GRAND ISLAND CENTRAL SCHOOL DISTRICT
AGREEMENT FOR STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

In consideration for the use of the Grand Island Central School District's Computer System (DCS), I agree that I have been provided with a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. I agree to adhere to the staff policy and the regulations and to any changes or additions later adopted by the District. I also agree to adhere to related policies published in the Staff Handbook. I shall report all violations of the District's policy on use of computerized information resources to District officials.

All technology tools provided to staff are the property of the District and will fall under the guidelines listed below. This Agreement applies to all District technology resources including, but not limited to, on- and off-site use of blogging, social networking sites and tools, wikis, and podcasting or broadcasting tools provided by the District. In addition, employees who use personal technology equipment to perform job duties, including but not limited to cell phones, computers, tablets, smart phones and iPods which are not owned by the District, must comply with this agreement when using their own technology equipment while connected to the District wireless guest network (see Regulation #6410R.2 -- Staff Use of Personal/Mobile Technology).

Expectations for employee conduct while using these resources include, but are not limited to, the following:

1) Student Personal Safety

   a. Employees who supervise students with access to technology resources will be familiar with the District Regulation #7315R -- Student Use of Computerized Information Resources (Acceptable Use Guidelines) as well as the District *Code of Conduct* and enforce the provisions outline in both documents.

   b. Student use of technology will be supervised to the extent appropriate. Digital ethics is the responsibility of all who monitor student use.

2) Illegal or Destructive Activities

   a. Employees will not go beyond their authorized access to the District network or other computer equipment or software. This will include accessing the files or accounts of others without authorization.

   b. Employees will not disrupt or attempt to damage or disrupt any technology tools, infrastructure, network capacity, system performance, or data.

   c. Employees will not use District equipment or personal equipment connected to the District guest network to engage in illegal acts.

3) System Security

   a. Employees are responsible for the security of all technology tools, files passwords.

b. Employees will promptly notify their immediate supervisor of security problems.

c. Employees with access to student records may not use, release, or share these records (or information contained in these records) except as authorized by Federal and State law.

d. Employees whose position and responsibilities require a cell phone or other mobile device for District business purposes and who receive that service through the District service plan must notify the District *immediately* if their device is lost or stolen. Employees should contact their immediate Supervisor and/or Technology Coordinator. For District supplied devices, cell and data service will be terminated immediately to protect the organization from unauthorized use.

e. Personally owned flash drives shall not be used for District official business purposes.

4) Inappropriate Conduct

a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;

b. Potentially damaging, dangerous, or disruptive material;

c. Racial, sexual or other harassment or bullying in violation of District policies or regulations; and

d. False or defamatory statements.

5) Inappropriate Access to Material

a. Technology resources will not be used to access or disseminate material that is profane, obscene (pornographic), or advocates illegal acts, violence, or illegal discrimination. Inadvertent inappropriate access will be reported immediately to the supervisor.

b. Business use of instant messaging within the email program is allowed for District staff. The use of Internet games, web chats, unauthorized software, or non-authorized instant messaging software (e.g. AOL Instant Messenger, etc.) is prohibited.

c. Use of publicly available non-District created Web collaboration tools such as blogs, wikis and social networking tools for work purposes is acceptable, if conducted in accordance with Regulation #6410R.1 -- Social Media Guidelines for Employees. Staff must use District authorized resources to create teacher or classroom web pages. Unofficial personal use of social networking sites or Web 2.0 collaboration tools during the work day and using District technology resources is not permitted without prior supervisor approval initiated by an employee's supervisor. Excessive use of personal technology devices for non-work related activity during the work day is not permitted and may result in disciplinary action.

6) Expectation of Privacy

Employees have no expectation of privacy in files, disks, or documents that have been created in, entered in, stored in, downloaded from, or used on District equipment.

7) Discipline

a. Staff members who engage in unacceptable use may lose access to technology tools provided by the District and may be subject to further discipline in accordance with applicable law and collective bargaining agreements.

b. Deliberate violations of this agreement (e.g., malicious acts or omissions; searching for, viewing or otherwise visiting pornographic or sexually explicit sites) are cause for disciplinary action up to and including termination.

8) Unacceptable Uses

a. Illegal or malicious use, including downloading or transmitting of copyrighted material such as music, videos and games.

b. To solicit personal information with the intent of using such information to cause emotional or physical harm.

c. To disrupt the work of other users. This includes the propagation of computer viruses and use of the Internet to make unauthorized entry to any other Internet resource.

d. Use for private business purposes. This includes, but is not limited to, the installation or loading of personal business programs onto your computer for your use for tasks not associated with your District job duties.

e. Downloading of music, games or other programs for personal use, or streaming of music or video for personal use, are prohibited under all circumstances.

I understand that failure to comply with these policies and accompanying regulations may result in the loss of my access to the DCS and may, in addition, result in the imposition of discipline under the law and/or the applicable collective bargaining agreement. I further understand that the District reserves the right to pursue legal action against me if I willfully, maliciously or unlawfully damage or destroy property of the District.

Staff Member Signature: _____

Date: _____

School Building: _____