DEER PARK UNION FREE SCHOOL DISTRICT
INSTRUCTIONAL TECHNOLOGY

41 Homer Avenue • Deer Park, New York 11729
Phone: (631) 274-4380 • Fax: (631) 274-8852

Eva J. Demyen
Superintendent

Christopher Kauter
District Administrator for
Instructional Technology

Dear Parent/Guardian:

As a new school year begins, you are required to review the Deer Park School District's Acceptable Use Policy (AUP) with you and your child. The AUP requires that every student who accesses the district's computer network and uses the Internet during school is aware of the procedures of the school district. The AUP is enclosed with this letter and should be read by both parent/guardian and student. In accordance with new procedures, you are **not** required to sign and return the form.

Through the district's computer network, students have access to a wealth of databases and educational resources worldwide. The Deer Park School District maintains a web filter that is designed to block access to inappropriate websites; however, keep in mind that no web filter is 100% effective. Our staff will remain vigilant in monitoring student access to the Internet and inform my office of potentially inappropriate websites, which we can block. As a district, we believe that the benefits to the students from access to the Internet, in the form of educational resources and opportunities for collaboration exceed the disadvantages. District personnel will continue to provide students with computer and Internet safety lessons to ensure that our students have the tools they need to be safe and successful learners in the 21st Century.

Please review the AUP with your child. You may deny internet access to your child and the use of computer software intended for educational purposes. Parents who wish their child be denied these services will make a formal request in writing to the Superintendent of Schools. Failure to make such request will be implied consent for your child to access the district's computer network and the Internet.

Best regards,

Christopher Kauter
District Administrator
Instructional Technology

CC: Ms. Eva Demyen, Superintendent
Board of Education

8630-R 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

- The Superintendent of Schools shall designate a District Administrator of IT to oversee the district's computer network.
- The District Administrator of IT shall monitor and examine all network activities, as appropriate, to ensure proper use of the system. He/she shall maintain an updated inventory of all computer hardware and software resources.
- The District Administrator of IT shall develop and implement procedures for data back up and storage. These procedures will facilitate the disaster recovery and notification plan and will comply with the requirements for records retention in compliance with the district's policy on School District Records (1120); taking into account the use of onsite storage and storage in the cloud.
- The District Administrator of IT shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The District Administrator of IT shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations (including policy 4526, Computer Use in Instruction) governing use of the district's network.
- The District Administrator of IT shall take reasonable steps to protect the network from viruses or other software and network security risks that would comprise the network or district information.
- 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.
- Consistent with applicable internal controls, the Assistant Superintendent of Business in conjunction with the District Administrator of IT will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

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 IT.
- 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 staff and third party 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 and must be of sufficient complexity as determined by the district.
- Only those network users with permission from the District Administrator of IT 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.
- All network users are expected to take reasonable precaution to secure district information stored on devices they use, including maintaining responsible custody over computer resources, ensuring no unauthorized use of district devices, and exercising prudent judgement when browsing the internet and opening email.

- 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 staff and third party 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.
- 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 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.
- Exhibiting careless behavior with regard to information security (e.g., sharing or displaying passwords, leaving computer equipment unsecured or unattended, etc.).

V. No Privacy Guarantee

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. Sanctions

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. District Responsibilities

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 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. Disposal of district computer resources shall ensure the complete removal of district information, or the secure destruction of the resource. 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. Network Etiquette and Privacy

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 encourage 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 IT.

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 IT. 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.

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.

Network Security

Users are expected to inform the District Administrator of IT 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.

Physical Security

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

Media Publications

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

Adoption Date: January 22, 2008

First Reading: August 25, 2009

Adoption Date: September 22, 2009

First Reading: March 19, 2013

Adoption Date: April 23, 2013

First Reading: August 5, 2014

Adoption Date: August 26, 2014

First Reading: March 8, 2016

Adoption Date: March 22, 2016

Adoption Date: May 10, 2016

First Reading: July 26, 2016

Adoption Date: August 30, 2016