally identifiable information is not released to external parties without your consent unless required by law.

Cookies

Cookies are pieces of information stored by your web browser on behalf of a website and returned to the website on request. This site may use cookies for two purposes: to carry data about your current session at the site from one webpage to the next and to identify you to the site between visits. If you prefer not to receive cookies, you may turn them off in your browser, or may set your browser to ask you before accepting a new cookie. Some pages may not function properly if the cookies are turned off. Unless otherwise notified on this site, we will not store data, other than for these two purposes, in cookies. Cookies remain on your computer, and accordingly we neither store cookies on our computers nor forward them to any external parties. We do not use cookies to track your movement among different websites and do not exchange cookies with other entities.

Information Voluntarily Provided by You

In the course of using this website, you may choose to provide us with information to help us serve your needs. For example, you may send us an email to request information, an application or other material, and you may sign up for a mailing list. Any personally identifiable information you send us will be used only for the purpose indicated. Requests for information will be directed to the appropriate staff and may be recorded to help us update our site. We will not sell, exchange, or otherwise distribute your personally identifiable information without your consent, except to the extent required by law. We do not retain the information longer than necessary for normal operations.

Each webpage requesting information discloses the purpose of that information. If you do not wish to have the information used in that manner, you are not required to provide it. Please contact the person listed on the specific page, or listed below, with questions or concerns on the use of personally identifiable information.

While no system can provide guaranteed security, we take reasonable efforts to keep information you provide to us secure, including encryption technology (if any), and physical security at the location of the server where the information is stored.

Communication Preferences

You can stop the delivery of informational emails from the District by following the specific instructions in the email you receive. Depending on the respective service, you may also have the option of proactively making choices about the receipt of email, telephone calls, and postal mail for particular District information and activities.

Links to Non-District Websites

District websites provide links to other websites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by this Online Privacy Statement; they may have their own policies or none at all. Often you can tell you are leaving a District website by noting the URL of the destination site. These links to external websites open a new browser window as well.

Please email your questions or concerns to the System Administrator [*insert contact information*].