SECTION V: INTERNET POLICIES

INTERNET USE

It shall be the policy of Wallace School District 65-R to provide educative and curriculum related opportunities to the students of the district by providing tele-computing services by (Internet). By adopting this policy recognizes that access to the Internet, data is available through the Internet and the placing of data onto the Internet may be technically difficult to monitor and control. Software will be installed to attempt to restrict/block access to inappropriate material. It shall, in recognition of the educative and curricular benefits of Internet, be the policy of this district to revoke the privilege of any user who misuses the Internet by engaging in activities not related to the educative purposes or to the curricular offerings of the district.

User access will be prohibited and revoked to any person who uses the Internet for activities such as but not limited to, receiving or inputting pornographic materials; promoting violence; engaging in racial; gender or other slurs; receiving or transmitting information pertaining to dangerous instrumentalities such as bombs; automatic weapons; or other illicit firearms; weaponry; or explosive devices; for engaging it's uses of a defamatory nature; for personal attacks on or "flaming" of another; for engaging in non-educative or non-curricular related conversations; including chat rooms; and for accessing or inputting items of a strictly entertaining or recreational nature not related to the educative purposes or the curriculum of this district.

Additionally, to the extent that it can be reasonably determined by the administration what fees if any have been incurred by a person for non-authorized purposes; it shall be the policy of this district to seek reimbursement and full restitution from the student or his or her guardian, for use of the Internet in a manner inconsistent with this policy.

It shall further be the policy of this district to provide a copy of this policy and Internet guidelines to each student user of the Internet and to his or her parent or guardian.

Internet Safety and Acceptable Use Policy - Board Policy 6800

Internet Safety Policy

It is the policy of the Wallace School District 65-R to comply with the Children's Internet Protection Act (CIPA). With respect to the District's computer network, the District shall: (a) prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) provide for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities online; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) implement measures designed to restrict minors' access to materials (visual or non-visual) that are harmful to minors.

1. Definitions. Key terms are as defined in CIPA. "Inappropriate material" for purposes of this policy includes material that is obscene, child pornography, or harmful to minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that: (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

2. Access to Inappropriate Material. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

3. Inappropriate Network Usage. To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so- called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

4. Supervision and Monitoring. It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent and the Superintendent's designees.

5. Social Networking. Students shall be educated about appropriate online behavior, including interacting with others on social networking websites and in chat rooms, and cyberbullying awareness and response.

6. Adoption. This Internet Safety Policy was adopted by the Board at a public meeting, following normal public notice.

B. Computer Acceptable Use Policy

This computer acceptable use policy is supplemental to the District's Internet Safety Policy.

1. Technology Subject to this Policy. This Computer Acceptable Use Policy applies to all technology resources of the District or made available by the District. Technology resources include, without limitation, computers and related technology equipment, all

forms of e-mail and electronic communications, and the internet.

2. Access and User Agreements. Use of the District technology resources is a privilege and not a right. The Superintendent or designee shall develop appropriate user agreements and shall require that employees, students (and their parents or guardians), and others to sign such user agreements as a condition of access to the technology resources, as the Superintendent determines appropriate. Parents and guardians of students in programs operated by the District shall inform the Superintendent or designee in writing if they do not want their child to have access.

   The Superintendent and designees are authorized and directed to establish and implement such other regulations, forms, procedures, guidelines, and standards to implement this Policy.

   The technology resources are not a public forum. The District reserves the right to restrict any communications and to remove communications that have been posted.

3. Acceptable Uses. The technology resources are to be used for the limited purpose of advancing the District's mission. The technology resources are to be used, in general, for educational purposes, meaning activities that are integral, immediate, and proximate to the education of students as defined in the E-rate program regulations.

4. Unacceptable Uses. The following are unacceptable uses of the technology resources:

   a. Personal Gain: Technology resources shall not be used, and no person shall authorize its use, for personal financial gain other than in accordance with prescribed constitutional, statutory, and regulatory procedures, other than compensation provided by law.

   b. Personal Matters: Technology resources shall not be used, and no person shall authorize its use, for personal matters.

      Occasional use that the Superintendent or designee determines to ultimately facilitate the mission of the District is not prohibited by. this provision. Examples of occasional use that may be determined to ultimately facilitate the mission of the District: sending an e-mail to a minor child or spouse; sending an e-mail related to a community group in which an employee is a member where the membership in the community group facilitates the District's mission.

      This occasional use exception does not permit use by employees contrary to the expectations of their position. For example, employees may not play games or surf the net for purposes not directly related to their job during duty time; nor may students do so during instructional time.

      The occasional use exception also does not permit use of the technology resources for private business, such as searching for or ordering items on the internet for non-school use; or sending an e-mail related to one's own private consulting business.

c. Campaigning: Technology resources shall not be used, and no person shall authorize its use, for the purpose of campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question.

d. Technology-Related Limitations: Technology resources shall not be used in any manner which impairs its effective operations or the rights of other technology users.

1. Users shall not use another person's name, log-on, password, or files for any reason, or allow another to use their password (except for authorized staff members).
2. Users shall not erase, remake, or make unusable another person's computer, information, files, programs or disks.
3. Users shall not access resources not specifically granted to the user or engage in electronic trespassing.
4. Users shall not engage in "hacking" to gain unauthorized access to the operating system software or unauthorized access to the system of other users.
5. Users shall not copy, change, or transfer any software without permission from the network administrators.
6. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
7. Users shall not engage in any form of vandalism of the technology resources.
8. Users shall follow the generally accepted rules of network etiquette. The Superintendent or designees may further define such rules.

e. Other Policies and Laws: Technology resources shall not be used for any purpose contrary to any District policy, any school rules to which a student user is subject, or any applicable law. Without limitation, this means that technology resources may not be used:

1. to access any material contrary to the Internet Safety Policy; or to create or generate any such material.
2. to engage in unlawful harassment or discrimination, such as sending e-mails that contain sexual jokes or images.
3. to engage in violations of employee ethical standards and employee standards of performance, such as sending e-mails that are threatening or offensive or which contain abusive language; use of end messages on e-mails that may imply that the District is supportive of a particular religion or religious belief system, a political candidate or issue, or a controversial issue; or sending e- mails that divulge protected confidential student information to unauthorized persons.
4. to engage in or promote violations of student conduct rules.

5. to engage in illegal activity, such as gambling.
6. in a manner contrary to copyright laws.
7. in a manner contrary to software licenses.

5. Disclaimer. The technology resources are supplied on an "as is, as available" basis. The District does not imply or expressly warrant that any information accessed will be valuable or fit for a particular purpose or that the system will operate error free. The District is not responsible for the integrity of information accessed, or software downloaded from the Internet.
6. Filter. A technology protection measure is in place that blocks and/or filters access to prevent access to Internet sites that are not in accordance with policies and regulations. In addition to blocks and/or filters, the District may also use other technology protection measures or procedures as deemed appropriate.

   Notwithstanding technology protection measures, some inappropriate material may be accessible by the Internet, including material that is illegal, defamatory, inaccurate, or potentially offensive to some people. Users accept the risk of access to such material and responsibility for promptly exiting any such material.

   The technology protection measure that blocks and/or filters Internet access may be disabled only by an authorized staff member for bona fide research or educational purposes: (a) who has successfully completed District training on proper disabling circumstances and procedures, (b) with permission of the immediate supervisor of the staff member requesting said disabling, or (c) with the permission of the Superintendent. An authorized staff member may override the technology protection measure that blocks and/or filters Internet access for a minor to access a site for bona fide research or other lawful purposes provided the minor is monitored directly by an authorized staff member.

7. Monitoring. Use of the technology resources, including but not limited to internet sites visited and e-mail transmitted or received, is subject to monitoring by the administration and network administrators at any time to maintain the system and insure that users are using the system responsibly, without notice to the users. Users have no privacy rights or expectations of privacy with regard to use of the District's computers or Internet system. All technology equipment shall be used under the supervision of the Superintendent and the Superintendent's designees.

8. Sanctions. Violation of the policies and procedures concerning the use of the District technology resources may result in suspension or cancellation of the privilege to use the technology resources and disciplinary action, up to and including expulsion of students and termination of employees. Use that is unethical may be reported to the Commissioner of Education. Use that is unlawful may be reported to the law enforcement authorities. Users shall be responsible for damages caused and injuries sustained by improper or non-permitted use.

Sexting

Sexting is defined as the act of sending sexually explicit messages or photos electronically. Although

sexting usually occurs via a text message sent between cell phones, digital pictures of sexually explicit subjects are also exchanged using e-mails, iPods, pagers, and social networking sites, such as Facebook.

By bringing cell phones and other devices to school, the student and parents consent to the search of that device when school officials have a reasonable suspicion that such a search will reveal a violation of school rules. The mere possession of sexually explicit digital pictures on any device is prohibited on school grounds. Sending, sharing, viewing, or possessing pictures, text messages, e-mails or other material of a sexual nature in electronic or any other form on a computer, cell phone or other electronic device is strictly prohibited.

Student Expectations
If a student receives a sexually explicit picture he/she should immediately:

1. report the incident to an adult
2. delete the picture

Both the sender and the receiver of sexually explicit pictures may be punished if the recipient kept the picture.

Consequences for Sexting
Parents will be promptly notified upon the discovery that their child is the subject of or in possession of sexually explicit pictures. School officials will report the existence of sexually explicit pictures of any student to law enforcement to determine whether a crime has been committed and did not immediately delete it.

RISKS OF FACEBOOK AND OTHER SOCIAL NETWORKING

The purpose of this message is to give our students information about the risks of using Facebook and similar social networking sites. These sites are public sources of information. Your school administrators, your parents, and law enforcement may see the information. It is also accessible to people who you don't even know now, but may later want to impress; such as university admissions and scholarship officials and prospective employers. In fact, many large companies now search the Internet as a means of conducting background checks on job applicants. What you say now on Facebook may affect you years later.

What you say now on Facebook may also affect you right now. Pictures or writings that show that you have violated student conduct rules may result in school discipline. A picture of a student drinking beer may very well lead to a suspension from activities if the school learns about it. Criminal charges may be filed against you based on information posted on Facebook.

Here are some common sense guidelines that you should follow when using Facebook and the Internet in general:

a. Don't forget that your profile and Facebook forums are public spaces. Don't' post anything you wouldn't want the world to know (e.g., your phone number, address, IM screens name, or specific whereabouts).
b. Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school.
c. People aren't always who they say they are. Be careful about adding strangers to your friends list. It's fun to connect with the new Facebook friends from all over the world, but avoid

meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.

d. Harassment, hate speech and inappropriate content should be reported. If you feel someone's behavior is inappropriate, react. Talk with a trusted adult, or report it to Facebook or the authorities.
e. Don't post anything that would embarrass you later. Think twice before posting a photo or info you wouldn't want your parents or boss to see!
f. Don't mislead people into thinking that you're older or younger. If you lie about your age, Facebook will delete your profile.

We urge all students to follow these common sense guidelines.

LAPTOP SUSPENSIONS

VIOLATION	1st Offense	2nd Offense
* Unattended Laptop	1 Day	3 Days
* Games, Chat, Skype (Video)	3 Days	7 Days
* Unauthorized System Changes (Includes unauthorized extensions)	5 Days	20 Days
* Inappropriate Use, Care	2 Days	7 Days
* Abuse of Laptop	3 Days	7 Days
* Printing Inappropriately	3 Days	7 Days
* Inappropriate Pictures (Desktop, Screen Saver, Saved File)	10 Days	20 Days
* Inappropriate Internet Site	5 Days	20 Days
* Inappropriate Comments	5 Days	20 Days
* Jr. High - No computer in cart for nighttime charging	3 Days	Days double for each offense
* Jr. High - No charger on laptop cart for nighttime charging	1 Day	Days double for each offense

* The administration retains the right to suspend the student's laptop computer for a longer period of time if the offense warrants or for any offense not listed above. This includes suspending the laptop for the remainder of the semester or school year.
* The third offense will result in the loss of the laptop for a quarter, semester or rest of the school year.