

Acceptable Use Electronic Network

Grades PK – 2

Parents and Students:

Please read together, sign and return the Individual User Access Informed Consent Form to the school. This document is available at www.crestwood.k12.il.us

Statement of Purpose

Crestwood School believes that all students should have access to technology when they act in a responsible, efficient, courteous and legal manner. Internet access and other online services, available to students and teachers, offer a multitude of global resources. Our goal in providing these services is to enhance the educational development of our students. All school Internet use is filtered and monitored.

Acceptable uses of technology are devoted to activities that support teaching and learning. The following are our agreements about the use of technology at Crestwood School:

Terms of Agreement

Using the computer correctly and responsibly is very important. I promise to follow these rules:

1. I promise to use all computer equipment carefully and not damage, change or tamper with the hardware, software, settings or the network.
2. I promise never to use any form of electronic communication to harass, frighten, or bully anyone.
3. I promise to use the computer and the Internet for schoolwork only. I will use the programs and websites that my teacher has approved.
4. I promise not to share my passwords.
5. I will not view, send or display inappropriate messages or pictures.
6. I promise to tell an adult if I read or see something on the computer that is inappropriate.
7. I promise to obey copyright laws.
8. I will not use my personal email account or any personal electronic device at school except with the permission of a staff member.
9. I promise to print only when my teacher tells me to.
10. I promise to only use my own file or my own folder on the student server.
11. I understand that if I break any of my promises, I might not be able to use the computers.

Education

- Education about online safety and digital citizenship (online behavior, communication, cyber-bullying, literacy, etiquette, rights and responsibilities and security) will be covered in the K-8 curriculum each school year.

1 “Electronic communication” means a communication transmitted by means of an electronic device including, but not limited to, a telephone, cellular phone, computer, pager, iPods or other mp3 or audio-video players and cameras.

Individual User Access Informed Consent Form

Dear Parents/Guardians:

Crestwood School has the ability to enhance your child's education through the use of electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication.

The District *filters* access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. Even with the use of filters it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child or ward should follow, and Crestwood School respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have an Internet account, sign the *Authorization* form below and return it to your school.

Students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the *Acceptable Use of Electronic Networks* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic network, including the Internet.

Student Name (*please print*)

Student Grade

Parent/Guardian Name (*please print*)

Parent/Guardian Signature

Date

Keeping Yourself and Your Kids Safe On Social Networks

For students:

- Put everything behind password protected walls, where only friends can see.
- Protect your password and make sure you really know who someone is before you allow them onto your friend's list.
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators.
- Don't post anything your parents, principal or a predator couldn't see.
- What you post online stays online - forever!!!! So ThinkB4UClick!
- Don't do or say anything online you wouldn't say offline.
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pics online.
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!
- And, unless you're prepared to attach your blog to your college/job/internship/scholarship or sports team application...don't post it publicly!
- Stop, Block and Tell! (don't respond to any cyberbullying message, block the person sending it to you and tell a trusted adult).
- R-E-S-P-E-C-T! (use good netiquette and respect the feelings and bandwidth of others).
- Keep personal information private (the more information someone has about you, the more easily they can bully you).
- Google yourself! (conduct frequent searches for your own personal information online and set alerts ... to spot cyberbullying early).
- Take 5! (walk away from the computer for 5 minutes when something upsets you, so you don't do something you will later regret).

And for parents:

- Talk to your kids - ask questions (and then confirm to make sure they are telling you the truth!)
- Ask to see their profile page (for the first time)...tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe...and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic...there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you had they known, when you were fifteen.
- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer...and reading their blog. One is between them and the paper it's written on; the other between them and 700 million people online!
- Don't believe everything you read online - especially if your teen posts it on her blog!

For more information, visit www.WiredSafety.org; www.stopcyberbullying.org.

Reprinted with permission from "Parry Aftab's Guide to Keeping Your Kids Safe Online, MySpace, Facebook and Xanga, Oh! My!" Parry Aftab, Esq., www.aftab.com.

Resources for Students and Parents

Resources for students:

Federal Trade Commission - Social Networking Sites: Safety Tips for Tweens and Teens www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

Connect Safely - Social Web Tips for Teens www.connectsafely.com/Safety-Tips/social-web-tips-for-teens.html (2008).

Life online (Girls Scouts and Windows) - lmc.girlscouts.org/Online-Safety-Topics/Social-Networking/Is-It-Safe-/Test-Your-Knowledge-on-Social-Networking-Safety.aspx. Test for knowledge of networking safety.

Resources for parents:

Safety Web - Social Networking Safety Tips for Parents, Monitoring Social Networking of your Child www.safetyweb.com/social-networking-safety-tips. Great comprehensive article for parents.

Connect Safely - Social Web Tips for Parents www.connectsafely.com/Safety-Tips/social-web-tips-for-parents.html (2008).

National Cyber Security Alliance - Social Networking <http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks>

National Consumers League - Social networking security and safety tips www.nclnet.org/technology/9-safe-computing/152-social-networking-security-and-safety-tips.

DHS U.S. CERT - Socializing Securely: Using Social Networking Services www.us-cert.gov/reading_room/safe_social_networking.pdf.

DHS U.S. Computer Emergency Readiness Team - Staying Safe on Social Network Sites www.us-cert.gov/cas/tips/ST06-003.html (January 26, 2011).

Internet Safety: Social Networking Sites for Children www.privatewifi.com/internet-safety-social-networking-sites-for-children/ (March 30, 2011).

8 Safe Social Networks for Kids kommein.com/8-safe-social-networks-for-kids/ (Jan. 5, 2011). List of sites that are compliant with Children's Online Privacy Protection Act and have parental controls