SUNNYSIDE UNION ELEMENTARY SCHOOL
STUDENT ACCEPTABLE USE POLICY

INTRODUCTION

It is essential that students and their parents you understand their privileges and responsibilities when using Sunnyside Union Elementary School District computer network. The Student Acceptable Use Policy ("AUP") describes the computer network and explains the privileges and responsibilities associated with use of the computer network by students. All District students are required to read and sign this document. An electronic version of this document is available on the District website.

CONCEPTS AND ROLES

ROLE OF THE GOVERNING BOARD

The Governing Board intends that technological resources provided by the district be used in a safe, responsible, and proper manner in support of the instructional program and for the advancement of student learning.

The Governing Board recognizes the harmful effects of bullying on student learning and school attendance and desires to provide safe school environments that protect students from physical and emotional harm. District employees shall establish student safety as a high priority and shall not tolerate bullying of any student.

ROLE OF THE SCHOOL OFFICIALS

School officials shall notify students and parents/guardians about authorized uses of district computers, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with district regulations and the district's Acceptable Use Agreement.

School officials, with input from students and appropriate staff, shall regularly review and update this policy, and other relevant procedures to enhance the safety and security of students using the District's technological resources and to help ensure that the District adapts to changing technologies and circumstances.

School officials shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced.
To reinforce these measures, school officials shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision.

School officials shall establish regulations to address the safety and security of students and student information when using email, chat rooms, and other forms of direct electronic communication.

School officials shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Student use of district computers to access social networking sites is prohibited. To the extent possible, school officials shall block access to such sites on district computers with Internet access.

ROLE OF TEACHERS AND MEDIA SPECIALISTS

All instructional staff shall receive a copy of this Acceptable Use Agreement, and the related board policies and administrative regulations, describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All students using these resources shall receive instruction in their proper and appropriate use.

ROLE OF PARENTS/GUARDIANS

Acceptable Use Agreement

Before a student is authorized to use the district's technological resources, the student and his/her parent/guardian shall sign and return the Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree not to hold the district or any District staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They shall also agree to indemnify and hold harmless the district and district personnel for any damages or costs incurred.

ROLE OF STUDENTS

Obligations and Responsibilities

Students are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, the user obligations and responsibilities specified below, and the district's Acceptable Use Agreement.

1. The student in whose name an online services account is issued is responsible for its proper use at all times. Students shall keep personal account numbers and passwords private and shall only use the account to which they have been assigned.

2. Students shall use the District's system safely, responsibly, and primarily for educational purposes.

3. Students shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

4. Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, and appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors.

5. Unless otherwise instructed by school officials, students shall not disclose, use, or disseminate personal identification information about themselves or others when using email, chat rooms, or other forms of direct electronic communication. Students also shall be cautioned not to disclose such information by other means to individuals contacted through the Internet without the permission of their parents/guardians.

6. Personal information includes the student's name, address, telephone number, Social Security number, or other personally identifiable information.

7. Students shall not use the system to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

8. Students shall not use the system to engage in commercial or other for-profit activities.

9. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.

10. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Any materials utilized for research projects should be given proper credit as with any other printed source of information.

11. Students shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

12. Students shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or use another individual's identity.

13. Students shall report any security problem or misuse of the services to school officials.

14. The District reserves the right to monitor use of the district's systems for improper use without advance notice or consent. Students shall be informed that computer files and electronic communications, including email, are not private and may be accessed by the district for the purpose of ensuring proper use.

Accountability
Whenever a student is found to have violated Board policy, administrative regulation, or the District's Acceptable Use Agreement, school officials may cancel or limit a student's user privileges or increase supervision of the student's use of the district's technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

Cyber bulling
No student or group of students shall, through physical, written, verbal, or other means, harass, sexually harass, threaten, intimidate cyber bully, cause bodily injury to, or commit hate violence against any other student or school personnel.

Cyber bullying includes the transmission of harassing communications, direct threats, or other harmful texts, sounds, or images on the Internet, social media, or other technologies using a telephone, computer, or any wireless communication device. Cyber bullying also includes breaking into another person's electronic account and assuming that person's identity in order to damage that person's reputation.

Students may submit to a teacher or administrator a verbal or written complaint of conduct they consider to be bullying.

Complaints of bullying shall be investigated and resolved in accordance with site-level grievance procedures specified in Board policy and administrative regulations
.
When a student is reported to be engaging in bullying off campus, school officials shall investigate and document the activity and shall identify specific facts or circumstances that explain the impact or potential impact on school activity, school attendance, or the targeted student's educational performance.

When the circumstances involve cyber bullying, individuals with information about the activity shall be encouraged to save and print any electronic or digital messages sent to them that they feel constitute cyber bullying and to notify a teacher or school official so that the matter may be investigated.

If the student is using a social networking site or service that has terms of use that prohibit posting of harmful material, school officials also may file a complaint with the Internet site or service to have the material removed.

Any student who engages in bullying on school premises, or off campus in a manner that causes or is likely to cause a substantial disruption of a school activity or school attendance, shall be subject to discipline, which may include

suspension or expulsion, in accordance with district policies and regulations. Provision for educating minors about inappropriate online behavior, including interacting with other individuals on social networking websites, chat rooms and cyber-bullying awareness and response is addressed at each school site.

PRIVACY AND CONFIDENTIALITY

Both student and employee records are protected by various State and Federal laws. Both students and employees have a responsibility to safeguard confidential information from unauthorized persons. Students shall not seek to access or use confidential information for their own unauthorized purposes. Students must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, magnetic tape, email, network storage, etc.), paper, photograph, and microfiche information. Included under this precaution is the disposal of any confidential materials. Students may not use school technology for commercial purposes, including auctioning, selling offering, providing or purchasing goods or services for personal use. Students who fail to follow rules and procedures relating to confidentiality may lose their technology privileges, and/or be subjected to disciplinary procedures.

GUIDELINES FOR SPECIFIC TECHNOLOGY RESOURCES

Overview

The District has created extensive networks with information and computing resources for staff and student use. These resources are provided to allow students and others in the District to perform tasks effectively in meeting the goals and needs for which the District has established.

By nature, design, and function, the District's computer network and resources must provide a relatively "open" environment. While automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources, the primary responsibility for maintaining the security of this information and its resources lies with the student.

Improper use of any of these resources can cause problems related to the needs of some or all students in the District. Violation of specific Local, State, and Federal laws may call for prosecution under the law including fines and imprisonment. The District may take disciplinary action against students for misuse of computer, network, and information resources.

USE OF DISTRICT LAPTOP COMPUTERS

Laptop computers that are issued to students are provided for the purpose of preparing/delivering school work for the District. With the convenience of portability comes an increased risk of theft, loss, or damage. Students are expected to take all reasonable precautions to keep laptops issued to them safe and secure. When transporting laptops off campus, please take care to not leave them in unattended automobiles, hot or damp places, or where there is an increased risk of damage or theft. Students are to follow established District checkout procedures for taking their laptop home overnight, on weekends, and over holidays and breaks. Students who choose to take their laptop home must have homeowner's/renter's insurance covering damage or loss of the equipment. District insurance is in force while the machine is on campus. Misuse, abuse, neglect, willful damage, transferred to another school, expelled or violation of district policy while using a laptop shall be grounds for the District to request the laptop's return.

USE OF PERSONALLY OWNED SOFTWARE OR EQUIPMENT

The District attempts to ensure that all hardware and software meet specific standards which will operate without causing disruption of the District's computer and network resources. Therefore, the use of personally owned software or software that can be downloaded from the Internet as well as personally-owned computer hardware is not permitted.

SOFTWARE COPYRIGHT LAW

Violations of copyright law have the potential of costing the District millions of dollars. Students are prohibited from installing any software. Students not install software licensed for one workstation on multiple machines. Inappropriate use of software may lead to disciplinary action. Violation of copyright law is a felony and may result in any

combination of disciplinary action and/or prosecution and fines including litigation costs and payment of damages under applicable local, State, and Federal statutes.

USE OF THE INTERNET AND INTRANET

Internet

The Internet provides an extremely valuable resource for learning and communicating with people throughout the world. It can be a marvelous tool to enhance student education and productivity. Unfortunately, the Internet also contains a large amount of information that is inappropriate for use in an educational institution.

While it is hoped that student will enjoy the use of Internet resources, it must be emphasized that these resources are provided at District expense to enhance student education effectiveness. Students are not to let personal use of the Internet encroach on or displace time spent performing their work duties. Inasmuch as every transaction students complete on the Internet represents to the world our District and everything it stands for, it is imperative that student not use the Internet in such a way as to bring civil or criminal liability or public reproach upon themselves or the District.

Materials obtained from the Internet are copyrighted and, with proper citation, limited educational use is permitted under the Principle of Fair use as contained in U.S. copyright law. These materials may not be redistributed on the Internet or in any other manner without written consent of the copyright owner or as prohibited by law. Materials are protected by copyright whether they bear copyright information or not.

Intranet

The District Intranet is separate and distinct from the Internet. It consists of those networked electronic resources within the Sunnyside Union Elementary School District. Access to many of these resources is public, thus contributing to the Internet at large. Others are accessible only from within the District network or by password. Note that access to District-only resources is not to be shared with others outside the District.

No one may attach to the District network any wired or wireless device without prior approval of the Director of Information Technology. This includes, but is not limited to: computers, laptops, PDAs, hubs/routers or base stations. Furthermore any use of unauthorized means to bypass the districts internet content filter is strictly prohibited (i.e. proxies). Using such proxies may lead to disciplinary action ranging from revoking your internet and email account, up to expulsion.
For security purposes, never leave a session opened and logged in with your account, without logging out and closing the browser window, no matter how brief the interruption.

USE OF COMPUTER RESOURCES

The computing resources of the District are used by thousands of students and employees. In order to ensure that these resources are available and working properly, use of these resources must not negatively impact others.

Students must not attempt to utilize computer systems or their resources for which access has not been granted. Students must not attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer, or network system. Attempts or actions of this nature are a felony and may result in any combination of disciplinary action and/or prosecution and fines including litigation costs and payment of damages under applicable local, State, and Federal statutes.

USE OF NETWORK STORAGE

In addition to network file servers used in a classroom setting, the District provides each student with 1 gigabyte of network storage called an F: Drive (home directory). This space is accessible from anywhere on the Intranet and includes private layers of access. Public and class folders are for disseminating course materials, announcements, and instructional web pages. Students are to observe all applicable laws (including copyright) and District policies in

the use of shared directories. Storage and account access may not be shared or used for any purpose other than the direct support of instruction.

COMPUTER ACCOUNTS

User I.D.s and Passwords

In order for students to utilize the District's computer and network resources, each student will be assigned a "user id" and password. Students may be provided with access levels which allow them to view, create, alter, delete, print, and transmit information. Use of district technology, network, and internet services does not create any expectation of privacy. The school reserves the right to search and/or monitor any information created, accessed, sent, received, and/or stored in any format by students on the district computer and network.

This means that it is extremely important that students use a password that cannot be guessed by others through knowledge about you. For example, never use personal names such as nickname or pets or names that begin or end with numbers. Never use Social Security numbers, bank PIN numbers, words which can be found in any dictionary, names spelled backwards, or adjacent keys on a computer keyboard (i.e., QWERTY). All of the above provide an easy way for a "cracker" to break into a computer system and, using your rights and privileges, cause damage and destruction. Students must also never write down their user id or password unless it is stored in a location away from the school site. Even then, it should be written such a way that no clue is given as to the purpose for its use. Please contact the Information Technology Services if you suspect unauthorized access to a school account.

Security

Students are responsible for maintaining the security of personal accounts and may not release user I.D. or passwords for use by any other individual. Failure to do so by releasing this information to another individual may be considered false representation and result in disciplinary action.
Students should never leave a workstation unattended while signed on to any account; doing so provides an opportunity for another person to engage inappropriate conduct using another student's identity.

COMPUTER VIRUSES

Despite the development of new technologies to combat malicious viruses, worms, and other damaging programs that attack computers and networks, these problems persist. The District attempts to maintain anti-virus software in order to minimize the impact of these viruses, but it is the responsibility of each student to take precautions to protect the computer network.
Students should not open email attachments sent from an unknown or unrecognized source.
Likewise, do not download any software from the Internet unless directed to by teacher and authorized by the Information Technology Department. It is not unknown for even a very respectable company to unknowingly release products which include hidden or unknown viruses. Do not share any downloaded software with others until it has been verified that it does not contain viruses.

ELECTRONIC MAIL

The District encourages the use of electronic mail (email) to enhance communication and school activities. The following policies are necessary to ensure appropriate use and to prevent or limit disruptions to school activity and computer services. Please read carefully:

Cautions

The nature of electronic mail at this date makes it susceptible to misuse. Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both within the District as well as externally throughout the world.

In addition, while email accounts may be password protected, it is up to the individual user to ensure that a password is set and that the password is one that cannot be easily guessed or "hacked".

Users of the District's email services need to be aware that use of these services is a privilege granted with the expectation that it will be used for school purposes and in a courteous manner similar to other forms of communication. All email sent or received by individuals through the District is the property of the District and may be requested by your principal and examined with just cause.

There is no guarantee that email received was in fact sent by the purported sender, since it is a simple matter, although a violation of this policy, to disguise the sender's identity. Furthermore, email that is forwarded may be modified by the forwarder. As with any document, if you receive a message which appears unusual or which you feel may be questionable, check with the purported sender to verify authorship and authenticity.

While the District does not have the time nor inclination to monitor or read all individual email messages, in the event that questionable or inappropriate use is suspected or known, such email may be examined and may be cause for disciplinary action ranging from revoking your email account up to expulsion. Users should also be aware that in the general course of school, System Administrators and email operators may require observation of messages in order to verify system operation.

SPAM
The District maintains a system for limiting the amount of unwanted or offensive email received from the Internet. Known as SPAM, much of this email is automatically generated by computer programs and is often used to propagate computer viruses, or distribute pornography and fraudulent business offerings. The email may appear to have come from a trusted address and others may receive such messages that falsely appear to have come from you. The District's email filtering system cannot eliminate all SPAM and it is possible that benign messages may occasionally be blocked. If/when expected email has been blocked, please notify your teacher.

Personal Use
Private or personal non-commercial use of the District's email is NOT permitted.

State, Federal, and Copyright Laws
In addition to this policy, use of the District's email services is subject to all applicable Federal and State communications and privacy laws as well. In particular, users need to be aware that attaching programs, sound, video, and images to email messages may violate copyright laws, and data files containing student information is subject to all privacy laws.

Restrictions
- Electronic mail may not be used for:
- Unlawful activities
- Commercial purposes
- Personal financial gain
- Use that violates this policy or other State and Federal policies
- Any form of harassment
- Chain letters, sending or forwarding
- Spam mail, that is, to exploit list servers or other broadcast systems which amplify widespread distribution of unsolicited email
- File storage. (Use F: Drive.)
- Mail bombs, that is, to re-send the same email repeatedly to one or more recipients with the intent to interfere with the recipient's use of email
- Any other use which interferes with computing facilities and services of the District or its employees
- Personal fund-raising

- Jokes, etc.

Representation
Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the District unless they are appropriately authorized, explicitly or implicitly, to do so. Where appropriate and based on context, an appropriate disclaimer would be, "These are my own statements and views and do not represent those of the Sunnyside Union Elementary School District."

False Identity
Student shall not employ a false identity in sending email or alter forwarded mail out of the context of its original meaning.

Misuse of Computing Services
Email services shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive strain on District computing facilities, or cause interference with others' use of email, email systems, or any computing facilities or services. For example, attaching large files over 1 megabyte and sending these to multiple users or repeatedly to the same user is a violation of this policy. The District's email system is not designed for file storage. Such use is prohibited. Please use your F: Drive for storing or archiving files.

Security and Confidentiality
The confidentiality of electronic mail cannot be assured. Users should exercise extreme caution in using email to communicate confidential or sensitive material.

Virus Dangers
As mentioned, proper precautions must be taken to guard against the infection of computers and files by viruses. Likewise, using email attachments to distribute viruses and/or worms and other damaging software is common-place today. Never open email or attachments unless you are expecting them. Even when a known person sends an attachment, the safest practice is to verify that anti-virus software is being used by the sender before opening the attachment.

Non-District Email Accounts
Students who email accounts other than those hosted by the District shall emphasize that the District has no control over such accounts. Nevertheless, students should report any and all suspicious or threatening email received.

OTHER SERVICES
Please note that this policy addresses issues common to all students. Other specific policies may apply to those studying in specialized environments or completing specialized tasks.
If you have any questions about this or other policies, please contact school officials.