Crestwood School

Acceptable Use of Electronic Network

Crestwood School recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, Crestwood School will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their education.

These procedures are written to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

Privileges
The use of the District's electronic resources is a privilege, not a right, and inappropriate use may result in disciplinary action, limitation or loss of those privileges and/or appropriate legal action. Administration will make all decisions regarding whether or not a user has violated this Procedure, and follow the board policies for discipline. District's electronic resource use for the user may be suspended, revoked or denied access by the administration if deemed necessary.

Indemnification
The user agrees to indemnify the School District for any losses, cost or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these policies or procedures.

Network
The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of learning and educational research;
- Participation in blogs, wikis, bulletin boards, educational social networking sites and groups and the creation of content for podcasts, and web pages that have been approved by the administration and support learning and educational research;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;

Unacceptable network use by district students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installation and use of games, audio files video files or other applications (including shareware or freeware) without permission or approval from the administration,
- Support or opposition for ballot measures, candidates and any other political activity;

- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Internet Safety

Personal Information and Inappropriate Content

- Students should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority immediately.

Filtering and Monitoring

- Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.
- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.
- Students are not allowed to use electronic mail, chat rooms, social networking sites, discussion forums or other forms for personal electronic communications.
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district.
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

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.

Copyright
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Log off if leaving the computer.

No Expectation of Privacy
The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Illinois.

Disciplinary Action
All users of the district's electronic resources are required to comply with the district's policy and procedures *and agree to abide by the provisions set forth in the district's user agreement*. Violation of any of the conditions of use explained in the *Crestwood School's* Acceptable Use of Electronic Network Policy could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges, and or appropriate legal action.

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. If a filter has been disabled or malfunctions 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.

_____

Parent/Guardian Name (*please print*)

_____ _____

Parent/Guardian Signature Date

Students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic network, including the Internet.

_____ _____

Student Name (*please print*) Grade

_____ _____

Student 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.stopcyberbulling.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) - lmk.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