Farmington Public Schools Information Technology
CONFIDENTIAL NON-DISCLOSURE and USE AGREEMENT
Contractors/Sub Contractors
Network Access/Remote Access Connectivity

As a guest staff being provided through a contractor/sub contractor of Farmington Public Schools you are being provided access to the Farmington Public Schools network to allow you the ability to perform your job as _____ within the Farmington Public Schools data/voice/video network.

As a contractor/subcontractor working with individuals of the Farmington Public Schools you may have access to areas in the network and/or access to information that is confidential.

As a contractor or subcontractor of Farmington Public Schools and by signing this ***Confidential Non-Disclosure and Use Agreement,*** you agree to treat all the District's Employee and Student information as confidential data. You also agree not to at any time represent yourself as an employee of the Farmington Public Schools.

You also agree:

1. Not to disclose or publish any confidential data including, but not limited to, Employee and Student information that is made available or accessible to you as part of this assignment with Farmington Public Schools. All contractors and subcontractors are to be aware of their duty under the **Family Educational Rights and Privacy Act (FERPA)** to keep any and all student record information confidential. As a contractor/subcontractor for Farmington Public Schools this ***Confidential Non-Disclosure and Use Agreement*** is your notification of this law.

2. Not to remove any data from authorized locations or make any copies of any employee and/or student information.

3. Not to use any data or information for personal use, benefit or gain.

4. To immediately inform the Farmington Public Schools Director of Information Technology if you become aware, suspect or have knowledge that an individual is acting in violation of this Agreement, whether that is another contractor/sub contractor or District employee.

5. That the use of the Farmington Public Schools network is a privilege and that responsible use is required. Some examples of irresponsible use would include, but not be limited to, the placing of unlawful information on the system, or information which conveys an offensive, profane, sexually suggestive message, or harasses or disturbs by pestering or tormenting, including, but not limited to, intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity in either public or, upon registration of complaint, private messages or other systems that are accessed through the Farmington Public Schools network. That Farmington Public Schools will be the sole arbiter of what constitutes irresponsible use.

6. That the Farmington Public Schools network may not be used for conduct that embarrasses, harms, or in any way distracts from the good reputation of the Farmington Public Schools, its faculty and staff, or any organizations, groups, and institutions with which the Farmington Public Schools network is affiliated. The Farmington Public Schools will be the sole arbiter of what constitutes unacceptable behavior. It also includes illegal or unauthorized entry or attempt to gain access to another's files, computers, or computer systems.

7. That the Farmington Public Schools reserves the right to review any material stored in files to which all users have access and will edit or remove any material which the District, in its sole discretion, believes may be unlawful, conveys an offensive, profane, or sexually suggestive message, or harasses or disturbs by pestering or tormenting, including, but not limited to, intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity. There is no expectation of privacy for any individual who sends, receives, or stores information via the Farmington Public Schools network.

8. That all information services and features on the Farmington Public Schools network are intended for professional use and any commercial or unauthorized use of those materials or services, in any form, is expressly forbidden.

9. That in consideration for the privilege of using the Farmington Public Schools network and in consideration for access to the information contained in it, I release the Farmington Public Schools network and its operators and sponsors, Farmington Public Schools and its faculty and staff, and all organizations, groups and institutions with which the Farmington Public Schools is affiliated, from any claims or liability I may have, of any nature arising from the use, or inability to use, the Farmington Public Schools network.

10. That my access to the Farmington Public Schools network is subject to such rules and regulations of system usage as may be established by the administrators of the system, which may be changed from time to time. Violation of this network agreement may result in disciplinary action.

You also understand that disclosure, transfer or unlawful use of an employee's, student, or other individual's social security number may be a violation of federal and/or state law and that such matters may be referred to the appropriate legal authority.

To prevent the disclosure, transfer, removal, and/or unlawful use of this sensitive data you agree to sign this ***Confidential Non-Disclosure and Use Agreement.*** This signed agreement will be retained by Farmington Public Schools.

I acknowledge receipt of the Farmington Public Schools Technology Network Acceptable Use Policy #4137 and Procedure #4137-1 and agree to comply with them as applicable.

I, _____, have read and understand the ***Confidential Non-Disclosure and Use Agreement*** and above noted policy and procedures. I further understand that my signature indicates our agreement to comply with the above stated terms. Any violation will be handled in accordance with Farmington Public Schools policies, practices and/or procedures including all federal and state laws.

Signature: _____ DATE: _____

Printed Name: _____

Title: _____

Company: _____

FARMINGTON PUBLIC SCHOOLS NETWORK ACCEPTABLE USE TERMS AND CONDITIONS

GENERAL NETWORK INFORMATION

Farmington Public Schools (FPS) Network is a service provided by Farmington Public Schools. The system administrators are employees of Farmington Public Schools and reserve the right to monitor all activity on the FPS Network. All users must submit a signed FPS Network Registration Agreement before obtaining a user account and password.

Because of the complex association between many government agencies and networks, the end user of this network must adhere to strict guidelines. They are provided here so that users, and the parents of users who are under 18 years of age, are aware of their responsibilities. The FPS Network may modify these rules at any time by publishing the modified rule(s) on the FPS Network and at each school's Media Center. Any signature at the end of the FPS Network Registration Agreement is legally binding and indicates the signer has (have) read the Terms and Conditions carefully and understands their significance.

INFORMATION CONTENT & USES OF THE SYSTEM

Users agree not to submit, publish, or display on the Network any information which conveys an offensive, profane, or sexually suggestive message. Users further agree not to harass or disturb by pestering or tormenting, including, but not limited to, intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity.

Users agree not to use the facilities of the FPS Network to conduct any business or business activity. Neither shall they solicit the performance of any activity which is prohibited by law. Users agree not to publish on this Network any information which contains any advertising or any solicitation of other users to use goods or services without the explicit approval of Farmington Public Schools.

Because the Network provides, through connection to Oakland Schools and QUEST, access to other systems around the world, users (and the parent(s) of a user if the user is under 18 years of age) specifically understand that the system administrators and Farmington Public Schools do not have control of the content of information existing on these other systems. Users, who are under 18 years of age and their parents/guardians, are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material. Farmington Public Schools does not control such material. Nor does it condone and nor permit use of these materials on the FPS Network.

Parents of minors having accounts on the Network should be aware of the existence of such materials and monitor home usage of the system. Users accessing such materials over the Network are subject to the discipline of the school/department, Farmington Public Schools Student Code of Conduct and Farmington Public Schools Board of Education Policies. Such activities may also result in termination of the user's account on the FPS Network, as well as suspension or expulsion.

UPDATE USER ACCOUNT INFORMATION

Users must notify FPS Network of any changes in account information.

ONLINE CONDUCT

Any action by a user that constitutes an inappropriate use of the FPS Network, or improperly restricts or inhibits other users from using and enjoying the FPS Network, is prohibited. Transmission of material, information or software in violation of any local, state or federal law is prohibited.

In consideration for the privilege of using the FPS Network and in consideration for access to the information contained in it, users release the FPS Network and its operators and sponsors, Farmington Public Schools and its faculty and staff, and all organizations, groups and institutions with which the Farmington Public Schools is affiliated, from any and all liability or claims of any nature arising from the use, or inability to use, the FPS Network.

FPS Network shall be used for educational purposes only.

CHILDREN'S INTERNET PROTECTION ACT POLICY (C.I.P.A.)

Farmington Public Schools intends that all Internet safety policies and technology protection measures comply with the provisions of the Children's Internet Protection Act (CIPA), 47 USC 254(h), as amended. Accordingly, the Farmington Public Schools shall take all actions necessary and appropriate to implement and enforce the following policies with respect to student access to and use of the Internet through the District's computer network, and in accordance with Farmington Public Schools Student Code of Conduct.

General Warning and Individual Responsibility of Parents and Users. All student users and student parents/guardians are advised that access to the electronic network, including the Internet and World Wide Web, may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet, and must not access these sites. Parents of minors are the first and best source of guidance as to what materials to avoid. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to a teacher or administrator.

Personal Safety. In using the computer network and Internet, including electronic mail (e-mail), and other forms of direct electronic communication, students are advised not to reveal personal information, such as a home address or telephone number. Students are not to use their last name or provide any other information which might allow a person to locate them, unless they first obtain the permission of a supervising teacher. Students are not to arrange a face-to-face meeting with a person the student has only met through the computer network or Internet without the student's parent's permission (unless the student is 18 years or older). Regardless of age, a student should never agree to meet such a person in a secluded place or in a private setting.

Confidentiality of Student Information. No user, shall disclose personally identifiable information concerning students on the Internet without the permission of a parent or guardian, or if the student is 18 or over, the permission of the student. Student users should never disclose private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. The district may release directory information, as defined by District policy 5124, and as permitted by "Permission for Student Photographs & Work to Appear on the Internet" form attached.

Active Restriction Measures. The District and its Internet access provider shall utilize filtering software and/or other technologies to prevent students from accessing materials that are (1) obscene, (2) constitute child pornography, or (3) are otherwise harmful to minors. The District shall also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such material or any other material, which is inappropriate for minors. Internet-filtering software or other technology-based protection systems may be disabled with the permission of an administrator, as deemed necessary and appropriate, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

For purposes of this policy, the term "harmful to minors" shall be defined in the same manner as in the Communications Act of 1934, as amended (47 USC 254) {h} {7} {G}, which means:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

For purposes of enforcing this policy and as for other purposes in the district's operation of its network, the District reserves the right to monitor, inspect, copy, review and store without prior notice any activity of the computer network and Internet access, and any information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District, and no user shall have any expectation of privacy regarding such materials.

NETWORK ETIQUETTE

Users shall abide by generally accepted rules of network etiquette. These include, but are not limited to:

- Be polite. Do not get abusive with messages to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities. There is no expectation of privacy.

- Do not use the network in such a way that it would disrupt the use of the network by other users.
- All communications and information accessible via the network should be respected as private property and should not be accessed without explicit authorization.

ELECTRONIC MAIL

Electronic mail (e-mail) is an electronic message sent by, or to a user, in correspondence with another person having Internet mail access. Messages received on the FPS Network are normally retained for 30 days or until deleted by the recipient. A canceled FPS Network account will not retain its e-mail. Users are expected to remove old messages in a timely fashion. E-mail privacy is not guaranteed.

A. The District System Administrator will determine procedures for retention and removal of all e-mail on the FPS network.

B. The District System Administrator will cooperate fully with district administrators to facilitate internal investigations regarding suspected violations of the network or law.

Farmington Public Schools reserves the right to cooperate fully with local, state or federal officials in any investigation concerning or related to any e-mail transmitted on the FPS Network.

COPYRIGHTED MATERIAL

Each user shall follow all copyright laws regarding the use, duplication, application, distribution and/or repurposing of intellectual property (e.g. software, text, video, visual images, audio/music). Each user shall make certain no copyrighted material is used without explicit permission of the copyright holder (e.g. author, programmer, producer, developer, and publisher).

DISK USAGE

System administrators reserve the right to set quotas for disk usage on the System. A user who exceeds the quota is required to delete files to return to compliance.

SECURITY

Security on any computer system is high priority, especially when the system involves many users. If a user can identify a security problem on the FPS Network, the user must notify a system administrator. The user should not demonstrate the problem to others. Passwords to the system should not be easily guessable by others, nor should they be words which could be found in a dictionary. Passwords should not be shared with any other users or family members. Attempts should not be made to log in to the system using another member's account. Users should

immediately notify a system administrator if their passwords are lost, stolen, or if there is reason to believe that someone has obtained unauthorized access to their accounts. Any user identified as a security risk, or having a history of problems with other computer systems, may be denied access to the FPS Network.

VANDALISM

Vandalism is strictly prohibited, and is defined as any malicious attempt to harm or destroy the data or computer system of another user, whether on the FPS Network, or any of the agencies or other networks that are connected to Oakland Schools or QUEST. Vandalism includes the uploading or creation of computer viruses. It also includes illegal or unauthorized entry to another's files, computers or computer system, or an attempt to gain such access (e.g. hacking). Abuse of Technology constitutes a Level II violation of the Farmington Public School's Student Code of Conduct including suspension or expulsion.

TERMINATION OF ACCOUNT

FPS, or its designee, reserves the right, in its sole discretion, to suspend or terminate the user's access to and use of the FPS Network upon any suspected breach of these Terms and Conditions. Before a suspension or termination or as soon as practicable, the user will be informed of the suspected breach and be given an opportunity to present an explanation.

ENFORCEMENT PROVISIONS

In order to ensure adherence to the Terms and Conditions, Farmington Public Schools reserves the right to monitor all activity on the system and to inspect any files, including e-mail stored on the system. Privacy is not guaranteed.

Violations of the Terms and Conditions will result in disciplinary action according to the policies of the Farmington Public Schools Board of Education and the Student Code of Conduct.

TECHNOLOGY USE GUIDELINES

OPPORTUNITIES

Every student has the opportunity to use available technology resources designated for student access for the purpose of educational growth. The trust that defines the Farmington Public Schools educational community requires that technology resources be used for educational purposes consistent with the mission of the district, unselfishly, with good manners, responsible behavior, and for the good of the community as a whole. These guidelines apply to all technology resources.

RESPONSIBILITES

1. **Authorized usage.** Students using technology as an educational resource shall also accept the responsibility for the preservation and care of that technology. Only those students with appropriate and explicit authorization may use any technology.

   It is the student's responsibility to obtain written permission from an authorized person before removing any technology resource from the school premises. Each student who takes possession of equipment acknowledges that s/he will be the sole operator, whether on or off the school premises.

   It is the student's responsibility to incur no charges when accessing electronic resources (e.g. databases, bulletin boards, e-mail, Internet) unless authorized by the supervising teacher or designated individual. Payments for unauthorized charges are the responsibility of the student. Authorized access is to be limited to district accounts and excludes personal accounts.

2. **School/departmental policies and procedures**. It is the student's responsibility to follow policies and procedures established by each school/department for the use of any technology. It is the student's responsibility to follow the directions of the teacher or designated individual in the use/access of all technology.

   It is the student's responsibility to keep food, drink and other harmful objects away from technological systems as directed by the school/department.

   It is the student's responsibility to monitor content and volume of printed documents as well as their H drive files as directed by the school/department. If multiple copies of a document are needed, a copy machine should be used instead of a printer.

3. **Use of copyrighted intellectual property.** It is the student's responsibility to follow all copyright laws regarding the use, duplication, application, distribution and/or repurposing of intellectual property (e.g. software, text, video visual images, audio/music). It is the student's responsibility to make certain no copyrighted, material is used without explicit permission of the copyright holder (e.g. author, programmer, producer, developer, and publisher).

4. **Privacy of property of individuals and/or the district**. It is the student's responsibility to respect the privacy of others, and to maintain his/her own privacy, regarding electronic resources and passwords. Students shall not access, copy, or modify passwords, files, e-mail, voice mail, or other materials belonging to other users without explicit authorization of the supervising teacher or designated individual. In the case of suspected misuse or threat to an electronic systems, system administrators have the responsibility to review passwords, files, e-mail, voice mail or other materials stored on any district system by users.

5. **Video usage**. It is the student's responsibility to secure permission from the supervising teacher or designated individual to air a video production. Appropriate visual, textual, and audio content is expected. It is the student's responsibility to obtain the appropriate consent of people, places, and/or events being shown in a video production. Particular attention should be paid to brand names of products or services shown in the presentation.

   It is the student's responsibility to be aware that certain individuals and events may be precluded from video productions due to religious or cultural objections. The supervising teacher or designated individual will assist the student in making appropriate decisions as referred to below in #6.

6. **Appropriate use**. It is the student's responsibility to keep material inappropriate for school use from being used or created on district technology systems (including electronic resources, and textual, video, and/or audio materials). Students are responsible for reporting inappropriate sites to their supervising teacher.

   It is the student's responsibility to not use any technology in a manner which conveys an offensive, profane or sexually suggestive message, or to use technology to harass, disturb by pestering or tormenting, including but not limited to intimidation because of a person's race, color, religion, gender, sexual orientation, or ethnicity.

7. **Damage, vandalism or destruction of technological systems**.
   - Students using technology shall respect the integrity of technological systems and information. It is the student's responsibility to make sure no technology is destroyed, modified, relocated or abused in any way.
   - Virus protection software is installed on the FPS Network to protect the information stored there as well as the integrity of the network. The student will not attempt to compromise the virus protection software.
   - It is the student's responsibility to not use or develop files that infiltrate, harm, or damage components of a computer or computing system/network. It is a student's responsibility to keep infected files off district computers and networks.

8. **Violations and misuse.** It is the student's responsibility to report any violations or misuse of technology to the supervising teacher or designated individual.

DISCIPLINARY ACTION

The consequences of violating these technology guidelines constitute a Level II violation of the Student Code of Conduct of Farmington Public Schools.

Administrative Procedure #4137-1
Revised: 02/08/05