

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Code **IJNDB-R** Issued **2/21**

Please read the following carefully before signing the attached documents.

Technology is a vital part of the education and the curriculum of the School District of Newberry County. In an effort to promote learning and expand educational resources for students, the district is making available computers, computer networks, and Internet access for all students, faculty, and staff. The district's goal in providing this service is to promote the educational use of technology to access and utilize information effectively. Access to these computers and networks will allow students to be successful in accomplishing this goal by allowing them to communicate with others on a global level and access educational materials worldwide.

With this access comes the availability of materials that may not be considered to be of educational value in the context of the school setting. However, on a global network, it is impossible to control all the materials and an industrious user may discover controversial information. We firmly believe that the valuable information and interaction available on these networks far outweigh the possibility that users may locate materials that are not consistent with the educational goals of the district. In compliance with the Children's Internet Protection Act (CIPA), 47 USC Section 254(h), the district uses technological devices to filter and block obscene materials, child pornography, or "harmful to minors" materials as defined by the CIPA.

Access to the computers, networks, technology, and Internet is a privilege, not a right. With this privilege, there is also the responsibility to use the technology solely for educational purposes and not to access inappropriate materials. These guidelines are provided so that users are aware of their responsibilities when using the network. Any violations of these guidelines will subject users to appropriate disciplinary actions and possible denial of access to the network.

Prior to accessing information technology resources, parents/legal guardians will be provided with a copy of the policy and administrative rule to review with their student. If after reading the policy and administrative rule, parents/legal guardians agree that they understand the policy and administrative rule, that their student will comply with the guidelines set forth herein and that they understand the consequences for violating these guidelines, their agreement will be assumed without a written response. If the parents/legal guardians **do not** agree that their student will access information technology resources in accordance with the policy and administrative rule, the parents/legal guardians will sign a statement of opting out. The Technology Use Opt-Out Agreement will be placed in the student's permanent record and the student will not have access to school/district information technology resources.

Terms and Conditions for Use

The following conditions for the acceptable use of computers and networks will apply to all district administrators, faculty, staff, and students. All technology equipment will be used under the supervision of the site technology coordinator or classroom teacher.

- Users will not erase, rename, view, or make unusable anyone else's computer files, programs, or disks.
- Users will not let other persons use their name, logon, password, or files for any reason (except for authorized staff members). Users will not reveal personal information about themselves as well as others (e.g., phone number and address).

PAGE 2 - IJNDB-R - USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

- Users will not use or try to discover another user's password.
- Users will not use the computers or networks for any non-instructional or non-administrative purpose (e.g., games or activities for personal profit).
- Users will not use the computers for unlawful purposes such as illegal copying or installation of software.
- Users will not copy, change, or transfer any software or documentation provided by the district, teachers, or another student without permission from the site technology coordinator.
- Users will not write, produce, copy, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such code is often called a virus.
- Users will not deliberately use the computers to annoy, bully, or harass others with language, images, or threats. Computers used to harass, intimidate, or bully are defined as electronic communication devices reasonably perceived to have the effect of either of the following:
 - harming a student emotionally or damaging a student's property, or placing a student in reasonable fear of personal harm or property damage
 - insulting or demeaning a student or group of students causing substantial disruption in, or substantial interference with, the orderly operation of the school
- Users will not deliberately access or create any obscene or objectionable information, language or images such as pornography; indecent, vulgar, profane, or lewd materials; or advertisements. Violation of this item may result in action by local, state, or federal authorities.
- Users will not intentionally damage the system, damage information belonging to others, misuse system resources, or allow others to misuse system resources.
- Users will not tamper with computers, networks, printers, or other associated equipment except as directed by the teacher or site technology coordinator.
- Users will not download files from the Internet except with the permission of the teacher or site technology coordinator.
- Users will not install personal software, VPN software, or make any unauthorized changes to the operating system on school devices.
- Users will report all violations of these guidelines to the teacher or site technology coordinator.
- Users will not capture, record, or transmit the words and/or images of any student, staff member, or other person in the school without the express prior notice and explicit consent.

Consequences of Violations

Use of the technology systems operating in the district is a privilege and not a right. Violation of the policy and administrative rule concerning the use of technology will result in disciplinary actions similar to other code of conduct violations.

PAGE 3 - IJNDB-R - USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

- Level 1 Warning: Student would lose computer privileges/Internet access until a parent conference is held. Further loss of privilege and length of time will be determined by the administration.
- Level 2 Pattern of abuse or flagrant violations: Any student who, after a Level 1 warning, continues to engage in serious or persistent misbehavior by violating the district's previously communicated written standards of conduct may be removed from class and recommended for suspension.
- Level 3 Expellable offense: Student could be expelled from school if he/she engages in conduct that contains the elements of the offense of criminal mischief as defined by local, state, and federal law. Expulsion may be considered in flagrant violations that blatantly corrupt the educational value of computers or the Internet or compromise another computer network.

Reporting

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to building level administration and local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Video Surveillance Cameras

For security purposes, the district has installed video surveillance cameras on all campuses.

Personally-Owned Devices Policy

The district currently has limited Internet bandwidth provided by the State of South Carolina and limited wireless access in the schools. When given permission by school staff/administration, students are allowed to bring personal electronic devices (PEDs) to school for educational purposes. These devices should be connected to the guest wireless (Internet access only).

Personal Electronic Devices

- All personal electronic devices are subject to the same policies and procedures established for the use of district owned equipment. Each classroom teacher will choose when mobile devices can be used within his/her classroom. The use of a personal or any other electronic device will be at the discretion of the teacher and school administration.
- Students and staff members should connect personal devices to the appropriate network: NCS D guest.
- The device is to be used during class with the express permission and under direct supervision of the classroom teacher.
- The owner takes full responsibility of his/her personal device. All devices are brought to school at the owner's risk.
- No device may be used to record, store, or transmit any type of image, sound, or video, without the explicit permission of the teacher or school administrator.

PAGE 4 - IJNDB-R - USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

- The district reserves the right to confiscate or inspect a student's personal electronic device if there is reason to believe that it was used to violate policies, administrative procedures, or school rules. Devices may be confiscated at any time if guidelines are not followed. Return of the device is contingent on the outcome of a meeting with the student and parents.
- Employees should not access confidential student information from personal devices.

Email Usage

The district's email is available to authorized users for educational and district related purposes. The district prohibits the use of its email system for unprofessional or inappropriate purposes including, but not limited to, the following:

- any use that violates local, state, and/or federal laws or regulations
- setting up or operating a commercial business
- email that could be perceived as harassing, offensive, threatening, obscene, sexual, racist, or discriminatory to the receiver

In compliance with the Federal Rules of Civil Procedure sections 16, 24, 34 and 37, the district reserves the right to archive, monitor, and/or review all use of its email system. Users should not expect the right to privacy in any electronic message created, transmitted, or received on the district's email system. All emails transmitted on the district's email system are property of the district.

Mailbox Retention

All users will have a usable limit of total emails pace on the email server. When 90 percent of the user mailbox space is filled, the user will receive an automatic notification that he/she is reaching the limit amount. Once users receive this notification, they will need to remove unwanted or old email from the system. Users will be limited to 25 megabyte email attachments coming into and sending out from the district. Any attachments larger than 25 megabytes will be blocked by the system and the user will be notified.

All users are encouraged to file or archive email that is needed beyond one school year.

Email attachments being sent into the district with files extensions of .exe, .bat, .pif, .scr, .zip, .msi, .dll, and .reg will be blocked due to virus/security concerns.

Note: The district reserves the right to retain email records for one calendar year with no reasonable expectation of electronic email records being accessible or recoverable beyond this period of time, due to server space limitations and cost to maintain.

Issued 4/27/97; Revised 6/25/01, 1/26/09, 5/21/12, 5/22/17, 8/28/17, 2/22/21