Aurora Public Schools Internet Responsible Use Agreement

The District's Responsible Use Policy ("RUP") is to allow all employees, volunteers and currently enrolled students (defined as "user") to use computers and the network for educational purposes, research and communication. This agreement prevents unauthorized disclosure of or access to sensitive information that is the property of the Aurora Public Schools including, but not limited to, student records and personnel files. This agreement further prevents unlawful online activities including bullying, gambling, and searching for, saving or dispensing pornography.

Every student needs skills and knowledge to succeed as effective citizens, workers and leaders. The 21st century learning environment includes all types of resources and computing devices. Digital resources and web 2.0 tools may include blogs, wikis, other online applications, and communication applications for email, social networking, instant messaging, video conferencing, and other forms of direct electronic communications. Students have access to computing devices including, but not limited to, desktop computers, laptops, ebooks, ipods, cell phones, or other digital devices. The use of computer applications, online resources and devices support the Aurora Public Schools curriculum and standards.

The District complies with the Children's Internet Protection Act ("CIPA")* and uses technology protection measures to block or filter, to the extent practicable, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to parents, guardians, teachers, administrators or law enforcement authorities as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including email. This agreement complies with all laws associated with blocking content that is dangerous or inappropriate for minors.

Responsible Uses of the APS Computer Network or the Internet

Accessing the APS Computer Network and the Internet is critical for all APS business functions and student success today. All students must have their parents or guardians sign this agreement and the District will keep it on file in the student records. Once signed, that permission/acknowledgement remains in effect until the student loses the privilege of using the District's network due to violation of this agreement or is no longer enrolled as an APS student. Even without signature, all users must abide by this policy.
All users (defined in the first paragraph) are required to follow this agreement and report any misuse of the network or Internet to a teacher, supervisor or other appropriate District personnel. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate District personnel. By using the network, users have agreed to this agreement.

Unacceptable Uses of the Computer Network or Internet

APS reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for students, employees, schools, network or computer resources, or (2) that lacks legitimate educational content/purpose, or (3) other activities as determined by the District as inappropriate.
A few examples of inappropriate activity may include but are not limited to:

- Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Criminal activities that can be punished under law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:

1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
2. Spreading untruths or rumors about individuals or groups of people in e-mail messages or social networking sites.
3. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email.
4. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
5. Using a District computer to pursue in order to unlawfully access and/or change any information

6. Accessing, transmitting or downloading large files, printing large documents, including "chain letters" or any type of "pyramid schemes".

- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
  1. Using another's account password(s) or identifier(s);
  2. Interfering with other users' ability to access their account(s); or
  3. Disclosing anyone's password to others or allowing them to use another's account(s).

- Using the network or Internet for Commercial, Political and Religious purposes:
  1. Personal advertising, promotion or financial gain;
  2. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitations or lobbying for religious or political purposes.

Student Internet Safety

1. The student's parent or guardian is responsible for monitoring the minor's use at home or away from school.
2. Students should not reveal personal information about themselves or other persons on the Internet. For example, students should not reveal their name, home address, telephone number, credit card number, or display photographs of themselves or others.
3. Students should not meet in person anyone they have met only on the Internet.
4. Students must abide by all laws, including this Responsible Use Policy and all District policies.

Penalties for Improper Use

The use of District resources is a privilege, not a right, and misuse will result in the restriction or cancellation of District provided accounts and/or use of District equipment. Misuse may also lead to disciplinary and/or legal action for both students and employees, up to or including suspension, expulsion, dismissal from District employment, or criminal prosecution by law enforcement authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

I have read and understand, and I will abide by the guidelines of the Responsible Policy of the Aurora Public School District.

Date:	_____	School:	_____
Student Name:	_____	Student Signature:	_____
Parent/Legal Guardian Name:	_____	Parent/Legal Guardian Signature:	_____

Please return this form to your child's school where it will be entered into the District's Student Information System.

*http://ifea.net/cipa.html **http://www.fcc.gov/cgb/consumerfacts/cipa.html