Instruction

Internet Safety Policy

The Board of Education of Township High School District 214 ("Board") has adopted the following policy in accordance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act (P.L. 106-554).

This policy provides for the monitoring of the online activities of minors, and addresses the following areas:

- use of technology measures to restrict minors' access to materials harmful to minors and/or inappropriate;
- the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- unauthorized access, including so-called "hacking," and other unlawful activities by minors online; and
- unauthorized disclosure, use and dissemination of personal information regarding minors.

Section I. - Curriculum

By being connected to the Internet, students and staff have potential access to electronic mail communication; to information via the World-Wide Web; and to various research sources including certain university library catalogs, the Library of Congress, and other research databases. Access to the Internet and Township High School District 214's (the "District's") network is a privilege and is not a public forum for general use. Employees and students may load District-assigned student work onto the District's network. However, employees and students shall not load onto the District's network or Internet any unlawful, inappropriate, or copyrighted works that are not in accordance with fair use guidelines. Employees will not use personal social networking sites to communicate/interact with students. The Board disclaims any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the Internet. Further, the Board disclaims responsibility for any information that may be lost, damaged or altered or unavailable when using the District's network. Employees and students shall be solely responsible for any unauthorized charges or fees resulting from their access to the Internet.

Section II. - Use of Technology Protection Measures

It is the policy of the Board of Education, through the use of internet filtering or blocking devices, to comply with the Children's Internet Protection Act. Such filtering or blocking device shall be used on all District computers with internet access and during all use of such computers, except as specifically provided below.

It shall be the responsibility of the administration of the District to assess those filtering or blocking devices available for use and to determine the filtering device most effective and appropriate for the School District's needs.

The Superintendent or Superintendent's designee may, on a case by case basis, authorize the disabling of filtering or blocking devices to permit adults to engage in bona fide research or for other lawful purposes. Disabling requests will not be granted if the Superintendent determines that the potential harm or disruption incident to the request outweighs its educational or professional benefit.

All online activities of students and minors may be monitored by those school officials with direct supervisory responsibility for those activities. In addition, school officials may monitor students' and

minors' online activities on District computers when not under the direct supervision of school staff. Such monitoring may consist of (i) direct observation of online activities; (ii) review of internet logs and other use records; (iii) generation of internet activity reports or summaries; or (iv) any other method that the Superintendent determines provides for the effective review and monitoring of online activities.

Section III - Access to Inappropriate Materials on the Internet and the World Wide Web

It is the policy of the Board, to the extent permitted by law, to limit access by minors to inappropriate matter on the Internet and the World Wide Web. This policy shall be accomplished through (i) the use of the filtering or blocking devices described in Section II, (ii) enforcement of the District's responsible use of technology policy, and (iii) providing education and counseling to minors and students who use the District's computer system regarding the proper use of internet resources.

Section IV. - Electronic Mail, Chat Rooms, Social Networking Websites, and Other Forms of Electronic Communications

It is the policy of the Board to ensure the safety and security of minors when using electronic mail, chat rooms, social networking websites, and other forms of direct electronic communications. For this purpose, school officials may regularly review minors' online and internal communications on the District's computer network to assure the safety of students and minors. School officials may further communicate to minors, through the District's student handbook, its acceptable use policy, or other means, information regarding the safety risks raised by online communications and appropriate practices to protect against these risks.

Student use of social media and technologies for school purposes or in a manner that is considered to have a nexus to the District or the school are subject to disciplinary action in accordance with existing board policies, the student discipline code and the responsible use policy.

Section V. – Cyberbullying, Hacking. Unauthorized Access, and Unlawful Activities of Minors Online

Minors who use the District's computer network shall be permitted to do so only for authorized purposes and for lawful activities. This policy applies to (i) access to the District's own computer network, and (ii) access by minors to other networks and computers when using the District's network. School officials may communicate these restrictions to minors through the District's student handbook, responsible use policy, or other means. Unlawful or unauthorized online activities are identified as forms of misconduct subject to discipline under the School District's student discipline code.

Section VI. - Unauthorized Disclosure, Use and Dissemination of Personal Information

It is the policy of the District, consistent with State and Federal student records laws, to protect students and minors against the unauthorized disclosure, use and dissemination of personal information through the District's computer system. Users of the District's computer system shall be prohibited from disclosing personally identifiable information regarding students or minors outside the District's computer system, except in specifically authorized instances. This prohibition shall apply to all electronic communications either directed to non-District computers or accessible to non-District users, such as web page postings and other internet-accessible files.

Section VII. - Definitions

Terms used in this policy shall have the meanings set forth in the Children's Internet Protection Act.

The use of the term "Internet" or "network" in this policy refers to all information accessed through the District's network from the various sources as identified above and any and all information accessed using the District's means of access.

Choice of Law

The laws of the State of Illinois shall apply to any use of the District's websites and any use governed by 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 (l).
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.
720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications)

ADOPTED: April 3, 2014

Instruction

Administrative Procedure - Responsible 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 appropriate legal action.**

Terms and Conditions

Responsible 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. *(see 6:235 – AP2 Responsible Use Procedures)* 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) cyber-bullying awareness and response.

District-Issued Technology (Including One-To-One Programs) - The District may issue technology to users, including students and employees, for educational or extra-curricular purposes and/or District business, including through a one-to-one program. Use of District-issued technology is governed by this Internet Safety Policy, including the Responsible and Unacceptable Use provisions, regardless of when, where, or for what purpose the use occurs. This includes use that occurs outside of normal school hours (for students), before or after work times (for employees), for personal purposes, and/or off District property or away from related events or activities.

The user is responsible for reasonable care of District-issued technology at all times during which the technology is issued to the user, regardless of whether the technology is on school property or at related events or activities. This includes the requirement that the user not allow others to use the technology without authorization from an administrator. The procedures implemented by the Superintendent or designee for this Internet Safety Policy may contain further guidelines regarding responsible use, as may handbooks and other guidelines issued at the school level. Costs associated with repair or replacement of technology damaged as a result of a user's failure to exercise reasonable care shall be the responsibility of the user, including any fees for insurance premiums and deductibles, regardless of whether the damage is caused by the user or a third party. Users may be required to obtain and/or pay for insurance for District-issued technology in order to be issued such technology by the District.

Students may only use or access District-issued technology outside of school with parental or guardian supervision. The District is not responsible for unacceptable use of District-issued technology by students at any time, including outside of school, although students may face consequences for such misuse under this and other District policies.

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 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 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. Knowingly or recklessly causing a security breach or disruption of service to an individual or system;
m. Any use that violates any Board policy, including policies addressing bullying, harassment, and hazing, and student and employee discipline policies or codes of conduct;
n. Accessing or participating in any games without the express authorization of a supervisor (for employees) or teacher or administrator (for students and other users), or using the District's electronic resources for more than incidental personal use;
o. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
p. Using the network while access privileges are suspended or revoked.

A user should notify the District's Complaint Manager or Nondiscrimination Coordinator immediately under Board Policy 2:260 *Uniform Grievance Procedures* upon receipt of a communication through the District's electronic resources that the user believes is inappropriate or that makes the user feel threatened or uncomfortable.

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

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.

Information Assets - The users of Information Assets will be consistent with standard security practices. This Includes information, networks, and systems that are owned by District 214, information that District 214 is obligated to keep secure by applicable law or by contract and information exempt from disclosure under public records laws. District 214 Information Assets are written, spoken, electronic, printed, magnetic, optical and other mediums. The use of Information Assets will be operated effectively and will be used in compliance with applicable laws.

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 the Webmaster 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 Electronic Mail - The District's electronic mail 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 electronic mail account is strictly prohibited.
b. Each person should use the same degree of care in drafting an electronic mail 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 name is a registered domain 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 electronic mail 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 electronic mail system constitutes consent to these regulations.

The Superintendent or designee may authorize students to use personal technology for educational and/or extracurricular purposes, including for classroom instruction and extracurricular activities, through a Bring Your Own Device (BYOD) program. iPads are the primary device approved by the School District. Each student must return a Personal iPad Agreement, created by the Superintendent or designee, signed by both the student and the student's parent/guardian, before participating in a BYOD program.

A BYOD program authorized by the Superintendent or designee may include use of personal social media websites of students. Students must meet qualifications for holding an account from the social media website and must be authorized by a parent/guardian to utilize a particular social media website before using that website for educational purposes.

Students may use BYOD technology other than iPads on District property or at related events and activities only at times, at places, and for purposes expressly permitted by the BYOD program or school personnel. When a student uses personal technology at a time, at a place, in a manner, or for a purpose authorized by the BYOD program, the student's use of the personal technology is governed by this Internet Safety Policy, all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources, and Board Policy 7:190 *Student Discipline*. At all other times while on District property or at related events and activities, students must comply with requirements for the use of personal technology on District property or at related events and activities, even if the personal technology device used is one that is authorized for use in a BYOD program.

Internet Safety

Internet access is limited to only those "responsible 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 procedures implemented by the Superintendent or designee for this Internet Safety Policy shall allow users to make requests, including anonymous requests, to disable the filter for bona fide research or other lawful purposes.

The District and its employees shall take steps, to the extent practical, to educate, supervise, and monitor students' uses of electronic resources as required by CIPA and other federal and state laws.

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, 20 U.S.C §6751 et seq.
720 ILCS 135/0.01.

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system
Incident Referral accessible via staff login at http://tienet.d214.org
What Parents/Guardians Should Know
District 214 Student Handbook

Approved by Superintendent's Leadership Team: May 6, 2014

Instruction

Exhibit - Letter to Parents/Guardians Regarding Student Use of the District's Electronic Networks

On District letterhead

Date

Dear Parents/Guardians:

We have the ability to enhance your child's education through the use of electronic networks, including the Internet. The Internet offers vast, diverse, and unique resources. The District's goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Your authorization is needed before your child may use this resource.

The Internet electronically connects thousands of computers throughout the world and millions of individual subscribers. Students and teachers may have access to:

- Limited electronic mail communications with people all over the world,
- Information from government sources, research institutions, and other sources,
- Discussion groups, and
- Many libraries, including the catalog to the Library of Congress, and the Educational Resources Information Clearinghouses (ERIC).

With this educational opportunity also comes responsibility. You and your child should read the enclosed *Authorization for Electronic Network Access* and discuss it together. 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.

The District takes precautions to prevent access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. On an unregulated network, however, 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 or ward should follow. To that end, the School District supports and respects each family's right to decide whether or not to authorize Internet access.

Please read and discuss the *Authorization for Electronic Network Access* with your child. If you agree to allow your child to have an Internet account, sign the *Authorization* form and return it to your school.

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system
Incident Referral accessible via staff login at http://tienet.d214.org

Approved by Superintendent's Council: November 23, 2010

Instruction

Exhibit - Authorization for Electronic Network Access

Each staff member must sign this Authorization as a condition for using the District's Electronic Network connection. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted unsupervised access. Please read this document carefully before signing.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Authorization for Electronic Network Access* 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.

Terms and Conditions

Responsible 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 a legitimate business use.

Privileges - The 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 will make all decisions regarding whether or not a user has violated the terms of access privileges 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 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. Knowingly or recklessly causing a security breach or disruption of service to an individual or system;
m. Any use that violates any Board policy, including policies addressing bullying, harassment, and hazing, and student and employee discipline policies or codes of conduct;

n. Accessing or participating in any games without the express authorization of a supervisor (for employees) or teacher or administrator (for students and other users), or using the District's electronic resources for more than incidental personal use;
o. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
p. Using the network while access privileges are suspended or revoked.

A user should notify the District's Complaint Manager or Nondiscrimination Coordinator immediately under Board Policy 2:260 *Uniform Grievance Procedures* upon receipt of a communication through the District's electronic resources that the user believes is inappropriate or that makes the user feel threatened or uncomfortable.

Network Etiquette - You are 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 your messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal the personal information, including the addresses or telephone numbers, of students or colleagues.
d. Recognize that electronic mail (email) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be private property.
g.

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 users 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 this *Authorization*.

Security - Network security is a high priority. If you can identify a security problem on the Internet, you 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 the Webmaster 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 Electronic Mail - The District's electronic mail 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 electronic mail account is strictly prohibited.
b. Each person should use the same degree of care in drafting an electronic mail 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 name is a registered domain 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 electronic mail 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 electronic mail system constitutes consent to these regulations.

The Superintendent or designee may authorize students to use personal technology for educational and/or extracurricular purposes, including for classroom instruction and extracurricular activities, through a Bring Your Own Device (BYOD) program. iPads are the primary device approved by the School District. Each student must return a Personal iPad Agreement, created by the Superintendent or designee, signed by both the student and the student's parent/guardian, before participating in a BYOD program.

A BYOD program authorized by the Superintendent or designee may include use of personal social media websites of students. Students must meet qualifications for holding an account from the social media website and must be authorized by a parent/guardian to utilize a particular social media website before using that website for educational purposes.

Students may use BYOD technology other than iPads on District property or at related events and activities only at times, at places, and for purposes expressly permitted by the BYOD program or school personnel. When a student uses personal technology at a time, at a place, in a manner, or for a purpose authorized by the BYOD program, the student's use of the personal technology is governed by this Internet Safety Policy, all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources, and Board Policy 7:190 *Student Discipline*. At all other times while on District property or at related events and activities, students must comply with requirements for the use of personal technology on District property or at related events and activities, even if the personal technology device used is one that is authorized for use in a BYOD program.

Internet Safety

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

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 this *Authorization*.

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 procedures implemented by the Superintendent or designee for this Internet Safety Policy shall allow users to make requests, including anonymous requests, to disable the filter for bona fide research or other lawful purposes.

The District and its employees shall take steps, to the extent practical, to educate, supervise, and monitor students' uses of electronic resources as required by CIPA and other federal and state laws.

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, 20 U.S.C §6751 et seq.
720 ILCS 135/0.01.

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system
Incident Referral accessible via staff login at http://tienet.d214.org

Approved by Superintendent's Council: May 6, 2014

Instruction

Administrative Procedure – Authorization for Electronic Network Access Form

Authorization for Electronic Network Access Form

Submit to Building Principal.

Students and their parents/guardians need to sign this *Authorization for Electronic Network Access* each year while the student is enrolled in the School District. Staff members need to sign this *Authorization for Electronic Network Access* each year while employed by the School District.

Please check the appropriate box:

- ☐ Staff member
- ☐ Parent/Guardian of student
- ☐ Student *****

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including 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 appropriate 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 Internet.

_____

User Name (*please print*)

_____ _____

User Signature Date

As part of the online registration process, a parent/guardian must read and agree to the following:

I have read this *Authorization for Electronic Network Access*. 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 terms of this *Authorization* with my child. I hereby request that my child be allowed access to the District's Internet.

Approved by Superintendent's Council: May 6, 2014

Instruction

Administrative Procedure - Responsible Use Procedures

Purpose

It is the policy of the Board of Education of Township High School District ~~No.~~ 214 to encourage technology use which facilitates communication and the exchange of ideas and information in pursuit of the District's curricular, instructional, technological, and research goals. The District also supports the use of the District's email system as a tool for the efficient and effective communication of the District's resources and affairs.

The Opportunities and Risks of Technology Use

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting, or that may be harmful or disruptive. Because information on networks is transitory and diverse, the District cannot completely predict or control what users may or may not locate. The Board of Education believes that the educational value of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of the District.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, 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 or suitability of any information that is retrieved through technology;

3. breaches of confidentiality; or

4. defamatory material.

Privileges and Responsibilities

The District's email communication system is part of the curriculum and is not a public forum for general use. Users may access email only for educational purposes. The actions of users accessing email through the District reflect on the District; therefore, users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Users are responsible for their behavior and communications using the District's email system.

Users of the District's email system will:

A. Use or access District email system only for educational or administrative purposes.

B. Comply with copyright laws and software licensing agreements.

C. Understand that email and network files are not private. Network administrators and other designated school officials have access to all email messages and may review files and communications to maintain system integrity and monitor responsible use.

D. Respect the privacy rights of others and maintain confidentiality of all personnel and student records transmitted by means of the District email system.

E. Be responsible at all times for the proper use of email, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.

F. Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.

G. Abide by the policies and procedures of networks and systems linked by technology.

H. Respect the rights of others to use the email system.

Users of the District's email system will not:

A. Access, submit, post, publish, display or create any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially/religiously offensive, harassing, illegal or other material unsuitable in the educational setting or unrelated to the District's educational program.

B. Violation of law. Transmission of any material in violation of any international, U.S., or state law is prohibited. This includes, but is not limited to: copyrighted material, threatening, harassing or obscene material, or material protected by trade secret. Any attempt to break the law while using a District 214 Internet account or while connected to the Internet through a District 214 IP (Internet Protocol) address may result in litigation against the offender by the proper authorities. If such an event should occur, District 214 will fully comply with the authorities to provide any information necessary for the litigation process.

C. Interfere with or disrupt email use by other users; create and/or propagate unsolicited advertising, political lobbying, chain letters, pyramid schemes, computer worms, viruses, or other acts of vandalism. Vandalism includes any attempt to harm or destroy data of another user, the Internet, the District's Network or any other network. This includes, but is not limited to, uploading, downloading, creation or knowing transmission of computer viruses. If a user is uncertain whether his or her conduct is permissible, he or she should contact the Systems Administrator.

D. Use another Users' account or password to access the email system.

E. Distribute User passwords, copyrighted or plagiarized material or material protected as a trade secret.

F. Misrepresent themselves or others.

G. Trespass in others' email account, folders, work, or files, or gain unauthorized access to email resources or entities.

H. Post personal contact or other private information about oneself, a student or staff member, or otherwise invade the privacy of individuals or violating the Illinois School Student Record Act or Federal Right to Privacy Education Act.

I. Use the District email system for non-school purposes, personal financial gain, or for any illegal purpose or activity.

J. Forge or anonymously transmit email or other electronic materials.

K. Represent personal views as those of the District or those that could be interpreted as such.

L. Use the District email system while access privileges are suspended or revoked.

Disciplinary Actions

Violations of this policy, or any administrative regulations and/or guidelines governing the use of the District's email system, may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion (in the case of students), suspension with or without pay or termination (in the case of staff), or other appropriate legal or disciplinary action. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

Any expenses incurred by virtue of violation of this policy, including telephone long distance, per-minute or line charges, are the sole responsibility of the user.

No Expectation of Privacy

Users of the District's electronic resources have no expectation of privacy with respect to use of the District's electronic resources, including access of the District's Internet or Wi-Fi using personal technology, or with respect to any material created, transmitted, accessed, or stored via District electronic resources. This includes material created, transmitted, accessed, or stored for personal use, including incidental personal use, on or through the District's electronic resources. The District reserves the right to monitor users' activities on District electronic resources at any time for any reason without prior notification; to access, review, copy, store, and/or delete any electronic information accessed or stored therein; and to disclose such information to others as it deems necessary and/or as required by law. Users should be aware that information may remain on the District's electronic resources even after it has been deleted by the user. This section of this policy may only be altered through amendment of this policy, and may not be altered or diminished by the verbal or written assurances of any employee or representative of the District.

Staff Responsibilities to Students

Staff members utilizing the District's email system for instructional purposes with students are responsible for supervising such use. In selecting technology for teaching purposes, staff shall comply with the selection criteria for instructional materials and library-media center materials. Staff members are expected to be familiar with the District's policies and any administrative rules concerning student email use and the enforcement of them. When, in the course of their duties, staff members become aware of student or other staff member violations, they are expected to stop the activity and/or inform the building Systems Administrator and the Building Level Administrator.

Application of this Policy

For the purposes of this policy, District "staff" includes all District employees, volunteers and Board members.

Additional Rules/Actions

The Superintendent may establish regulations and guidelines, and shall take appropriate action to implement this Policy.

Related Documents:
5:130 Administrative Procedures - Email Retention
Global Compliance Module

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 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 Web page 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

Personal information is information about an individual by which that individual may readily be identified. The District does not collect personal information about users unless voluntarily provided by users. 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 Web page 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.

Exchange, Release, and Sale of Information Regarding Users

The District does not exchange, release, or sell any anonymous or personal information regarding users to third parties, other than those hired to manage the District's websites for the District, except to the extent required by law or unless explicitly identified at the time voluntary information is solicited from a user.

Web Links to Non-District Websites

District Websites provide links to other World Wide 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: **webmaster@d214.org**.

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system

Approved by Superintendent's Council: May 6, 2014

Instruction

Exhibit - Keeping Yourself and Your Kids Safe On Social Networks

There are several ways to safeguard children when accessing Social Networks. The most effective is to educate them from an early age about the risks they may encounter when online. This includes the risks, how to spot them, and what action to take. There are a number of online age-appropriate educational resources available to parents/guardians and teachers, and children themselves, covering every aspect of online safety for children. The information is posted on the District's website at http://www.d214.org/internetsafety/. Remember that these factors will change as children grow up and should be reconsidered regularly.

Students and parents should follow these tips to stay safe online.

The quick tips for teens:

* 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 cyber-bullies 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 pictures 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 cyber-bullying 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 cyber-bullying 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; www.stopcyberbulling.org; www.commonsensemedia.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.

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system

Instruction

Exhibit - Children's Online Privacy Protection Act

On District letterhead:

RE: Children's Online Privacy Protection Act

Dear Parent(s)/Guardian(s):

This letter is being sent as part of the District's continuing effort to educate parents and students about privacy protection and Internet use.

The Children's Online Privacy Protection Act gives parents control over what information websites can collect from their children. Many companies, however, are not providing information about what data a mobile app collects, who will have access to that data, and how it will be used. Allowing your child access to games and other seemingly harmless applications on a Smartphone or computer risks his or her exposure to intrusive marketing and access to personal information.

A recent survey of apps for children by the Federal Trade Commission found that 10 percent of apps with social networking services did not disclose their presence; 17 percent of the apps allowed children to make purchases without parent/guardian consent; and 58 percent contained constant advertising, while less than 20 percent disclosed that advertising would appear.

The following suggestions may help keep children from being bombarded by unwanted advertising, from making unwanted purchases and from disclosing personal information and location:

- Be choosy about the applications that you let your child use. Try the app yourself to check for advertising messages and/or social networking and purchase options before allowing your child access.
- Select activities that do not require access to the Internet or an application, such as looking at family pictures or listening to preselected music, screened and approved by you.
- Make certain that the ability to make purchases is password protected.
- Set up family rules and consequences explaining that all purchases made via a Smartphone or computer must have parent/guardian consent.
- Caution children about the use of social networking and other sites and/or apps that can pinpoint locations.
- Monitor computer and Smartphone use whenever and wherever possible.

For more information on the Children's Online Privacy Protection Act, please see the following links:

www.ftc.gov/opa/2012/12/kidsapp.shtm
www.ftc.gov/opa/reporter/privacy/coppa.shtml

Sincerely,

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 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 Electronic Networks*.
3. 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. All posted material should follow the style and guidelines of the District's Website. Material shall not be published in violation of the District's procedures on *Responsible Use of 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's 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 insure that all links are operational. When an external link is used, a popup will let visitors know they are leaving the District's website. 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 Netscape Navigator and 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.

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 Electronic Network Access*. 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 and Director of Community Engagement and Outreach 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, Human Resources, or Teaching and Learning) 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 "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 Web pages, 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 post all content and resources on the School District's approved Learning Management System.

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)

ADMIN. PROC.: 5:170-AP (Administrative Procedure - Copyright for Publication or Sale of Instructional Materials Developed by Employees), 6:235-AP (Administrative Procedure - Acceptable Use of Electronic Networks), 6:235-E2 (Exhibit - Authorization for Electronic Network Access), 6:235-E3 (Exhibit - Online Privacy Statement)

Related Documents:
Academic Handbook
Link to policy from Online Student Registration system
Incident Referral accessible via staff login at http://tienet.d214.org

Approved by Superintendent's Council: May 6, 2014