INTERNET SAFETY POLICY **7029**

It is the policy of the North Lake School District to comply with all State and Federal guidelines with respect to proper internet utilization and safety including complicity with WI State Statute 947.1025:

-Children's Internet Protection Act or CIPA (Pub. L. No. 106-554 and 47 USC 254(h)
http://www.fcc.gov/guides/childrens-internet-protection-act,
-Neighborhood Children's Internet Protection Act or NCIPA (Pub. L. No. 106-554),
-Broadband Data Improvement Act (Pub. L. No. 110-385),
-Children's Online Privacy Practice Act (COPPA)
http://www.ftc.gov/ogc/coppa1.htm

All students (PreK-8) must be under direct on-site supervision when they are on a computer while in the school building. On-site supervision means the staff member responsible for the student(s) is physically present in the room in which the network is being accessed or utilized by the student(s).

All students (PreK-8) are directed only to age appropriate sites that have been pre-selected, previewed, and deemed appropriate for student use.

Middle school students (Grade 5-8) will conduct guided searching practices leading them to develop 21st Century skills as independent, safe, secure and responsible users of the Internet.

Certain Web 2.0 services, such as social networking sites, wikis, podcasts, RSS feeds and blogs that emphasize online educational collaboration and sharing among users may be permitted by the District for curriculum-related learning activities; however personal use is restricted.

The North Lake School District recognizes that it is required by the Federal Government to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and cyber-bullying awareness and response. Students and parents need to know that for a minor's (under age 18) safety and security, students should never post a picture of themselves that is tied to personal information.

Parents and students must both fill out an opt-in form (Located with Acceptible Use Policy, Appendix H) to acknowledge reading and understanding their responsibilities with regard to computer/network use at North Lake School, as listed in this document.

Children's Internet Protection Act (CIPA)

The North Lake School District uses hardware and software to provide technology protection measures that identify and block or filter Internet access to prohibited materials (including but not limited to: visual depictions of obscenity, child pornography and other materials deemed harmful to minors). The district realizes that no technology protection measure is 100% fail-proof. If a student or staff finds that he or she has accessed an objectionable Internet site, the user is expected to exit the site immediately and notify the teacher, library media specialist**,** Information Technology staff or supervisor.

A. Acceptable Use and Expectations for Internet Safety

1. Blogs and social networking sites may be accessed when there is a specific curriculum objective directed toward Internet responsibility and safety. In this way students will learn to make conscientious decisions about their safety and security while using the Internet. Curriculum objectives also need to include the harmful

effects cyber-bullying can have on an individual and a school environment. Cyber-bullying is defined as using technology to promote deliberate, repeated, and hurtful behavior by an individual or group with the intent to harm others;

2. Each school year, students in grades PreK-8 will learn to safely use the Internet and the harms of cyber-bullying. The students will learn age-appropriate Internet safety strategies and the consequences of cyber-bullying through collaboration between guidance counselors, library media specialists, and classroom teachers;

3. Students are expected to limit their time while in school on social networks or blogs to curriculum assignments;

4. Students under 18 years of age are expected not to post personal information or pictures about themselves or others on the Internet;

5. Students and staff are expected to use appropriate language acceptable in an education setting;

6. Students and staff are expected to report cyber-bullying and criminal behavior such as gang activity, drug and alcohol sales, etc. to administrators.

B. Unacceptable Behaviors Include But Are Not Necessarily Limited to the Following:

1. Sending, accessing or displaying pornography or other offensive and inappropriate materials;

2. Using obscene, lewd, or profane language;

3. Harassing, insulting or attacking others;

4. Using the district's network including the Internet for any illegal purposes such as communicating gang activity, drug and alcohol sales etc;

5**.** Disclosing, using or disseminating personal identification information regarding themselves**,** current or former students, other minors, or staff members without permission;

6 Disclosing full names, birth dates, addresses, home and cell phone numbers, information about schools and school teams so that it is possible for someone else to locate a student or staff;

7. Impersonating another person's identity by posting inappropriate or altered pictures and false information;

8. Planning meetings with peers that result in criminal or risky behavior;

9. Sending a message to a person via e-mail or computerized communication system that threatens to inflict injury or physical harm to that person or their property, with the intent to frighten, intimidate, threaten, abuse, or harass that person;

10. Intentionally preventing or attempting to prevent the disclosure of his or her own identity when sending a message to a person;

11. Sending repeated messages via e-mail or computerized communication system with intent of harassing a person.

C. Consequences:

Students who commit any of the above listed acts of misconduct will be disciplined in one or more of the following ways:

Minimum Consequences:

1. The student's parents will be contacted;

2. The student will be given limited access to school telecommunications equipment, networks and services;

3. The student will be denied access to school telecommunications equipment, networks and services;

4. The student will be banned from bringing any software or data storage devices to school;

5. The student will be required to pay for all property damage;

6. The Internet Service Provider will be notified;

7. The student will receive in-school suspension;

8. The student will receive out-of-school suspension.

Maximum Consequences:

1. The student will be denied access to all district-owned computer equipment, networks, and services;

2. The appropriate law enforcement agencies will be notified;

3. The student will be recommended for expulsion.