

ACCEPTABLE USE PROCEDURES

Lincoln County School District #1 (LINCOLN COUNTY SCHOOL DISTRICT #1) makes available computing and network resources which may be used by students, staff, and patrons. These are intended to be used for educational purposes and to carry out the legitimate business of the District. Appropriate use of these resources includes instruction, independent study, authorized research, independent research, and the official work of District organizations and employees.

Lincoln County School District #1 is pleased to offer this resource which gives access to electronic mail (E-Mail) and the Internet. LINCOLN COUNTY SCHOOL DISTRICT #1 will require all potential users to acquire a Driver's License issued by LINCOLN COUNTY SCHOOL DISTRICT #1 before they will be given access to the system. To acquire the necessary Driver's License they must complete a questionnaire and attest in writing that they have read, understand, and will honor LINCOLN COUNTY SCHOOL DISTRICT #1's use restrictions pertaining to the network. Access to E-Mail and the Internet will enable students and staff to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Parents should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. LINCOLN COUNTY SCHOOL DISTRICT #1 has taken precautions to restrict access to these materials. However, on a global network it is impossible to control all materials, and users may discover inappropriate information. We believe the benefits gained via access to the Internet exceed any disadvantages. It is the responsibility of the users to honor LINCOLN COUNTY SCHOOL DISTRICT #1's use restrictions.

Students are responsible for good behavior on school computer networks just as they are in the classroom or a school hallway. Communications on the network are often public in nature, and general school rules for behavior and communications apply. Access to network services is granted to users who agree to act in a considerate and responsible manner. Access is a privilege--not a right. Access entails responsibility. Individual users of the District computer networks are responsible for their behavior and communications over those networks.

Lincoln County School District #1 reserves the right to monitor any and all information on the network. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. However, it shall not be the responsibility of the District to restrict, monitor, or control communications of individuals utilizing the network. Users should not expect that files stored within the network will always be private. The framework of responsible, considerate, and ethical behavior expected by the District extends to cover the use of school microcomputers and workstations, departmental computing facilities, general-use computers, District network resources, and networks throughout the world to which the District provides computer access. The following list does not cover every situation which pertains to proper or improper use of the resources, but it does address some of the responsibilities you accept if you choose to use a District computing resource or the network access which the District provides.

1. For any computer account, you are responsible for the use made of that account. You should set a password which will protect your account from unauthorized use and which will not be guessed easily. If you discover that someone has made unauthorized use of your account, you should change the password and report the intrusion to the system administrator. You should change your password on a regular basis to assure continued security of your account.
2. You must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other people, whether at Lincoln County School District #1 or elsewhere, unless specifically authorized to do so by those individuals. If an individual has explicitly and intentionally established a public server, or clearly designated a set of files as being for shared public use, others may assume authorization. However, if it is unclear whether some files are intended to be available for public use or not, you should assume that they are private files and are not intended for public access.
3. You must not attempt to decrypt or translate encrypted material, or obtain system privileges to which you are not entitled. You must refrain from any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects. If you encounter or observe a gap in system or network security, you must report the gap to the system administrator or your building administrator.

4. You must be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages that could create an atmosphere of discomfort or harassment for others. You must also refrain from transmitting to others in any location inappropriate images, sounds or messages which might reasonably be considered harassing. The District's policies on harassment apply equally to electronic displays and communications as they do to more traditional means of display and communication.
5. You must avoid wasting computing resources by excessive game playing or other trivial applications; by sending chain letters or other frivolous or excessive messages locally or over an attached network; by printing excessive copies of documents, files, images, or data. You must refrain from using unwarranted or excessive amounts of storage; printing documents of files numerous times because you have not checked thoroughly for all errors and corrections; or running grossly inefficient programs when efficient ones are available. You must be sensitive to the specialized nature of software, hardware, and services available in a limited number of locations, and allow access to those people whose work requires these specialized facilities.
6. You must not prevent others from using shared resources by running unattended processes or placing signs on devices to "reserve" them without authorization from the appropriate system administrator. Your absence from a public computer or workstation should be no longer than warranted by a visit to the nearest restroom. A device unattended for more than ten minutes may be assumed to be available for use, and any process running on that device terminated. You must also be sensitive to performance effects of remote login to shared workstations. When there is a conflict, priority for use of the device must go to the person seated at the workstation rather than to someone logged on remotely.
7. The District presents for your use many programs and data which have been obtained under contracts of license stating they may be used but not copied, cross-assembled, or reverse-compiled. In addition, other institutions and individuals on attached networks make software available under similar conditions. You are responsible for determining that programs or data are not restricted in this manner before copying them in any form, or before reverse-assembling or reverse-compiling them in whole or in any part. If it is unclear whether you have permission to copy such software or not, assume that you may not do so. Users are also prohibited from loading onto the system any software from personal or private sources without prior approval of the system administrator.
8. If you create or maintain electronically-stored data which is important to your work or to the District in general, you are responsible for the backup of that data. The District does backup data on its general access systems at regular intervals as preparation for a catastrophic loss of resources. However, you must decide whether or not this is an adequate substitute for making your own backups of the data you create or maintain.
9. Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. You are free and encouraged to publish your opinions, but they must be clearly and accurately identified as coming from you; or if you are acting as the authorized agent of a group, they must be identified as coming from that group. You must not falsely attribute (i.e., forge) the origin of electronic mail, messages, or postings. If you create, alter, or delete any electronic information contained in or posted to, any District computer resource or to any computer resource on an attached network, it will be considered forgery if it would be considered so on a tangible document or instrument. Users are also cautioned against listing personal addresses, phone numbers, credit card numbers, or social security numbers which may be stored on the system and accessed by others.
10. You must not create or willfully disseminate computer viruses. You should be sensitive to the ease of spreading viruses and should take steps to insure your files are virus free.
11. *You will not misuse, abuse, destroy, or damage the hardware components of the technology equipment.* Again, the above are only examples and not an exhaustive list. You also should be aware that there are Federal, State, and sometimes local laws which govern certain aspects of computer and telecommunications use. Members of the school community are expected to respect these laws, as well as to observe and respect District rules and regulations. Violations of appropriate use may result in one or more of the following actions:
 1. A written warning to the offender.
 2. A restriction of system access for a specified term.
 3. A revocation of all system privileges for a specified term.

4. A statement of charges to the appropriate disciplinary authorities, which, with due process, could lead to additional penalties up to and including probation, suspension, or expulsion. Where applicable, violations of local, State, or Federal laws will be reported to law enforcement officials.

Lincoln County School District #1 is committed to providing error free access to network contents, but Lincoln County School District #1 shall not be held liable for any lost, damaged, or unavailable information due to technical or other difficulties. Lincoln County School District #1 reserves the right to, from time to time and on a case by case basis; charge a fee for consumable supplies and materials supplied by the District to users. The District also reserves the right to recover claims for any unauthorized debts to the District encumbered by violations of LINCOLN COUNTY SCHOOL DISTRICT #1's use restrictions. Lincoln County School District #1 reserves the right to refuse use of District computing resources to any person(s) found violating any prohibited, legal, ethical, or responsible guidelines outlined in District policies or handbooks. Adopted: 06/11/96