

<p style="text-align:center">UTICA CITY SCHOOL DISTRICT COMPUTER NETWORK ACCEPTABLE USE POLICY</p>

PURPOSE

The purpose of the Utica City School District Computer Network is to provide shared educational resources with its member schools and with regional districts. The resources are intended to enhance the collaboration and exchange of information between and among schools, school offices, and other State and educational entities.

MISSION

The Utica City School District Computer Network is committed to the use of technology to support district school improvement initiatives in the context of the NYS Long Range Plan for the Use of Technology in Elementary and Second Education and the New York State Learning Standards.

RATIONALE

The rationale for establishing the Utica City School District Local and Wide Area Computer Networks, and Internet access Network is to provide a mechanism that will advance and promote education in all of its school buildings. The Network is intended to facilitate the collaboration and exchange of information among all who are concerned and involved with education. The integration of networking technology into daily operations of your classrooms, libraries, and offices is intended to promote the development of high-quality technological resources in an effective, efficient, and economical manner.

GUIDELINES

It is imperative that staff, students, and visitors conduct themselves in a responsible, and legal manner while using District equipment and networks. This policy provides general guidelines for use by its users. Final determination of acceptable behavior rests with the Superintendent. The following factors define District policy for Computer Network and Internet access:

- A. Any use of District equipment or computer networks for inappropriate, illegal, obscene, or sexually exploitive purposes is prohibited. Illegal activities are defined as any violation of local, State and Federal laws as well as any violation of the District's established rules and regulations governing appropriate behavior. Inappropriate use is defined as any violation of the intended purpose to which the network access account was issued. Obscene activities are defined as any violation of generally accepted social standards

for use of publicly operated communication medium, which is accessible, by children and underage adults;

- B. Any use of the District's equipment for commercial purposes, or individual profit is prohibited;
- C. Any use of the District's equipment for partisan political activity is prohibited;
- D. Any use of the District's equipment that is intended to disrupt use by other users, deny intended services, or invade the privacy of others is prohibited;
- E. The District's network accounts shall be used only by authorized students and staff as approved by the building principal/district administrators. Users are solely responsible for all activity that occurs while logged in under their operating or individual accounts. This includes, but is not limited, to unauthorized long distance telephone charges, surcharges, and/or equipment or line charges, and assumption of liability or damages caused by misuse of the equipment, software or network systems;
- F. It is expected that all users will prudently use the District's resources and prevent waste wherever possible. Users may not intentionally write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self replicate (e.g., computer virus), damage or otherwise hinder the performance of any computer's memory, file system, or software;
- G. Users may not intentionally tamper with networks, terminals, printers, wiring, etc., or attach unauthorized devices or equipment to the network. Installation, modification, or removal of software will be done only under the supervision of a qualified technician and with the approval of the principal/district administrators;
- H. Students, staff, parents, and administrators are prohibited from disclosing student records, personnel information, confidential records, or internal financial data to unauthorized recipients;
- I. Any user's network communications that traverses another network is subject to that network's acceptable use policy;
- J. Student use is permitted with appropriate administrative authorization, and proper supervision. Supervision of student use and activities are the responsibility of the building principal.
- K. Users must recognize and observe applicable copyright laws and usage restrictions. Unauthorized duplication, deletion, alteration, or reconfiguration of District software, or any other activity deemed an infringement of a product copyright is prohibited;

- L. All data and other work created, stored, or maintained on District computing resources is the property of the District. Users are not permitted to inappropriately delete stored information, regardless of authorship, or to otherwise alter access to their computing resources in a manner which would deny the District access to historical information or which would otherwise impede normal functioning of the business of the District. Specifically, users are not permitted to “clean” information from their computers prior to departure, retirement, reassignment, etc., as such actions could be deemed a deliberate denial of service. This policy is not intended to preclude any legal rights of authorship to the owner of published material, created in the course of their duties with the District.

- M. The District reserves the right to read and/or access users’ files when necessary to resolve problems reported by the owner of those files, or in similar situations with the knowledge and consent of the owner. Access to a user’s directory and files may be necessary to remove extraneous files from the system or verify proper system operation, or to effectuate fixes and upgrades, or to comply with bona fide investigations. When access is required without the knowledge and consent of the owner, the activity will be logged by the building Technology representative, along with the reasons for access, for review by the Superintendent;

- N. Access to District computing resources shall terminate upon student graduation or employee termination of employment. Building Principals shall notify the designated Technology focal point (usually the “Sysop”) of any changes of student status. The Director of Personnel, and/or the employee’s termination date is determined, irrespective of the employee’s prior knowledge of the termination;

- O. Each building Principal (or his/her designated representative) is the first level of responsibility to review alleged infractions of this policy and will coordinate with District staff to determine appropriate corrective action. The Principal shall notify the Director of Technology in writing describing the incident and disposition, within three business days. This requirement shall not preclude nor affect the need to immediately notify the Director of Technology on matters of an urgent nature which require immediate corrective action;

- P. The Superintendent is the final authority on the resolution of any conflicts between this policy and other established procedures. The Superintendent is the final decision authority on all matters related to the District Computer Network.

SANCTIONS

- A. Violations may result in loss of access. Users involved will be informed of the nature of these violations, and will have an opportunity to respond to them;
- B. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior;
- C. Users may be required to make full financial restitution;
- D. When applicable, law enforcement agencies may be involved.

START-UP SCREEN NOTICE

- A. The following statement shall be displayed upon startup, “Your use of the workstation implies that you have read, understand and agree to abide by the Utica City School District’s Acceptable Use Policy for access to the device.”