

Central Community Unit School District #301

Employee Acceptable Use Policy

PO Box 396

Burlington, IL 60109

Tel: (847)464-6005 | Fax: (847) 464-6021

Todd Stirn, Superintendent

Central Community Unit School District #301 requires every employee who accesses a computer and browses the Internet while on the school premises to turn in a signed Acceptable Use Policy. **The form should be signed and returned to the District Office.**

Access to a computer will provide each employee with Internet access. Please note that the Internet is an association of diverse communication and information networks. The transmission of any material that violates any U.S. or state law or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets. Use for commercial activities by for-profit institutions is not acceptable. Use for product advertisement or political lobbying is also prohibited. Unauthorized and time-consuming recreational game playing, lottery, auctioning, or gambling is also prohibited. Please read the following pages to find out more.

Part of the school district's responsibility in preparing our employees for the 21st Century is to provide them with access to the World Wide Web. We believe that use of this global information network is very important. It is each employee's responsibility to learn and understand his/her role as a 'network citizen' and the code of ethics involved with this new global community.

Please review these materials carefully.

Access to the Internet

The School Board's goal is to include the Internet in the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

The School District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Individual School Board members and administrative staff members shall be treated like teachers. "Internet" includes all information accessed by Internet sites, E-Mail, on-line services, and bulletin board systems.

Curriculum

The use of the Internet shall be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the employees. The Internet shall comply with the selection criteria for instructional materials and library-media center materials. Teachers may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum. The Internet is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's connection to the Internet must be in support of education and/or research, and be in furtherance of the School Board's stated goal. Use is a privilege, not a right. General rules for behavior and communications apply when using the Internet. The District's *Authorization for Internet Access* contains the appropriate uses, ethics, and protocol for the Internet. Electronic communications and downloaded material may be monitored or read by school officials.

Authorization for Internet Access

Each teacher must sign the District's *Authorization for Internet Access* as a condition for using the District's Internet connection. The failure of any employee or teacher to follow the terms of the *Authorization for Internet Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Acceptable/Unacceptable Use of Internet

The Board of Education is committed to the goal of providing electronic network facilities for employees and staff of District #301. The Network is expected to be used in a responsible, efficient, ethical and legal manner in accordance with the mission of the Central Community Unit School District. Users must acknowledge their understanding of the general policy as a condition of receiving an account or using the networks.

Acceptable uses of the network are activities which support teaching and learning. Network users are encouraged to develop uses which meet their individual needs and which take advantage of the network's functions: web development, conferences, bulletin boards, data bases, and access to the Internet. Network users are encouraged to develop uses which meet their individual needs and which take advantage of the network's functions: web development, conferences, bulletin boards, data bases, and access to the Internet.

Unacceptable uses of the network include: violating the rights and privacy of employees of the District without proper authorization, using profanity, obscenity or other language. Transmission of any material in violation of any U.S. or state law or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets. Use for commercial activities by for-profit institutions is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

Privacy:

Investigating or reading another user's file is considered a violation of privacy. Reading unprotected files is intrusive, reading protected files, by whatever mechanism, is considered the same as "breaking and entering." Violations include, but are not limited to:

- Attempting to access another user's files without permission.
- Furnishing false or misleading information or identification in order to access another user's accounts.
- Attempts to access District computers, computer facilities, networks, systems, programs or data without authorization.
- Unauthorized manipulation of the District's computer systems, programs or data.

Theft:

Attempted or detected alteration of software, data or other files as well as disruption or destruction of equipment or resources is considered theft. Violations include, but are not limited to:

- Using subterfuge to avoid being charged for computer resources.
- Deliberate, unauthorized use of another user's account to avoid being billed for computer use.
- Abusing specific resources such as the Internet.
- Removing computer equipment without authorization.
- Copying or attempting to copy data or software without authorization. Users should assume that any software they did not create is copyrighted.

Vandalism:

Violations include, but are not limited to:

- Sending mail or a program which will replicate itself (such as a computer virus) or do damage to another user's account.
- Tampering with or obstructing the operation of the District's computer systems.
- Inspecting, modifying or distributing data or software (or attempting to do so) without authorization.
- Damaging computer hardware or software.

Harassment

Sending unwanted messages or files to other users may be considered harassment. Violations include, but are not limited to:

- Interfering with legitimate work of another user.
- Sending abusive or obscene messages via computers.
- Using computer resources to engage in abuse of computing center personnel or other users.

Miscellaneous:

Other acts considered unethical and abusive include, but are not limited to:

- Unauthorized and time-consuming recreational game playing.
- Deliberately slowing down the network.
- Non-productive or idle "chatting."
- Using computer accounts for work not authorized for that account.
- Sending chain letters or unauthorized mass mailings.
- Using the computer for personal profit or other illegal purposes.
- Personal and political advertisement.
- Display of offensive material and graphics in public areas.

Users must have a valid, authorized account and may only use those computer resources for which they are specifically authorized. Users may only use their account in accordance with its authorized purpose. Users are responsible for safeguarding their own account. Users should not allow another user to use their account unless authorized by the system administrator for a specific purpose. Passwords should be changed often to ensure that private and secure files are kept that way.

Users should promptly report misuse of computing resources, or potential loopholes in computer systems security to the network administrator, and cooperate with the systems administrator in their investigation of the abuse. It is the employee's responsibility to learn proper techniques and standards for participation, and understand that if he/she misuses the network, he/she will lose their access privileges. In order to be issued access privileges, must fill out the Central Community Unit School District #301 Acceptable Use application on a yearly basis.

Penalties for Computer Abuse:

Abuse or misuse of the District's computing facilities and services may not only be a violation of network policy and user responsibility, but it may also violate the criminal code. Action may include, but is not necessarily limited to:

- Suspension or revocation of computing privileges.
- Reimbursement to the District or the appropriate institution for resources consumed.
- Other legal action including action to recover damages.
- Referral to law enforcement authorities.
- Referral of offending faculty, staff, and/or employees to District authorities for disciplinary action.