All Personnel

Employee Use of Technology

Employee Account Agreement

Employee Name _____

Position _____

School/Department _____

I have read the Stockton Unified District Employee Acceptable Use Policy and Employee Security Agreement. I agree to follow the rules contained in this policy. I understand that if I violate the rules, I may face disciplinary action in accord with board policy and collective bargaining agreements.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims or damages of any kind whatsoever arising from my use of, or inability to use, the district system, including, but not limited to, claims that may arise from the unauthorized use of the system to offer, provide, or purchase products or services.

Signature _____ Date _____

****

(This space reserved for System Administrator)

Assigned Use Name: _____

Assigned Temporary Password: _____

All Personnel

Employee Use of Technology

Employee Acceptable Use Policy (AUP)

Stockton Unified School District ("the District" or "Stockton") is now offering Internet access for employee use. This document contains the Acceptable Use Policy for your use of Stockton's Technology Network.

Educational Purpose

Stockton's Technology Network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high quality self discovery activities. Stockton's Technology Network has not been established as a public access service or a public forum. The District reserves the right to place reasonable restrictions on the material you access or post through the system. You are also expected to follow the rules set forth in the AUP and the law in your use of Stockton's Technology Network.

You may not use Stockton's Technology Network for commercial purposes. This means you may not offer, provide, or purchase products or services through Stockton's Technology Network. You may not use Stockton's Technology Network for political activities which do not serve or promote an authorized educational purpose of the District. Under no circumstances shall you use Stockton's Technology Network to: conduct political activities, solicit political campaign support or contributions, or reproduce, post, distribute or disseminate political campaign materials

"The District may suspend any individual's access to the District system upon any violation of the AUP."

District Responsibilities

The Superintendent or designee will serve as the coordinator to oversee the District system. A Designated Site Administrator serving as the building level coordinator for the District system will approve building level activities, ensure teachers receive proper training in the use of the system and the requirements of this Policy, establish a system to ensure adequate supervision of students using the system, maintain executed user agreements, and be responsible for interpreting the District Acceptable Use Policy at the building level.

All Personnel

Employee Use of Technology

Employee Acceptable Use Policy (AUP)
(Continued)

The Director of Information Services will establish a process for setting up individual and class Accounts, set quotas for disk usage on the system, establish a retention schedule, establish a District virus protection process, and security policies.

UNACCEPTABLE USES

The following uses of Stockton's Technology Network are considered unacceptable:

1. Illegal Activities

You will not attempt to gain unauthorized access to Stockton's Technology Network or to any other computer system through Stockton's Technology Network or go beyond you authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing." You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. You will not use Stockton's Technology Network to engage in any other illegal act, such as, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

2. System Security

You are responsible for your individual account and should take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person. You will immediately notify the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access. You will avoid the inadvertent spread of computer viruses by following the District virus protection procedures if you download software.

3. Inappropriate Language

Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages. You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. You will not post information that could cause damage or a danger of disruption. You will not engage in personal attacks, including but not limited to, attacks that could be construed as disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion or political beliefs. You will not

All Personnel

Employee Use of Technology

Employee Acceptable Use Policy (AUP)
(Continued)

harass another person. Harassment means a knowing and willful course of conduct directed at a specific person, group, or entity which seriously alarms, annoys, or terrorizes that person, group, or entity, and which serves no legitimate purposes.

If you are told by a person to stop sending messages to them, you must stop. You will not knowingly or recklessly post false or defamatory information about a person or organization.

4. Respect for Privacy

You will not repost a message that was sent to you privately without permission of the person who sent you the message. You will not post private information about another person.

5. Respecting Resource Limits

You will use the system only for educational and career development activities and limited, high quality, self discovery activities. High quality means activities not in conflict with this Policy. You will not download large files unless absolutely necessary. If necessary, you will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to your personal computer. You will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people. You will check your email frequently, delete unwanted messages promptly, and stay within your email quota. You will subscribe only to high quality discussion group mail lists that are relevant to education or career development.

6. Plagiarism and Copyright Infringement

You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writing of others and presenting them as if they were yours. You will respect the rights of copyright owners. Copyright infringement occurs when you reproduce a work that is protected by a copyright without authorization. If a work contains language that specifies appropriate use of that work, you must follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing.

7. Inappropriate Access to Material

You will not use Stockton's Technology Network to access material that is profane or obscene (i.e. pornography), that advocates illegal acts, or that advocates violence or unlawful discrimination towards other people based on but not limited to, their race, national origin, sex,

All Personnel

Employee Use of Technology

Employee Acceptable Use Policy (AUP)
(Continued)

sexual orientation, age, disability, religion, or political beliefs (i.e. hate literature). A special exception may be made if the purpose of your access is to conduct research. Prior to such research employees will notify their designated site administrator. If you mistakenly access inappropriate information, you should immediately notify another District employee. This will protect you against a claim that you have intentionally violated this policy.

YOUR RIGHTS

Employees should be aware that computer files and communications over electronic networks, including email and voice mail, are not private. This technology should not be used to transmit confidential information about students, employees, or District affairs.

To ensure proper use, the Superintendent or designee may monitor the District' technological resources, including email and voice mail systems, at any time without advance notice or consent. If passwords are used, they must be known to the Superintendent or designee so that he/she may have system access when the employee is absent.

LIMITATION OF LIABILITY

The District makes no guarantee that the functions or the services provided by or through the District system will be error free or without defect. The District will not responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

TECHNICAL SERVICES PROVIDED THROUGH DISTRICT SYSTEM

Email

Email will allow employees to communicate with people from throughout the world. Users will also be able to subscribe to mail lists to engage in group discussions related to educational subjects.

All Personnel

Employee Use of Technology

Employee Acceptable Use Policy (AUP)
(Continued)

World Wide Web

The Web provides access to a wide range of information in the form of text, graphics, photographs,
video, and sound, from throughout the world. The Web is a valuable research tool for students and employees.

Telnet

Telnet allows the used to log in to remote computers.

File Transfer Protocol (FTP)

FTP allows users to download large files and computer software.

Newsgroups

Newsgroups are discussion groups that are similar to mail lists. The District will provide access to selected newsgroups that relate to subjects that are appropriate to the educational purpose of the system.

Internet Relay Chat (IRC)

IRC provided the capability of engaging in "real-time" discussions. The District will provide access to IRC only for specifically defined educational activities.

Blocking software

The District will subscribe to a service to provide blocking software.

All Personnel

Employee Use of Technology

Employee Security Agreement

With the introduction of Internet access to Stockton Unified School District's wide area network, security of existing systems is of paramount concern. Currently any workstation on the wide area network is an access point for District records and information. These workstations are located in offices where control can be exercised and can be considered secure. The addition of Internet access to the network allows any workstation anywhere in the world access to our data. This is where identification and authentication of people using our system becomes very important.

The connection to the Internet being built has protection against random access of any systems inside Stockton Unified School District, while allowing access to authorized users. The system's design allows an employee to use any workstation, anywhere in the world to access the system as if they were in their office. The only thing keeping an unauthorized user (hacker) from the same access is the identification and authorization codes assigned for access. Should an unauthorized user gain knowledge of identification and authorization codes, they have system access. Identification and authorization codes are currently managed by Information Services (IS). Each site has designated a security supervisor whose responsibilities include: identification of new users, system access to new users, and levels of user access. IS assigns to all new users identification codes and assists the new user in establishing the authorization passwords. This is similar to the account number and PIN number used for an ATM card. The identification code and password are the only way the system can verify an authorized individual is attempting to access the system. User identification codes and passwords are to be treated exactly the same as a bank card. Nobody but the identified user should have knowledge of either one.

The following policies have been established to protect network security:

1. Identification codes and passwords are not to be written down.
2. Do not tell anyone a password.
3. Choose passwords that are not easily associated with the user.
4. Change passwords frequently.
5. Do not let others observe when entering codes and passwords.
6. All new files added to a computer on the network will be virus scanned prior to use.

All Personnel

Employee Use of Technology

Employee Security Agreement
(Continued)

Any computer connected to the network with a modem presents an additional security risk to the system. These modems must be approved and registered with the Site Security Supervisor. Any modem connected to the system found to be unregistered will be removed by the Site Security Supervisor.

Site security supervisors are also responsible for informing IS when users are no longer allowed access to a system. This may be due to employee termination or reassignment.

All Personnel

Employee Use of Technology

Guest Account Agreement

Name _____

Address _____

Phone _____

I have read the Stockton Unified School District Acceptable Use Policy and Security Agreement. I agree to follow the rules contained in this Policy. I understand my account may be terminated as follows:

My account may be terminated at any time upon notice tome. In this event, I will be given the opportunity to remove my personal files.

If my account is unused for more than 30 days, it may be terminated and my personal files removed without notice.

The purpose for which this account is provided is: _____

_____

I agree to limit my use of my account to activities related to the above stated purpose.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims or damages of any kind whatsoever arising from my use of, or inability to use, the District system, including, but not limited to, claims that may arise from the unauthorized use of the system to offer, provide, or purchase products or services.

Signature _____ Date _____

Guest Account Authorized by _____

School or Department _____

All Personnel

Employee Use of Technology

Guest Acceptable Use Policy (AUP)

Stockton Unified School District ("the District" or "Stockton") is now offering Internet access for limited guest use. This document contains the Acceptable Use Policy for your guest use of Stockton's Technology Network.

Educational Purpose

Stockton's Technology Network has been established for a limited educational purpose. The term "educational purpose" include classroom activities, career development, and limited high quality self discovery activities. Stockton's Technology Network has not been established as a public access service or a public forum. The District reserves the right to place reasonable restrictions on the material you access or pose through the system. You are also expected to follow the rules set forth in the AUP and the law in your use of Stockton's Technology Network.

You may not use Stockton's Technology network for commercial purposes. This means you may not offer, provide, or purchase products or services through Stockton's Technology Network. You may not use Stockton's Technology Network for political activities which do not serve or promote an authorized educational purpose of the District. Under no circumstances shall you use Stockton's Technology Network to: conduct political activities, solicit political campaign support or contributions, or reproduce, post, distribute or disseminate political campaign materials.

"The District may suspend any individual's access to the District system upon any violation of the AUP."

District Responsibilities

The Director of Information Services will establish a process for setting up guest accounts, set quotas for disk usage on the system, establish a retention schedule, establish a District virus protection process, and security policies.

All Personnel

Employee Use of Technology

Guest Acceptable Use Policy (AUP)

(Continued)

UNACCEPTABLE USES

The following uses of Stockton's technology Network are considered unacceptable:

1. **Illegal Activities**

You will not attempt to gain unauthorized access to Stockton's Technology Network or to any other computer system through Stockton's Technology Network or go beyond your authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing". You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. You willnot use Stockton's Technology Network to engage in any other illegal act, such as, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

2. **System Security**

You are responsible for your individual account and should take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person. You will immediately notify the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access. You will avoid the inadvertent spread of computer viruses by following the District virus protection procedures if you download software.

3. **Inappropriate Language**

Restrictions against inappropriate language apply to public messages, private messages, and material posed on Web pages. You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. You will not post information that could cause damage or a danger of disruption. You will not engage in personal attacks, including, but not limited to, attacks that could be construed as disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. You will not harass another person. Harassment means a knowing and willful course of conduct directed at a specific person, group, or entity which seriously alarms, annoys, or terrorizes that person, group, or entity, and which serves no legitimate purpose. If you are told by a person to stop sending

All Personnel

Employee Use of Technology

Guest Acceptable Use Policy (AUP)

(Continued)

messages to them, you must stop. You will not knowingly or recklessly post false or defamatory information about a person or organization.

4. **Respect for Privacy**

You will not repost a message that was sent to you privately without permission of the person who sent you the message. You will not post private information about another person.

5. **Respecting Resource Limits**

You will use the system only for educational and career development activities and limited, high quality, self discovery activities. High quality means activities not in conflict with this Policy. You will not download large files unless absolutely necessary. If necessary, you will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to your personal computer. You will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people. You will check your email frequently, delete unwanted messages promptly, and stay within your email quota. You will subscribe only to high quality discussion group mail lists that are relevant to education or career development.

6. **Plagiarism and Copyright Infringement**

You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. You will respect the rights of copyright owners. Copyright infringement occurs when you reproduce a work that is protected by a copyright without authorization. If a work contains language that specifies appropriate use of that work, you must follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing.

7. **Inappropriate Access to Material**

You will not use Stockton's Technology Network to access material that is profane or obscene (i.e. pornography), that advocates illegal acts, or that advocates violence or unlawful discrimination towards other people based on, but not limited to, their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs (i.e. hate literature). If you mistakenly access inappropriate information, you should immediately notify a District employee. This will protect you against a claim that you have intentionally violated this Policy.

All Personnel

Employee Use of Technology

Guest Acceptable Use Policy (AUP)

(Continued)

YOUR RIGHTS

Guests should be aware that computer files and communications over electronic networks, including email and voice mail, are not private. This technology should not be used to transmit confidential information about students, employees, or District affairs.

To ensure proper use, the Superintendent or designee may monitor the district's technological resources, including email and voice mail systems, at any time without advance notice or consent.

LIMITATION OF LIABILITY

The District makes no guarantee that the functions or the services provided by or through the District system will be error free or without defect. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

TECHNICAL SERVICES PROVIDED THROUGH DISTRICT SYSTEM

Email

Email will allow guests to communicate with people throughout the world. Users will also be able to subscribe to mail lists to engage in group discussions related to educational subjects.

World Wide Web

The Web provides access to a wide range of information in the form of text, graphics, photographs, video, and sound, throughout the world. The Web is a valuable research tool for students and employees.

Telnet

Telnet allows the user to log in to remote computers.

All Personnel

Employee Use of Technology

Guest Acceptable Use Policy (AUP)

(Continued)

File Transfer Protocol (FTP)

FTP allows users to download large files and computer software.

Newsgroups

Newsgroups are discussion groups that are similar to mail lists. The District will provide access to selected newsgroups that relate to subjects that are appropriate to the educational purpose of the system.

Internet Relay Chat (IRC)

IRC provides the capability of engaging in "real-time" discussions. The District will provide access to IRC only for specifically defined educational activities.

Blocking software

The District will subscribe to a service to provide blocking software.

All Personnel

Employee Use of Technology

Guest Security Agreement

With the introduction of Internet access to Stockton Unified School District's wide area network, security of existing systems is of paramount concern. Currently any workstation on the wide area network is an access point for District records and information. These workstations are located in offices where control can be exercised and can be considered secure. The addition of Internet access to the network allows any workstation anywhere in the world access to our data. This is where identification and authentication of people using our system becomes very important.

The connection to the Internet being built has protection against random access of any systems inside Stockton Unified School District, while allowing access to authorized users. The system's design allows an employee to use any workstation anywhere in the world to access the system as if they were in their office. The only thing keeping an unauthorized user (hacker) from the same access is the identification and authorization codes assigned for access. Should an unauthorized user gain knowledge of identification and authorization codes, they have system access.

Identification and authorization codes are currently managed by Information Services (IS). Each site has designated a security supervisor whose responsibilities include: identification to new users, system access of new users, and levels of user access. IS assigns to all new users identification codes and assists the new user in establishing the authorization passwords. This is similar to the account number and PIN number used for an ATM card. The identification code and password are the only way the system can verify an authorized individual is attempting to access the system. User identification codes and passwords are to be treated exactly the same as a bank card. Nobody but the identified user should have knowledge of either one.

The following policies have been established to protect network security:

1. Identification codes and passwords are not to be written down.
2. Do not tell anyone a password.
3. Choose passwords that are not easily associated with the user.
4. Change passwords frequently.
5. Do not let others observe when entering codes and passwords.
6. All new files added to a computer on the network will be virus scanned prior to use.

All Personnel

Employee Use of Technology

Guest Security Agreement
(Continued)

Any computer connected to the network with a modem presents an additional security risk to the system. These modems must be approved and registered with the Site Security Supervisor. Any modem connected to the system found to be unregistered will be removed by the Site Security Supervisor.

Site security supervisors are also responsible for informing Information Services when users are not longer allowed access to a system. This may be due to employee termination or reassignment.