User and Management Guide for District 65's Electronic Resources and Internet Access

Evanston/Skokie
School District 65

Last Revised 4-23-13

Kids' Rules for Online Safety

- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
- I will never send a person my picture or anything else without first checking with my parents.
- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do receive a message like that, I will tell my parents right away so that they can contact the service provider.
- I will talk with my parents so that we can set up rules for going online. We will decide the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
- I will not give out my Internet password to anyone (even my best friends) other than my parents.
- I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or jeopardize my family's privacy.
- I will be a good online citizen and not do anything that hurts other people or is against the law.

Information for Parents and Educators

The Illinois Attorney General's Office developed a set of internet safety training modules, including age-appropriate webinars that cover topics facing youth when they use online tools. Learn more at Illinois Attorney General - Safeguarding Children - Internet Safety.

The Illinois Attorney General's Office also developed a cyberbullying web site to address the expansion of bullying, hurtful and humiliating messages through social networking sites and cell phones. Learn more at Illinois Attorney General - Stop Cyberbullying.

Introduction

Evanston/Skokie School District 65 supports student, teacher, and staff access to rich information resources along with the development of appropriate skills to analyze, evaluate, and use such resources.

Telecommunications, electronic information, and networked services open schools, classrooms, and library media centers to a broad array of resources. Access to the Internet enables students, teachers and staff to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging information with people around the world. Many of these resources also are accessible from home.

District 65 recognizes that technologies affect the manner in which information is accessed and communicated and may also alter instruction and student learning. The expectation is that use of District 65's technology and Internet access will be consistent with and support the district's educational objectives.

Use of the district electronic resources is a privilege, not a right. Violations of this Acceptable Use Policy Agreement may result in a loss of access to electronic resources. Inappropriate use by staff, teachers or students may lead to disciplinary and/or legal action, including but not limited to suspension, expulsion, or dismissal from employment from the school district, and referral to the Human Resources Department and/or Superintendent for appropriate action. When appropriate, criminal prosecution by government authorities will be pursued.

Purpose

The purpose of District 65's technologies are to support the work of the district. These resources are used to help effectively manage and communicate information, provide an efficient and effective work environment, enhance the educational experience and increase student achievement, provide equal access to educational resources, and support the goals and initiatives of the district. Inappropriate or unauthorized use may be subject to disciplinary action including suspension, expulsion, or termination for violations of the district's Acceptable Use Policy.

Internet Safety

In compliance with the Children's Internet Protection Act ("CIPA"), the school district uses software to protect against online access to sites containing obscene, pornographic, or harmful or inappropriate sites. In addition, the district blocks commercial and other sites that may not be consistent with the district's education mission. The district maintains and uses software that scans network traffic for objectionable words or concepts, commercial addresses, or unwanted characteristics as determined by the administration and school board and decisions regarding access to sites are conservative. District staff may request that specific sites be unblocked by providing a written request to Instructional Technology.

No software is foolproof. There is still the risk that an Internet user may be exposed to sites containing objectionable information. An account user who incidentally connects to such a site must immediately disconnect from the site and notify a teacher or supervisor. If an account user sees another user accessing inappropriate sites, he or she must immediately notify a teacher or supervisor.

District 65 reserves the right to monitor its network services, equipment, any users' online activities at any time with or without notice, and to access, review, copy, store, or delete any electronic communications or files and disclose them to others as deemed necessary. Monitoring is aimed to prevent abuse of the system or access to inappropriate matter, as well as to help enforce the policies as determined by the school board or other authorized authority.

Teachers, staff, and students should not share private information, pictures, or other communications on social media sites using district equipment or resources. All users of District computers shall take reasonable measures to protect against providing access to confidential student information before such information is loaded onto the network.

Any harassment, intimidation, or threatening communications should be reported to Information Services and the building administration.

Internet access from outside the school is the domain and responsibility of the account user and/or parent or guardian. Content used to harass, embarrass, threaten, or defame others or disrupts school climate or operations may result in disciplinary action.

In accordance with HB4583 that was enacted on 7/19/2010, it is a violation of the law and the district's acceptable use policy for an individual to knowingly disseminate or obtain any material that depicts nudity of other sexual conduct, including self images or image of another minor, by electronic capture or transfer.

Teacher and Staff Responsibilities

The district's teachers and staff are responsible for acquiring the knowledge and skills necessary to incorporate the use of technology into effective practice and to ensure that students learn the technology skills and applications outlined in the district's curriculum.

Instructional and digital resource materials should support and enrich the curriculum. They should also take into account the varied instructional needs, learning styles, abilities, and developmental levels of their students. The district expects faculty to use digital tools and resources throughout the curriculum and guide students in safe use of online and other technologies. Teachers should structure access to internet resources in ways that guide students to previously evaluated resources, monitor their use, and intervene if the resource is not being used appropriately. Teachers and students are expected to use the wide array of secure resources that the district provides for instructional purposes.

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.

Teachers and staff should not communicate with or engage students using social networking sites, either within or outside of school hours. As a matter of practice, teachers should not view students' social networking sites, as this may expose the teacher to unanticipated reporting liabilities.

The district may review and monitor employees' public social networking sites and act upon the information contained in these sites. Complaints regarding the content on (and use of) social networking sites will be investigated and appropriate action taken.

Staff and Teacher Acceptable Use Agreements

Staff and teachers using district-provided Internet access must have an approved account. The use of the district's technology and electronic networks is an integral part of an employee's work responsibilities in District 65. Therefore, all staff and teachers are required to sign an acceptable use agreement each year that indicates that they are aware of, understand, and agree to the requirements and limits of using the districts electronic systems. This agreement shall be included in the employee's personnel folder. Staff and teachers should use the district's guest network when connecting personal equipment and computers.

Instructional Practices and Compliance

From time to time, the district will publish specific and detailed learning standards for students and teachers. These skill standards will serve as guides for classroom instruction and professional development.

Student and Parent Responsibility

Appropriate Internet access is the shared responsibility of the school, the student, and the family. At the time of registration, parents and guardians must acknowledge that they have read and discussed the following with their child. Additionally, parents/ guardians are responsible for their children's out-of-school access to online resources. In the event such out-of-school actions have an adverse effect on the culture or climate at school, the district reserves the right to act in accordance with district policies and rules. These include consequences identified if a student or staff member engages in, hazing, harassment, bullying, or other inappropriate or prohibited behavior.

Students using district-provided digital tools and resources must have an approved account and be supervised by District 65 professional staff. Students using Internet access are responsible for appropriate on-line behavior. They are expected to respect and take care of hardware and software provided for their use. Intentional damage to equipment, software, or the network will result in disciplinary action and charges for repair or replacement to the student's family.

Disciplinary consequences for violations of expected behaviors and use of district and school networked information are outlined in the student handbook available on the web at http://www.district65.net/parentsandstudents/Handbook.

System Management and Privileges

Network services are provided for educationally related communications, research, and other activities. Access to District 65's network services is provided to administrators, staff, teachers, and students who agree to act in a considerate and responsible manner.

a. Administrators, staff and teachers must submit a properly signed Acceptable Use Policy Agreement to the designated administrator or principal. For students, parents sign an acknowledgement form at the time of registration.

b. Each user is assigned a network account that includes a username and private password. The user is responsible for ensuring the security of their username and password.

c. User access to certain types of files (e.g. HTML, graphics, streaming video or audio, etc.) and storage space may be restricted to ensure efficient and secure functioning of the district's network and storage resources, or to protect users' files.

d. Information Services and the Curriculum and Instruction Department staff must approve all instructional software installed on district equipment and the network. Any software approved for installation on the network or district computers must be installed by Information Services staff and becomes the property of District 65. All licenses and original media must be submitted to Information Services at the time of installation.

e. Faculty and staff are discouraged from purchasing software with their own resources. It is strongly recommended that users seek approval from Information Services and the Curriculum and Instruction Department if purchases are to be made. The district will not be responsible for any loss due to failure to obtain appropriate authorizations for purchasing software, nor for loss of software due to system upgrades or configuration changes that may render the software unusable.

f. When using personal computers or other technology, users should connect to the guest user network. The district assumes no responsibility for the maintenance, damage, loss, repair, or replacement of personal equipment connected to or data stored on the district network or storage devices.

g. No equipment may be removed from district premises without prior written authorization. Information Services staff or principals may authorize teachers, or in certain cases students, to check out computers or other equipment for removal from the building premises for education or work purposes.

   All teachers, staff, and students must sign an authorization form with the appropriate approvals prior to removing equipment from district premises. Teachers, staff, and students are responsible for the financial loss or damage of any equipment in their care. The forms must be countersigned by the principal or authorized supervisor and submitted to Information Services.

Privacy and Security

Equipment, network resources, messages, files, programs, and software applications that are stored on, or relayed by, District 65's computers and servers are not private. They may be accessed (just as with school lockers), reviewed, added, deleted, or modified by Information Services staff or administrators at any time without advance notification in order to assure system integrity, provide routine maintenance, monitor responsible use of the system, or for any other purpose approved by the Superintendent.

Moreover, District 65 maintains logs of Internet sites accessed by users, retains email and text messages, monitors bandwidth usage, and limits content storage capacity to ensure a safe working environment, to manage the district's technology resources, and to comply with federal and state regulations. These logs and records may be viewed by Information Services Department staff at any time and without notice.

The Information Services Department staff employs network management softwares that allow remote monitoring, viewing, or software installation or deletion, or intervention with a user's computer. This software is designed for security purposes, diagnosing problems, troubleshooting computer and network problems, and to support help desk activities. Whenever feasible and appropriate, notice will be provided to the user that equipment or files will be or have been accessed. Failure to monitor usage at any time does not void the district's right to monitor usage in the future.

As appropriate, these policies and provisions are subordinate to local, state and federal statutes.

Copyright and Plagiarism

Adherence to federal copyright law, including the Copyright Act of 1976, the Digital Millennium Copyright Act of 1998 and the Family Entertainment and Copyright Act of 2005, is required in both the print and the electronic environments. District 65 guidelines only permit copying specifically allowed by copyright law, fair use guidelines, license agreements, or proprietor's permission.

Teachers and students are responsible for ensuring that online resources, software, or the work of others is not copied or presented without appropriate attribution and permission. Editing work to alter or remove copyright notices is expressly prohibited. Illegally copied or unlicensed software is specifically forbidden for installation and use of the district's hardware and network.

Restrictions

Administrators, staff, teachers, and students may be disciplined for inappropriate use of Internet resources and communications regardless of when or where they occur. In compliance with the Illinois Harassing and Obscene Communications Act, (720 ILCS 135/0.01), the federal Children's Internet Protection Act (CIPA), the Federal Family Educational Rights and Privacy Act (FERPA), the Illinois Internet Safety Education Act (105 ILCS 5/27-13.3) and any and all other applicable local, state and federal statutes and guidelines, the following activities are not permitted using District 65's electronic resources:

- Accessing, uploading, downloading, transmitting, displaying or distributing obscene, abusive, intimidating, threatening, defamatory or sexually explicit material or language or otherwise harassing students or staff.
- Transmitting a student's personal information, work or picture with identifiable information without written parental permission.

- Using another person's passwords; trespassing in another person's folders, work or file.
- Selling or buying anything over the Internet for personal financial gain; or selling or purchasing any illegal substance.
- Using the Internet for advertising or promotion, including conducting for-profit business activities or engaging in solicitation for non-profit groups, religious purposes, lobbying, or votes.
- Damaging computers, computer systems or computer networks; vandalizing, damaging or disabling the property of another person or organization; debilitating or disabling computers, systems or networks through the intentional misuse or overuse of electronic distribution or storage space, the spreading of computer "viruses," or hacking.
- Violating copyright or otherwise using another person's intellectual property without his/her prior approval or proper citation.
- District 65's technology resources, communications systems, email, and web site are not a public forum.

Sanctions

Disciplinary action related to administrator, staff, teacher, and student access to electronic resources may be determined at the central administrative, building, or classroom levels in accordance with existing practice regarding inappropriate language or behavior, as stated in policies and guidelines contained in the student handbook or employee codes of conduct.

Storage Capacity

When user accounts are established, a specific amount of storage space is allocated for files. To ensure that account users remain within the allocated space, users should frequently review their stored files and email, deleting unwanted messages, files, or data that take up excessive storage space. The system administrator may delete or archive files of any type and email or voice messages from Account users' folders.

Users may request, in writing, additional file storage space. The decision from Information Services is final regarding additional storage space.

Files or programs that are determined to be installed without permission or are determined to be personal or not educationally related or justified may be deleted at any time, including program files, pictures, music, video, or files of any other type without prior notice. The district will not be responsible for files that are lost or deleted. Files that are considered valuable should be backed up to a personal hard drive.

Disclaimers

District 65 makes no warranties of any kind, either expressed or implied, for the access being provided.

The district's network, technology, website, and communications systems and tools are not a public forum.

The staff, the school, and the district are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on district resources, or for personal property used to access district resources.

The district is not responsible for the accuracy, nature, or quality of information stored on district resources or gathered through district provided access.

The district is not responsible for personal property used to access district computers or networks or for district-provided Internet access, nor will the district be responsible for unauthorized financial obligations resulting from use of district-provided access.

Even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means for enforcing the provisions of this policy. While the district may employ filters to limit access to certain kinds of sites and to prevent unwanted or inappropriate materials (SPAM) from being accessed or transmitted, there is no guarantee that all objectionable material will be caught or filtered. Limiting this kind of materials is the joint responsibility of all users accessing the district's telecommunications network and computing resources.

Web Publishing Guidelines

District and school web pages or social media sites are educational sites that offer a powerful communication tool to connect with parents, prospective parents, students, and community stakeholders. Each school website includes a staff directory, links to districtwide resources including curriculum resources, childcare, transportation, food and nutrition services, the school calendar, student handbook, bullying protocols, school board policy and other important information. Each site includes links for communications from the school principal and others. As a convenience, the District makes web page(s) available for all teachers and for the local Parent Teacher Association (PTA). These sites offer a convenient way for electronic communications, subject to the discretion and management of the school principal and/or Communications Office.

To ensure the safety of students and their rights to privacy, school web pages and social media sties should be carefully constructed to avoid identifying information about students and to ensure that information is published only for students whose parents have given permission.

Material appropriate for web publishing includes all legally required documents and postings, as well as information about the district, its schools, school board members, policies and procedures, programs and services, teachers, classes, accomplishments, celebrations, announcements, homework assignments, class projects and extracurricular activities and organizations. Personal information, not related to education, is not appropriate for web publishing on the district supported web or social media sites.

Publishing Expectations

The following are minimum expectations for the district and school web pages and social media sites:

- Material published shall contain verifiable information written with correct grammar and spelling, be welcoming, descriptive and include the author’s contact information; anonymous messages are prohibited.
- Material may not be defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or harassing nor invade the privacy of any individual
- Copyrighted materials published to the web must include a statement of copyright and indicate that permission has been secured.
- Publications must identify affiliation with the district, school, and/or department.
- Links to appropriate educational materials and information are allowed. Links to these external sites should open in a new browser window. Ongoing review to maintain links and verify that they are operational is expected.
- Publications should include relevant dates, including the date on which the publication was placed and date the page was last updated.
- Publications should include the district email address of the staff member responsible for the page. 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.
- District or school web or social media sites may not be used for personal or financial gain. No commercial or private accounts should be listed on any district or school web pages.

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 or social media sites.

- Student’s last name, last name initial, and grade-level shall **not** be published on a district or school web pages. However, in special circumstances (e.g., where accolades are warranted), the sponsoring staff member may contact the school principal or designee to determine if the parent/guardian signed a consent form allowing for the use of their child’s picture or other identifying information.
- Student records may not be disclosed. Web pages shall not display student pictures with a student identified by his or her name unless written parental permission is first granted (e.g., by executing the media consent form).
- Student email addresses shall not be listed on any district or school web page.

Content

All content published on the district or school web sites or on websites maintained by staff on other servers that students can access must be current and managed in accordance with the following:

1. Comply with state and federal laws concerning copyright, intellectual property rights, and legal uses of network computers.
2. Comply with Board of Education policies, administrative procedures, these guidelines, and other district guidelines provided for web publishing, including the Board’s *Access*

to Electronic Networks policy and the district's procedures on *User and Management Guide for District 65's Electronic Resources and Internet Access*.

3. Comply with the general publishing expectations listed below.

Materials that fail to meet these guidelines or are in violation of Board policy and/or procedures shall not be published on the district or school web sites. The district reserves the right to remove any materials 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.

Submitting Material for Publication on the District or School Websites

Each person submitting material for publication for the district or school web or social media site must have signed an Authorization for Electronic Network Access. Before material is published on the district or school web site, 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 web or social media site is deemed "work for hire," and the copyright in those works vests in the district.

All material submitted for the district web or social media site is subject to treatment as a district-sponsored publication.

Webmaster and Publishing Authority

The following categories describe the levels of authority regarding district and teacher maintained websites.

District-Level — The Communications Director serves as the district webmaster with overall supervision for the district web and social media sites. The Communications Director is responsible for adding administrative user accounts and district and teacher web pages. The Director also is available to support administrative departments, school webmasters and instructional technology staff as needed.

The district webmaster manages the district-level web publishing efforts and supervises other levels of web publishing. District-level publishing includes the district's homepage as well as publishing activities representing the district as a whole, e.g., information for the Board of Education, policy, updated annual reports, etc. The district homepage shall have a link to an Online Privacy Statement.

Department-Level — District departments (e.g., Business Office, Curriculum, Human Resources, Transportation, etc.) will publish their own web pages as part of the district's web site. The department supervisor or director is ultimately responsible for his/her respective department's web pages, but may appoint a staff member as the department's webmaster to fulfill the maintenance tasks. Department supervisor or director shall keep the district webmaster informed of who is the department webmaster or provide updated information to the District's webmaster for posting.

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 web site'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.

Web-published material should coincide with the department's printed material. The district webmaster should be consulted before publishing potentially sensitive material, e.g., school comparisons or student data. Administrative department directors are responsible to review departmental information and material before it is published to their pages on the district web site.

School-Level — the building principal is the webmaster for the school and is responsible for the school's web pages. A staff member may be appointed as the school webmaster to fulfill the maintenance, reviewing, and uploading tasks. This individual has overall supervision of the school web site, subscribes users, removes subscriptions for users no longer at the school, and ensures that all faculty and staff are using a district-issued web page or have a disclaimer on the page linking to an external page. The school webmaster also is responsible for scheduling instructional technology staff to assist with training at the school.

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. Teachers and staff who use web development tools other than those provided by the district shall place a disclaimer on their web page along with a link to the external site.

Instructional Technology Staff (Instech) support principals and school webmasters with site-based and individual training (based upon scheduling and availability). Instech are responsible for ensuring that teachers and staff members who use web development tools other than those provided by the district shall include the following disclaimer on their web page along with a link to the external site:

> *District 65 supports a home-to-school connection using a variety of technology tools, including teacher web pages. The following link will take you to an external web page created by Mr. Michel. This site is designed to support that home to school connection with parents and students, but is independent of the District site. The creator is solely responsible for the content therein*.

Definitions

The following definitions are used throughout the User and Management Guide and the district's Acceptable Use Agreements.

Acceptable Use Policy (AUP) – District policy, adopted by the board, outlines the permissible activities for use of the district's computing, Internet, email and telecommunications resources including equipment, storage space, software, and network. The district's Acceptable Use Policy incorporates the Acceptable Use Guidelines which may be changed from time to time.

Acceptable Use Agreement (AUA) – An agreement signed by each individual accessing or using the district's computing, Internet, email and telecommunications resources including equipment, storage space, software, and network. The agreement lays out the appropriate and inappropriate uses of the system.

Employees must formally sign an agreement each year to have access to the district's resources. Parents must sign an acknowledgement of their responsibilities to have read and discussed the Acceptable Use Policy with their children. Failure to provide a signed agreement each year does not relieve the employee or student from the requirements contained within the agreement. The act of logging into the system directly implies consent to be governed by the terms of the agreement and guidelines.

Children's Internet Protection Act (CIPA) – The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. *http://www.fcc.gov/cgb/consumerfacts/cipa.html*

Federal Family Educational Rights and Privacy Act (FERPA) – The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Illinois Harassing and Obscene Communications Act, (720 ILCS 135/0.01) – Illinois law that prohibits harassing or obscene communications using electronic communications including but not limited to telephones, computers, email, websites etc.
http://law.justia.com/illinois/codes/chapter53/1883.html

Illinois Internet Safety Education Act (105 ILCS 5/27-13.3) – Beginning with the 2009-2010 academic year, Illinois schools will be required to incorporate into the school curriculum a component on Internet safety to be taught at least once each year to students in grade 3 or above. *http://www.ltcillinois.net/Internet_Safety.html*

Public Forum –A vehicle set aside for expressive activities and communications. Unless expressly stated, District 65's technology resources, communications systems, email, and web site are **not** a public forum.

Streaming Audio or Video – Audio or video content that is received on a continuous basis.

User – Any authorized individual or group permitted to access or use the District 65 computing, Internet, email and telecommunications, network, and equipment.

User Account – An account establishes the user's username, password, email address, rights of access, and storage space. An individual may have only one user account and is responsible for protecting the username and password for the account. Usernames and passwords may not be exchanged or shared with other users.

Acceptable Use Agreement for Teacher and Administrator Access Use of Networked District 65 Information Resources

Directions: Please read and sign the following agreement. Your signature is required before an account will be issued to you. Please return this signed form to Information Services. A full and detailed list of requirements and restrictions is included in the User and Management Guide for District 65's Electronic Resources and Internet Access at www.District65.net.

The Internet

Internet access through the district is intended for instruction, research, and school administration. Network and Internet access is not for private business or personal, non-work related communications. By signing this agreement, the user agrees to abide by Board policies governing the use of District 65's technology and networked resources, including the Internet.

It is understood that while monitoring Internet access from outside the school is the domain of parents, guardians, or staff, individuals may be held responsible for harassing, embarrassing, threatening, or defamatory content provided outside of school and may be considered for disciplinary action. All suspected instances of online harassment should be reported to your principal or supervisor and Information Services.

Instructional Practices

Teachers and other educators are expected to select instructional materials, recommend research sources, and guide students on the use of instructional technology and materials on the Internet. Whenever possible, teachers should preview the appropriateness of the content ensure that it is appropriate to promote the objective of the lesson.

Privacy and Security

Internet safety and security are ongoing concerns for all Internet users. Unwanted email and offensive or harassing material are annoying and may result in significant problems, including identity theft. Information Services strongly cautions and discourages teachers and staff from providing their personal or financial information, home address, and district email address to websites, businesses, or individuals over the Internet. Personal information should never be given to any unsolicited inquiry.

District 65 employs filtering devices and software to provide a secure and safe network environment. While these systems are efficient, they are not foolproof and objectionable material may get through. Employees should report to Information Services any instances in which they receive objectionable, offensive, or unwanted material.

Equipment, network resources, messages, files, programs and software applications that are stored on or relayed by District 65's computers and servers are not private. District 65 and its representatives employ mechanisms to monitor users' on-line activities, including website browsing, email use, chat room participation, and other forms of electronic communications. District 65 reserves the right to monitor any users' online activities at any time with or without notice, and to access review, copy, store, or delete any electronic communications or files and disclose them to others as it deems necessary. All emails are permanently archived in accordance with federal and state laws.

Information Services staffs routinely use software to remotely access or control District 65 computers. Use of this software is critical to the proper service and maintenance of equipment, and to provide technical assistance to users. Whenever feasible, users will be notified when their equipment is or has been remotely accessed. However, the district reserves the right to access computers and files without notice.

Restrictions

In compliance with the Illinois Harassing and Obscene Communications Act, (720 ILCS 135/0.01), the federal Children's Internet Protection Act (CIPA), the Federal Family Educational Rights and Privacy Act (FERPA), the Illinois Internet Safety Education Act (105 ILCS 5/27-13.3) and all other applicable local, state and federal statutes and guidelines, the following activities are not permitted on District 65's electronic resources:

- Accessing, uploading, downloading, transmitting, displaying or distributing obscene, abusive, intimidating, threatening, defamatory or sexually explicit material or language or otherwise harassing students or staff.
- Transmitting a student's personal information, work or picture with identifiable information without written parental permission.
- Using another person's passwords; trespassing in another person's folders, work or file.
- Selling or buying anything over the Internet for personal financial gain; or selling or purchasing any illegal substance.
- Using the Internet for advertising or promotion, including conducting for-profit business activities or engaging in solicitation for non-profit groups, religious purposes, lobbying, or votes.
- Damaging computers, computer systems or computer networks; vandalizing, damaging or disabling the property of another person or organization; debilitating or disabling computers, systems or networks through the intentional mis- or overuse of electronic distribution or storage space, the spreading of computer "viruses," or hacking.
- Violating copyright, or otherwise using another person's intellectual property without his or her prior approval or proper citation; using another person's passwords; trespassing in another person's folders, work or files.

Sanctions

Violations of District 65 and school networked policies may result in the loss of access to the resources, reprimand, or personnel action, including dismissal or legal action. Alternative disciplinary action may be determined at the building and/or classroom level in line with existing practice regarding language and behavior. When appropriate, law enforcement agencies may be involved.

Teacher and Staff Supervision of Student Computer Use

Teachers, staff, and others whose duties include classroom management must sign a *Teacher and Administrator Acceptable Use Agreement* acknowledging responsibility for exercising reasonable supervision of student access to Internet and electronic mail, and responsible professional use prior to being issued an account.

EMPLOYEE AGREEMENT

I have read, understand, and agree to abide by the provisions of the User and Management Guide for District 65's Electronic Resources and Internet Access and the Acceptable Use Agreement of the Evanston/Skokie School District 65.

I understand and agree that in the event a third party makes a claim against the school district as a result of my use of the equipment, the computer network or the Internet provided by the school district, the school district reserves its right to respond to such a claim as it sees fit and to hold all offending parties, *including myself,* responsible.

I release District 65, its affiliates, and its employees from any claims for damages of any nature arising from my access or use of the computer network or the Internet provided by the School District. I understand that I am responsible for toll charges (if any) as a result of using District 65 Internet services. I also agree not to hold the school district responsible for materials improperly acquired on the system or for violations of copyright restrictions, user's mistakes or negligence, or any costs incurred by users.

Employee: ____ **Signature:** ____
Please Print

Date: ______/_____/_____

Evanston/Skokie School District 65
Acceptable Use Handbook