HIGHLAND COMMUNITY UNIT SCHOOL DISTRICT NO. 5

Serving the Communities of Alhambra, Grantfork, Highland, New Douglas, and Pierron

MICHAEL S. SUTTON
SUPERINTENDENT OF SCHOOLS

DEREK A. HACKE
ASSISTANT SUPERINTENDENT - INSTRUCTION

BRIAN L. ARTEBERRY
CHIEF SCHOOL BUSINESS OFFICIAL

2021-2022

Dear Parent(s)/Guardian(s),

We have the ability to enhance your child's education through the use of technology including electronic networks. The District's goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Your authorization is needed before your child may use this resource.

The authorization for your child to participate in the opportunities available with District technology resources includes three distinct parts that you must understand and consider separately. The three types of authorization and consent required include (1) the authorization for access and use of electronic networks and District resources, (2) the consent to publish your child's work product materials on the District website, and (3) the publication of your child's image on the District website. To provide authorization for the above opportunities, you and your child must sign the signature page of the Authorization for Electronic Network Access/Web Publication of Student Material/Display of Student Images on the District website. The signature page of the Authorization form shall provide you with the opportunities to designate your authorization and consent for each of these opportunities. Please read and discuss with your child the various sections of the Authorization form that corresponds to the different opportunities available.

Teachers may have access to:

- Limited e-mail communications with people all over the world
- Information from government sources, research institutions, and other sources
- Discussion groups
- Many libraries, including the catalog to the Library of Congress, and the Educational Resources Information Clearinghouses (ERIC)

Students may have access to:

- Information from government sources, research institutions, and other sources
- Discussion groups
- Many libraries, including the catalog to the Library of Congress, and the Educational Resources Information Clearinghouses (ERIC)

Students may have access to e-mail or other electronic messaging at school. With this educational opportunity also comes responsibility. You and your child should read the Authorization for Electronic Network Access and discuss it together. 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.

The District takes reasonable precautions to prevent access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. On an unregulated network, however, it is impossible to control all material and a user may discover inappropriate material. Ultimately, parent(s)/guardian(s) are responsible for setting and conveying the standards that their child or ward should follow. To that end, the School District supports and respects each family's right to decide whether or not to authorize Electronic Network Access.

With respect to the publication of student work product on the District website and display of a student's image on the District website, we believe that publishing student work and pictures that include students of the District provide a wonderful opportunity for students to share their accomplishments with other children and parents for educational growth. While the District tries to provide learning and sharing and opportunities for students through the use of technology, we also want to ensure that you understand the issues and concerns that may exist with Electronic Network Access. With concern for your child's privacy and safety, the permission slip provides a place for you to indicate how your child will be identified to give your child credit for his/her work that will appear on the District website.

Because respect for the work of students and others is an integral part of academic discipline, all student material published on the District website should be the original work of the student. If more that one student created the work, then each person who participated in the creation of the work will be identified as a joint author of the work.

Please read and discuss the Authorization for Electronic Network Access with your child. If you agree to allow your child to have Electronic Network Access, sign the Authorization form and return it to your school.

Sincerely,

Michael S. Sutton
Superintendent of Schools
MSS/adf

Instruction

Authorization for Electronic Network Access/Web Publication of Student Materials/ Consent to Display of Student Images on the Internet

Internet Access Authorization and Conditions

Each staff member must sign this Authorization as a condition for using the District's Internet connection. Each student and his or her parent(s)/guardian(s) must sign this Authorization for Internet access before being granted unsupervised access. School Board members and administrators are treated like teachers for purposes of this Authorization. ***Please read this document carefully before signing.***

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization does not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures 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 that each party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

Acceptable Use - Access to the District's Internet connection must be for the purpose of education or research, and be consistent with the educational objectives of the District.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation or limitation of those privileges. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time; his or her decision is final.

Unacceptable Use - The user responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
b. Unauthorized downloading of digital material, regardless of whether it is copyrighted or de-virused;
c. Downloading copyrighted material for other than personal use;
d. Using the network for private financial or commercial gain;
e. Wastefully using resources, such as file space, or network bandwidth for non-school activities;
f. Hacking or gaining unauthorized access to files, resources, or entities;
g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is a personal nature including a photograph;
h. Using another user's account or password;
i. Posting material authored or created by another without his/her consent;
j. Posting anonymous messages;
k. Using the network for commercial or private advertising;
l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
m. Using the network while access privileges are suspended or revoked;
n. Using technology resources for personal entertainment such as computer gaming;

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in your messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

c. Do not reveal the personal information, including addresses or telephone numbers, of students or colleagues.
d. Recognize that email is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

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

Security - Network security is a high priority. If you can identify a security problem on the Internet, the user must notify the system administrator or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to network.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses and vandalism to district computer hardware.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
b. Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.
c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.
b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such

messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.

d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

Use of the School District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this *Authorization*, and otherwise follow this *Authorization*.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this *Authorization*.

District networks with Internet access have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.

Instruction

Exhibit - 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 www.staysafeonline.org/in-the-home/social-networking (August 30, 2010).

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