

Instruction

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's electronic networks have no expectation of privacy in any material that is stored on, transmitted, or received via the District's electronic networks. 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.

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), 7:315 (Restrictions on Publications; High Schools), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

ADMIN. PROC.: 6:235-AP1 (Acceptable Use of the District’s Electronic Networks), 6:235-AP1, E1 (Student Authorization for Access to the District’s Electronic Networks), 6:235-AP1, E2 (Staff Authorization for Access to the District’s Electronic Networks)

ADOPTED: May 14, 2007; REVISED: Oct 25, 2007; July 18, 2012; October 19, 2016; May 20, 2020; Aug. 18, 2021

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

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-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;
3. District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

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 may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. 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 electronic networks. Some examples of unacceptable uses are:

- a. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;
- b. Using the electronic networks to engage in conduct prohibited by board policy;
- c. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;
- d. Unauthorized use of personal removable media devices (such as flash or thumb drives);
- e. Downloading of copyrighted material for other than personal use;
- f. Using the electronic networks for private financial or commercial gain;
- g. Wastefully using resources, such as file space;

- h. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;
- i. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;
- j. Using another user's account or password;
- k. Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;
- l. Posting or sending material authored or created by another without his/her consent;
- m. Posting or sending anonymous messages;
- n. Creating or forwarding chain letters, spam, or other unsolicited messages;
- o. Using the electronic networks for commercial or private advertising;
- p. Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;
- q. Misrepresenting the user's identity or the identity of others; and
- r. Using the electronic networks while access privileges are suspended or revoked.

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

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

No Warranties - The 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 - By using the District's electronic networks, the user agrees to indemnify the 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 or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as 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 malware, such as viruses and spyware.

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

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

- a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
- b. Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of *public domain* documents must be provided.
- c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
- d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The 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 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 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 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, such as spam or potential phishing emails, 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 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 supported if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using 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.: 20 U.S.C. §7131, Elementary and Secondary Education Act.
47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
720 ILCS 135/, Harassing and Obscene Communications Act.

ADOPTED: July, 2005; REVISED: May, 2006; October 19, 2016; Aug. 18, 2021

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 its 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 electronic networks 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

Revised: 12-20-2017; Aug. 18, 2021

Instruction

Exhibit - Staff 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. 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 electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. Administrative Procedure 6:235-AP1, *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. 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. 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. Due to limited storage space and varying network speeds, file sizes may be limited by the District webmaster.
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.

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 abusive, obscene, profane, sexual threatening, harassing, knowingly false or 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. Every effort should be made to ensure that all links are operational. Every link to an external website must open a new browser window.
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 Edge, 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.

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. 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*). 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. 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.

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.

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 homepage 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-Level

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.

CROSS REF.: 6:235 (Access to Electronic Networks), 7:315 (Restrictions on Publications; High Schools)

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

ADOPTED: July, 2005; REVISED: July 16, 2014; Oct. 19, 2016; Aug. 18, 2021

Instruction

Exhibit - Online Privacy Statement

Post the content of this exhibit on the District's website to inform website visitors of the information the District collects through its website and how it uses that information. Modify this exhibit as needed to reflect the District's practices.

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 email 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 you 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. Links to external websites open a new browser window.

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

ADOPT: 2005; REVISED: September 18, 2013; Sept. 21, 2016; Aug. 18, 2021

Instruction

Exhibit - Keeping Yourself and Your Kids Safe On Social Networks

For students:

- Put everything behind password protected walls, where only friends can see.
- Protect your password and make sure you really know who someone is before you allow them onto your friend's list.
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators.
- Don't post anything your parents, principal or a predator couldn't see.
- What you post online stays online - forever!!!! So ThinkB4Uclick!
- Don't do or say anything online you wouldn't say offline.
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pics online.
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!
- And, unless you're prepared to attach your blog to your college/job/internship/scholarship or sports team application...don't post it publicly!
- Stop, Block and Tell! (don't respond to any cyberbullying message, block the person sending it to you and tell a trusted adult).
- R-E-S-P-E-C-T! (use good netiquette and respect the feelings and bandwidth of others).
- Keep personal information private (the more information someone has about you, the more easily they can bully you).
- Google yourself! (conduct frequent searches for your own personal information online and set alerts ... to spot cyberbullying early).
- Take 5! (walk away from the computer for 5 minutes when something upsets you, so you don't do something you will later regret).

And for parents:

- Talk to your kids - ask questions (and then confirm to make sure they are telling you the truth!)
- Ask to see their profile page (for the first time)...tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe...and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic...there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you had they known, when you were fifteen.
- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer...and reading their blog. One is between them and the paper it's written on; the other between them and 700 million people online!
- Don't believe everything you read online - especially if your teen posts it on her blog!

For more information, visit www.WiredSafety.org.

Reprinted with permission from "Parry Aftab's Guide to Keeping Your Kids Safe Online, MySpace, Facebook and Xanga, Oh! My!" Parry Aftab, Esq., www.aftab.com.

Resources for Students and Parents

Resources for students:

Federal Trade Commission - www.consumer.ftc.gov/features/kids-online.

Connect Safely - Tips for Safe Social Networking for Teens www.connectsafely.org/social-web-tips-for-teens/ (2017).

NetSmartz - www.missingkids.org/netsmartz/resources.

Resources for parents:

National Crime Prevention Council – Social Networking Safety, Tips for Parents <http://archive.npc.org/topics/internet-safety/social-networking-safety.html>. Great comprehensive article for parents.

Connect Safely - Social Web Tips for Parents <https://www.connectsafely.org/social-web-tips-for-parents/> (2017).

National Cyber Security Alliance - Raising Digital Citizens <https://staysafeonline.org/get-involved/at-home/raising-digital-citizens/>.

Illinois Attorney General – Stay Connected Stay Informed <https://illinoisattorneygeneral.gov/cyberbullying/>.

Federal Trade Commission – COPPA: A few tips to keep your child safe online <https://www.consumer.ftc.gov/blog/2019/04/coppa-few-tips-keep-your-child-safe-online> (2019).

DHS U.S. CERT - Socializing Securely: Using Social Networking Services www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf.

DHS U.S Computer Emergency Readiness Team - Staying Safe on Social Network Sites <https://us-cert.cisa.gov/ncas/tips/ST06-003> (2019).

Safe Chat Room and Social Sites for Kids <https://www.common sense media.org/lists/safe-chat-rooms-and-social-sites-for-kids>.

ADOPTED: October, 2006; REVISED: August 17, 2001; October 19, 2016; Aug. 18, 2021