COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION
"Acceptable Use Policy"

The following rules and regulations govern the use of the district's computer network system, employee access to the Internet, and management of computerized records. It is in its entirety and represents the district's "Acceptable Use Policy."

I. Administration

All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the District Office and/or Office of the Department of Instructional Technology.

II. Internet Access

Student Internet access is addressed in policy and regulation 4526, Computer Use in Instruction. District employees and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's computer network.
- Employees are expected to review their e-mail daily.
- Communications with parents and/or students should be saved and the district will archive the e-mail records according to procedures developed by the District Administrator of Instructional Technology, Data Warehousing & Information System.
- Employees may access the Internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use.
- Employees are advised that they must not have an expectation of privacy in the use of the district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to **all users** of the district's computer system:

- Access to the district's computer network is provided solely for educational and/or research purposes and management of district operations consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically.
- Only those network users with permission from the District Administrator of Instructional Technology may access the district's system from off-site (e.g., from home).
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity for **all users** concerning use of the district's computer network. Any violation of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.

continued: <u>Prohibited Activity and Uses</u>

- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus, malware on the network, and not reporting security risks as appropriate.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software, using personal disks, or downloading files on the district's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for fraudulent purposes or financial gain.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while your access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

V. <u>No Privacy Guarantee</u>

Users of the district's computer network should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

VI. <u>Sanctions</u>

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VII. <u>District Responsibilities</u>

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or

continued: <u>District Responsibilities</u>

information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the user's own negligence or any other errors or omissions. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

The district will take reasonable steps to protect the information on the network and provide a secure network for data storage and use, including ensuring that contracts with vendors address data security issues and that district officials provide appropriate oversight. Even though the district may use technical and/or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

VIII. <u>Network Etiquette and Privacy</u>

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
2. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
3. Be polite – never send or encourage others to send abusive messages.
4. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
5. Do not use language that could be calculated to incite hatred against any minority group.
6. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.
7. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the District Administrator of Instructional Technology.
8. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
9. Pupils will not be allowed access to unsupervised and/or unauthorized chat rooms and should not attempt to gain access to them.
10. As part of our E-Rate and CIPA compliance, the District uses a filtering system to block inappropriate content from being accessed on the network. Staff or students finding unsuitable websites through the school network should report the web address to the District Administrator of Instructional Technology. In the event that an educational site is blocked, please fill out the appropriate form available on the Instructional Technology website and send it to the Instructional Technology Department.
11. Any personal laptop must be registered with the Instructional Technology Department prior to accessing the wireless network. The form is available on the Instructional Technology website.
12. Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. All sites visited leave evidence in the network and on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
13. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
14. Files held on the school's network will be regularly checked by the Instructional Technology Department.
15. Other than e-Boards and curriculum/course related blogs, web pages or through district issued e-mail accounts, social interactions between teachers and students are prohibited.

continued: <u>Network Etiquette and Privacy</u>

16. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

<u>Additional Guidelines</u>

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the Instructional Technology Department.

<u>Services</u>

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

<u>Network Security</u>

Users are expected to inform the District Administrator of Instructional Technology immediately if a security breach is identified. Do not demonstrate this problem to other users. Users must login with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

<u>Physical Security</u>

Staff users are expected to ensure that portable equipment such as laptops, digital cameras, iPads, iPod Touches and remote responders are securely locked away when they are not being used.

<u>Media Publications</u>

For the safety of our students, District employees should follow these guidelines when posting student-related information to the District's Web site:

- Documents/pictures may not include student last names.
- Family information (address, telephone number, e-mail address, etc.) may not be posted.
- Student location information (schedule, after-school activity participation, bus stop, etc.) may not be posted.

Publishing includes, but is not limited to:
- the school website/eBoards/blogs/wikis
- web broadcasting
- online newspapers

DEER PARK STAFF AGREEMENT FORM

After reading the Deer Park UFSD Acceptable Use Policy, please complete this form to indicate that you agree with the terms and conditions outlined in the above AUP document and agree to compliance with needed future revisions. **Your signature is required before access may be granted to the Deer Park UFSD network**.

As a staff member of Deer Park UFSD and a user of the computer network, I have read and hereby agree to comply with the Deer Park UFSD Acceptable Use Policy.

Staff Name (Please Print):   _____

Staff's School: _____

Staff Signature: _____

Date: _____