FARMINGTON PUBLIC SCHOOLS
NETWORK REGISTRATION AGREEMENT FOR ALL USERS

I, _____, a student or employee of Farmington Public Schools, understand and agree to comply with the *Network Acceptable Use Policy Terms and Conditions*. Further, I understand, agree and shall comply with the following terms and conditions:

1. The use of the District's network is a privilege and responsible use is required. Some examples of irresponsible use would include, but not be limited to, unapproved software, unlicensed software, key logging software or hardware devices, 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 District's network. The District will be the sole arbiter of what constitutes irresponsible use.

2. The District's network may not be used for conduct or communication that embarrasses, harms or in any way distracts from the good reputation of the District, its staff, students or any organizations, groups, or institutions with which the District's network is affiliated. The District 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.

3. The District reserves the right to review any material stored in files to which any users have access and will edit or remove any material which the District, in its sole discretion, believes may be unlawful, or constitutes irresponsible use as set forth in paragraph one, above. Any individual, who uses, sends, receives or stores information via the District's network has no expectation of privacy associated with such actions.

4. All information services and features on the District's network are intended for educational or professional use. Any commercial or unauthorized use of those features or services, in any form**,** is expressly forbidden.

5. In consideration of the privilege of using the District's network and in consideration of access to it, I release the District's network, its operators and sponsors, the District and its staff, and all organizations, groups and institutions with which the District is affiliated, from any liability and from any claims I may have, of any nature, arising from my use, my inability to use and from others' use of the District's network.

6. My access to the District's 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.

_____	_____	_____
Signature of Staff Member	Signature of Student	Signature of Parent/Guardian (if student is under age 18)
_____	_____	_____
Date	Date	Date

cc: Student or Personnel file

Revised 12/7/10

DISTRICT NETWORK ACCEPTABLE USE TERMS AND CONDITIONS

GENERAL NETWORK INFORMATION

The District network is a service provided by the District. The system administrators are employees of the District and reserve the right to monitor all activity on the District's network. All users must submit a signed *Farmington Public Schools 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 procedures. 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 District's network may modify these rules at any time by publishing the modified rule(s) on the District's website and at each school's media center. Any signature at the end of the *Farmington Public Schools 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 District's 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 the District.

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 the District 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. The District does not control such material. Nor does it condone and nor permit use of these materials on the District's 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, the District's "Student Code of Conduct" and the District's Board Policies. Such activities may also result in termination of the user's account on the District's network, as well as suspension or expulsion.

ONLINE CONDUCT

Any action by a user that constitutes an inappropriate use of the District's network, or improperly restricts or inhibits other users from using and enjoying the District's 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 District's network and in consideration for access to the information contained in it, users release the District's network and its operators and sponsors, the District and its staff, and all organizations, groups and institutions with which the District is affiliated, from any and all liability or claims of any nature arising from the use, or inability to use, the District's network.

The District's network shall be used for educational purposes only.

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

The District 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 District 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 the District's 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 (email), blogging, chatting, texting or any 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 District's network are normally retained for 120 days or until deleted by the recipient. A canceled District 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. Personally identifiable information about students is not to be sent via email.

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

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

The District 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 District's 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 District's 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 District's 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 District's 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 District's **"**Student Code of Conduct" including suspension or expulsion.

TERMINATION OF ACCOUNT

The District reserves the right, in its sole discretion, to suspend or terminate the user's access to and use of the District's 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, the District 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 District's Board and the Student Code of Conduct.

TECHNOLOGY USE PROCEDURES

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 District 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 procedures apply to all technology resources.

RESPONSIBILITIES

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 District 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 District's 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.

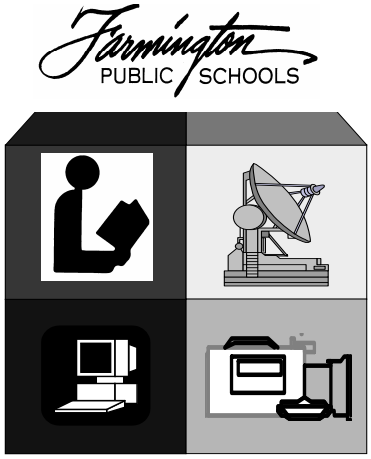
8. **Violations and misuse.** It is the student's responsibility to report any violations or misuse of technology to the supervising teacher or designated individual.

DISCIPLINARY ACTION

The consequences of violating these technology procedures constitute a Level II violation of the District's "Student Code of Conduct".

Administrative Procedure #4137.1 for Policy #4137
05/06/08
Revised 12/7/10

Permission for Students' Photographs & Work To Appear on the Internet



As part of the integration of technology into the curriculum, Farmington Public Schools (FPS) promotes the display of student work on the FPS created Network website.
(http://www.farmington.k12.mi.us)

Throughout the school year, many students will have opportunities to see their work published on the District's website for the community and world to view and enjoy.

Check the appropriate spaces below, in the event that your child's photograph and/or work are selected for inclusion on the FPS District site or the school's web page. Parents have the option, at any time, to request deletion of their student's work.

(PLEASE ANSWER <u>BOTH</u> QUESTIONS.)

Sign, date and return to your school office no later than _____

1. I give permission for samples of my child's work (poetry, short stories, book review, drawings, multimedia presentations, etc.) to appear on the school and/or FPS District web page. In the case that names are included with student work, only first names will be included.

_____Yes OR _____No

2. I give permission for my child's photograph to appear on the school and/or FPS District web page. No names will be used to individually identify students.

_____Yes OR _____No

_____ _____
Student's Name School

_____ _____
Teacher's Name Grade

_____ _____
Parent/Guardian Signature Date

Administrative Procedure #4137.1 for Policy #4137
Revised 12/7/10