JERSEY COMMUNITY UNIT SCHOOL DISTRICT NO. 100
JERSEY & GREENE COUNTIES, ILLINOIS
Phone Number 618-498-5561
Fax Number 618-498-5265

STAFF REQUIRED USE & INTERNET SAFETY POLICY (RUP)

PURPOSE: Jersey CUSD No. 100 provides its students and staff access to a variety of technological resources, including laptop computers. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school district's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

Jersey CUSD No. 100 intends that students and employees benefit from these resources while remaining within the bounds of safe, legal and responsible use. Accordingly, Jersey CUSD No. 100 establishes this policy to govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks. It also requires staff to abide by the Jersey CUSD No. 100 Technology Use Guidelines (Appendix A) and Staff Social Networking Guidelines (Appendix B). Additional rules may be added at any time as necessary and will become a part of this policy.

TERMS OF THE REQUIRED USE AND INTERNET SAFETY POLICY
Specifically, the staff: Will adhere to these guidelines each time the Internet is used at school or home.

- Will make available for inspection by an administrator upon request any messages or files sent or received at any Internet location. Files stored and information accessed, downloaded or transferred on district-owned technology are not private.
- Will use appropriate language in all communications avoiding profanity, obscenity and offensive or inflammatory speech. Cyber Bullying such as personal attacks and/or threats on/against anyone made while using district owned technology to access the Internet or local school networks are to be reported to responsible school personnel. Rules of netiquette should be followed conducting oneself in a responsible, ethical and polite manner.
- Will follow copyright laws and should only download/import music or other files to a district owned technology that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.
- Will never reveal identifying information, files or communications to others through email or post to the Internet that are not in compliance with HIPPA rules and regulations and personal Internet safety guidelines.
- Will not attempt access to networks and other technologies beyond the point of authorized access. This includes attempts to use another person's account and/or password.
- Will not share passwords or attempt to discover passwords. (Including sharing with other staff or substitute teachers.) Sharing a password could make you liable if problems arise with its use and subject to disciplinary action.
- Will not download and/or install any programs, files, or games from the Internet or other sources onto any district owned technology without Jersey CUSD No. 100 technology staff review for compatibility and scanning for computer viruses and other malicious software.
- Will not tamper with computer hardware or software, unauthorized entry into computers, and vandalism or destruction of the computer or computer files. Damage to computers may result in felony criminal charges.
- Will not attempt to override, bypass or otherwise change the Internet filtering software or other network configurations.
- Will use district technology for school-related purposes only and will refrain from use related to commercial, political or other private purposes.

- Will not make use of materials or attempt to locate materials that are unacceptable in a school setting. This includes, but is not limited to pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school media center. Specifically, all district owned technologies should be free at all times of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials (files).
- Will not connect any personal technologies such as laptops and workstations, wireless access points and routers, printers, etc to district owned and maintained local, wide or metro area network. Connection of personal devices such as iPods, smartphones, PDAs and printers is permitted but not supported by Jersey CSUD No. 100 technical staff. Home Internet use and cost is the responsibility of the staff member both in cost and configuration.
- Will not remove or alter the cache or site history in any browser on their laptop or on any other district owned device.
- Will back up data and other important files regularly. Jersey CUSD No. 100 will at times perform maintenance on the laptops by re-imaging. All files not backed up to server storage space or other storage media will be deleted during these processes. Students and staff are ultimately responsible for backing up all personal files on their own storage media.
- Will keep laptop secure and damage free.

Follow these general guidelines:

- Do not loan your laptop, charger or cords.
- Do not leave the laptop in vehicle.
- Do not leave your laptop unattended.
- Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.
- Do not allow pets near your laptop.
- Do not place the laptop in floor or in sitting area such as couches or chairs.
- Do not leave the laptop near table or desk edges.
- Do not stack objects on top of your laptop.
- Do not leave the laptop outside or use near water such as a pool.
- Do not check the laptop as luggage at the airport.

By signing this you agree to abide by the conditions listed above and assume responsibility for the care and proper use of Jersey CUSD No. 100 technology, including personally backing up personal data. Jersey CUSD No. 100 is not responsible for any loss resulting from delays, non-deliveries, missed deliveries, lost data, or service interruptions caused by user errors, omissions or reasons beyond the district's control. Information obtained via the Internet and other sources using Jersey CUSD No. 100 technologies is not guaranteed as to its accuracy or quality. I understand that should I fail to honor all the terms of this Policy, future Internet and other electronic media accessibility may be denied. Furthermore, I may be subject to disciplinary action, and if applicable, my Laptop computer may be recalled.

As the staff member, my signature indicates I have read or had explained to me and understand this Required Use Policy, and accept responsibility for abiding by the terms and conditions outlined and using these resources for educational purposes.

Staff (please print): _____

Staff Signature: _____ Date: _____

Terms and Conditions: This RUP is valid until the device is returned to the district.

JERSEY COMMUNITY UNIT SCHOOL DISTRICT NO. 100
JERSEY & GREENE COUNTIES, ILLINOIS
Phone Number 618-498-5561
Fax Number 618-498-5265

STAFF REQUIRED USE & INTERNET SAFETY POLICY (RUP)

APPENDIX A
TECHNOLOGY USE GUIDELINES

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

School district technological resources may only be used by students, staff and others expressly authorized by the Technology Department. The use of school district technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school district technological resources is use that is ethical, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Student Code of Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school district computers or electronic devices or who accesses the school network or the Internet using school district resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Furthermore, all students must adhere to any guidelines set forth in the Student Code of Conduct.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school district technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges.

Willful misuse may result in disciplinary action and/or criminal prosecution under applicable

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School district technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school district technological resources for political purposes or for commercial gain or profit is prohibited. Student personal use of school district technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school district business and is not otherwise prohibited by board policy or procedure.
2. School district technological resources are installed and maintained by members of the Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Technology Department.
3. Under no circumstance may software purchased by the school district be copied for personal use.
4. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Student Code of Conduct.
5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

6. The use of anonymous proxies to circumvent content filtering is prohibited.
7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. In addition, school employees must not disclose on school district websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) Users also may not forward or post personal communications without the author's prior consent.
10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.
11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the technology director or designee.
12. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.
13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.
14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
15. Employees shall not use passwords or user IDs for any data system (e.g., NCWISE, CECAS, time-keeping software, etc.), for an unauthorized or improper purpose.
16. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
17. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time, to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.
18. Views may be expressed on the Internet or other technological resources as representing the view of the school district or part of the school district only with prior approval by the superintendent or designee.
19. Without permission by the board, users may not connect any personal technologies such as laptops and workstations, wireless access points and routers, etc. to a district owned and maintained local, wide or metro area network. Connection of personal devices such as iPods, smartphones, PDAs and printers is permitted but not supported by Jersey CUSD No. 100 technical staff. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology.
20. Users must back up data and other important files regularly.
21. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use. The Jersey CUSD No. 100 technical staff does not support home or public Internet connections.

22. Students who are issued district owned and maintained laptops must also follow these guidelines:
    a. Keep the laptop secure and damage free.
    b. Use the provided protective book bag style case at all times.
    c. Do not loan out the laptop, charger or cords.
    d. Do not leave the laptop in your vehicle.
    e. Do not leave the laptop unattended.
    f. Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.
    g. Do not allow pets near the laptop.
    h. Do not place the laptop on the floor or on a sitting area such as a chair or couch.
    i. Do not leave the laptop near table or desk edges.
    j. Do not stack objects on top of the laptop.
    k. Do not leave the laptop outside.
    l. Do not use the laptop near water such as a pool.
    m. Do not check the laptop as luggage at the airport.
    n. Back up data and other important files regularly. Jersey CUSD No. 100 will at times perform maintenance on the laptops by reimaging them. All files not backed up to server storage space or other storage devices will be deleted during this process.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school district personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided for in the Children's Internet Protection Act (CIPA), and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology.

D. PARENTAL CONSENT

The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's e-mail communication by school personnel.

E. PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

Under certain circumstances, the board may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

F. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the school district network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access.

Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

G. PERSONAL WEBSITES

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school district or individual school names, logos or trademarks without permission.

1. Students

   Though school personnel generally do not monitor students' Internet activity conducted on non-school district devices during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy.

2. Employees

   Employees' personal websites are subject to Staff Social Networking Guidelines (Appendix B).

3. Volunteers

   Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or on-line networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school district may be terminated if the volunteer engages in inappropriate online interaction with students.

H. DISCLAIMER

Jersey CUSD No. 100 makes no warranties of any kind, whether express or implied, for the service it is providing. Jersey CUSD No. 100 will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or omissions. Use of any information obtained via the Internet is at the user's own risk. Jersey CUSD No. 100 specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

JERSEY COMMUNITY UNIT SCHOOL DISTRICT NO. 100
JERSEY & GREENE COUNTIES, ILLINOIS
Phone Number 618-498-5561
Fax Number 618-498-5265

STAFF REQUIRED USE & INTERNET SAFETY POLICY (RUP)

APPENDIX B
STAFF SOCIAL NETWORKING GUIDELINES

Staff decisions to use online social networking for personal use is at the employee's discretion. Jersey CUSD No. 100 does not affirmatively monitor social networking sites used by employees, if those sites/tools are not being accessed from the district's network; however Jersey CUSD No. 100 may take appropriate action if it becomes aware of, or suspects, conduct or communication on an online social media site that affects the workplace or violates an online code of ethics.

1. Do not accept students as friends on personal social networking sites. Decline any student initiated friend requests. Professional standards dictate that an adult should never be alone in an isolated space (i.e. one student, one teacher together in a classroom with the door closed after school operating hours). Social networking sites are structured to be closed environments. Please use district provided tools to communicate with your students, e.g., Edmodo, e-mail, forums, Google Groups, etc.

2. Do not initiate friendships with students on social networking sites.

3. Ensure that social networking posts are appropriate for the public. Remember that people classified as friends have the ability to download and share information with others.

4. Do not discuss students, their families, or co workers or publicly criticize school policies or personnel. This includes images obtained through your employment.

5. Weigh whether a posting will put your effectiveness as an employee at risk.

6. Set privacy settings carefully to ensure that you know who has access to the content on your social networking sites.