Urbana School District 116
Acceptable Use Policy
Guidelines for Acceptable Use of District Computer Network by Employees

Purpose: To provide guidelines intended to assist Urbana School District 116 (USD 116) staff in following established policies, practices, and procedures to use technology in a responsible and productive manner.

Policy: The Urbana School District 116 Wide Area Network (**WAN**) has been created to link school buildings, administrative sites, and support facilities together for the purpose of accessing, creating, analyzing, applying, and sharing information in accordance with the objectives and strategies set forth by the Urbana School District 116 Strategic Plan.

The Urbana School District 116 Local Area Network (**LAN**) has been created to interconnect computers, servers, printers/copiers, and other devices at the building level to collaborate, create, and share information. Employees are required to use the school system technology within the scope of their employment. Students and employees are expected to follow the accepted and established guidelines for technology usage. (Board Policy 5:192)

Urbana School District 116 views technology (including computers, mobile devices, scanners, digital cameras, video projectors, video cameras, and the Internet) as instructional tools for teaching and learning. Employees, Authorized Contractors, Mentors, and Volunteers of Urbana School District 116 are expected to use technology resources for educational, administrative and business purposes only. Any user of the Urbana School District 116 Network, Internet, and technologies should always reflect academic honesty, high ethical standards, and moral responsibility.

A. **Acceptable Use**

All users of Urbana School District 116 Network ("Network") must comply with the District's Acceptable Use Policy Guidelines, as may be amended from time to time.

The Network shall include all computer hardware and software owned or operated by the District, the District electronic mail (Email), the District's website, the District on-line services, Intranet and direct or wireless connection to the Network. "Use" of the Network shall include obtaining access from *any* computer, wired or wireless connection, personal or district laptop, personal or district mobile device; this includes external users (Contractors, guest, etc.).

Employees should have no expectation of privacy in their use of the Network. The District has the right to access, review, copy, or disclose any information sent, received or stored on the District's electronic mail system. The District has the right to and does monitor the use of the Network by employees, including but not limited to employees' access to the Internet and internal/ external e-mails, as part of Network maintenance to determine whether the use is consistent with Federal and State laws

and District policies and guidelines. Employees using the Network, as defined above, have no expectations of privacy on any computer/device on the network and the District has the right to inspect, access, review, copy, or disclose any information sent, received, or stored via use of the Network.

Employees should be aware that their personal computer files or Network use may be subject to public disclosure under the *Illinois Freedom of Information Act.*

Access to the Network is provided to employees for work-related purposes. Incidental personal use must be minimized and personal use may be terminated if the District, in its sole discretion, determines that the use is excessive.

B. **Privileges**

Access to the Network is provided as a privilege by the District and may be revoked at any time. Inappropriate use may result in discipline according to the Collective Bargaining Agreement between Urbana Education Association (Certified), IEA-NEA and Urbana School District #116 Board of Education, which can include the loss of technology use and privileges on the network.

The Network, including all information and documentation contained therein, is the property of the District, except as otherwise provided by law.

C. **Prohibited Use**

The following non-exhaustive list identifies prohibited use of the Network. The prohibited uses include, but are not limited to, the following:

1. Engage in activities which are inconsistent with the District's educational mission and Strategic Plan or which interferes with an employee's ability to perform her/his work responsibilities.

2. Access, retrieve or view indecent, obscene or profane materials. "Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.

3. Access, retrieve, view or disseminate any material in violation of any Federal or State laws or regulation or District policy or rules. This includes, but is not limited to: improper use of copyrighted material; improper use of the Network to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, District employee or user.

4. Transfer of any software to or from the Network without authorization from the Director of Instructional Technology, Assistant Superintendent of Curriculum and Instruction or Superintendent or designee.

5. Engage in any for-profit or non-school sponsored commercial activities, including advertising or sales without proper authorization.

6. Online harassment, threats, or intimidation of an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.

7. Disrupt the Network or interfere with the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.

8. Unauthorized establishment of wireless access points including peer-to-peer wireless access without prior authorization by the Director of Instructional Technology or designee.

9. Gain unauthorized access to the Network to vandalize the data or files of a student or staff user or the computer/mobile device of any other individual or staff user.

10. Forge or improperly alter electronic mail messages, use an account owned by another user without authorization, or disclose the user's individual password or that of another user.

11. Invade the privacy of any individual, including violating Federal or State laws regarding limitations on the disclosure of student records.

12. Download, copy, print, or otherwise store or possess any data that violates Federal or State copyright laws or these Guidelines.

13. Send nuisance electronic mail, text messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages via the Network.

14. Send District-wide mass electronic mail to users without prior authorization by the Director of Instructional Technology, Assistant Superintendents, or Superintendent or designee.

15. Conceal or misrepresent the user's identity while using the Network.

16. Post material on the District's website without authorization of the Communication Specialist, Director of Instructional Technology, Assistant Superintendents, or Superintendent or designee.

17. Accessing social networks (Facebook, Vine, MySpace, Twitter, etc.), "chat lines" or entering "chat rooms" outside the scope of an employee's job responsibilities or not part of a **class activity** or **District Professional Development activity** via the District's network. Teachers wanting to access Social Media sites must complete a Web Bypass form.

18. Users causing undue congestion of the network through lengthy downloads of files, or by engaging in idle activities; e.g., playing non-educational games, or games that are not part of a class activity: or, employees involved in actions other than their job responsibilities.

D. District Websites

Acceptable use of Urbana School District 116 Websites and all related resources requires web managers to:

1. Use the website to improve communications and services of the USD #116 schools or departments with students, parents and families, staff, the community-at-large, and the District, both nationally and globally.

2. Protect private information of students and staff such as addresses, phone numbers, passwords, and other personal information as applicable by all local, state, and federal laws.

3. Use appropriate language, graphics, and photos.

4. Respect all applicable copyright laws.

5. Understand that use of the website for commercial purposes or illegal activities is strictly prohibited, except when commercial purposes are specifically allowed by the USD #116 Board of Education.

6. In the use of photography on the public webpage, when identifying a specific person by first and last name, written permission by way of the standard Urbana School District 116 Publicity and Photo Release Form should be on file. The images of students should always follow the guidelines set forth within the Publicity and Photo Release Form.

7. Any web site or social media site created by a USD #116 employee for professional use must be job related and part of a District sponsored activity. All content of a web site or social media site created by the employee, including links to other sites not controlled by the employee, must conform to the Acceptable Use Policy Guideline and be mindful of all applicable Federal and State guidelines. Employees may not place any personal or editorial material on any District owned web site or social media site or any site created and maintained by an employee for professional use. Links to a site created by an employee for professional use can be published on any District owned web site, with the approval of the web site content owner, e.g. a building Principal can approve a teacher's

classroom web site link to be added to their building's web site staff list. This also includes district owned and sponsored social media sites.

E. Disclaimer

The District makes no warranties of any kind whether expressed or implied for the Network. The District is not responsible for any direct or indirect damages incurred, including the loss of personal information or data resulting from delays, non-deliveries, or service interruptions. Use of any information obtained via the Network is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through the Network and only facilitates the accessing and dissemination of information through its systems. The District is not responsible for any user's intentional access of material on the Internet that may be obscene, indecent, or of an inappropriate nature.

F. Security and User Reporting Duties

Security on the Network is a high priority and must be a priority for all users.

Users are prohibited from sharing their District login, Google Education IDs or passwords with any other individual. Any attempt to log in as another user will result in consequences as set forth in Section H of these Guidelines.

A user who becomes aware of any security risk or misuse of the Network should immediately notify their building's Principal, Assistant Principal, Dean, Technology Cadre member, or a member of the Technology Department via telephone or email.

G. Vandalism

Vandalism or attempted vandalism to the Network or equipment used to support the infrastructure of the Network is prohibited and will result in consequences as set forth in Section H of these Guidelines. Vandalism includes, but is not limited to, the downloading, uploading, unauthorized access to any district computer, creating and disseminating computer viruses, or physical damage to District owned student and staff computers, mobile devices, servers, routers, switches, access points, wiring closets or other infrastructure equipment.

H. Consequences for Violations

Any user of the Network that violates this policy shall be subject to discipline according to the Collective Bargaining Agreement between Urbana Education Association (Certified), IEA-NEA and Urbana School District #116 Board of Education and which may also include: (1) suspension or revocation of Network privileges, and/or (2) referral to law enforcement authorities or other legal action in appropriate cases.

I. **Web Bypass**

A Web Bypass is used by district personnel to access sites that are normally blocked. Teachers requiring access to sites that are blocked need to complete a Web Bypass form. This form must indicate the purpose of access and must have and list a direct correlation to the Common Core State Standards, Illinois Learning Standards, or National Educational Technology Standards. All forms submitted by the teacher will need to have a signature from the building Technology Cadre member, Administrator or Dean, and submitted to the Director of Instructional Technology for approval.

J. Grants

The school district must inventory all technology equipment purchased with grant funds regardless of the type of grant. In addition, all equipment must be engraved with a district inventory number indicating grant name, year of purchase, and school name. The grant recipient(s) should take responsibility for the management of the equipment and for monitoring its effective use within the school or classroom. Grant equipment should normally be kept in the school. The teacher may, with a completed Employee Equipment Agreement form on file, use the equipment at home for professional purposes. Transferring of technology equipment between schools will need approval by the building Principals and Director of Instructional Technology. After the grant has expired the equipment will remain the property of the District.

K. Email

Urbana School District 116 has transitioned to Google Apps for Education (GAFE) and all email users must comply with the rules set forth by the District and Google's email policies. Google domain users are encouraged to change their passwords at least twice a year. The password must have a minimum of 8 characters, and should contain at least one lowercase letter, one capital letter, one number, and one special character.

Urbana School District #116 Guidelines for Acceptable Use of District Computer Equipment and Network Access by Employees

This form must be read and signed by each user as a condition of using the Urbana School District 116 Computer Network. A copy of this document will reside inside of the employee's folder.

By signing this Authorization, I acknowledge that I have read and received a copy of the "Acceptable Use Policy Guidelines for Acceptable Use of Urbana School District 116 Computer Network by Employees" and that I understand, and agree to follow the Guidelines.

I acknowledge that accessing the Urbana School District 116 Computer Network is provided as a privilege by the District to support instruction and communication, and any inappropriate use may result in discipline and loss of use.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT COMPUTER NETWORK, AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE NETWORK.

Name:

School or Building

Signature:

Date: