

<p>Subject: Internet Safety</p> <p>Policy Reference <u>IIBE Acceptable Use of Technology</u></p> <p>Strategic Plan Goal Reference <u>Goal 1 Prepare all students to succeed as members of a global community and in a global economy</u></p>	<p>Date: May 10, 2007</p> <p>Enclosures: Attachment 1 – Internet Safety Addendum to AUP Attachment 2 – IIBE AUP with proposed revisions</p> <p>REASON FOR CONSIDERATION: Action _____ Information <u>X</u></p>
--	--

Background (Purpose)

Legislation approved by the 2006 General Assembly requires the addition of a student Internet safety component to division acceptable use policies (AUP). The legislation requires Internet safety to be integrated within each school division’s academic instructional program. To assist the division, the Department issued *Guidelines and Resources for Internet Safety in Schools* in October 2006.

Division Superintendents currently are required to submit an updated AUP biennially: The Internet safety component must be included in the September 2008 submission. During school year 2006-2007, the division's Internet safety policy should be developed, aligned with the state guidelines, and incorporated into the AUP. By June 1, 2007, each division must send a statement to the director of the Office of Educational Technology confirming the completion of this work. During school year 2007-2008, the division will review the progress and effectiveness of its Internet safety policy and the implementation of its Internet safety program. By September 1, 2008, each division must submit to the department a copy of the AUP, including the Internet safety policy, and a statement that the AUP and Internet safety program have been reviewed. The department will review division policies for compliance in September 2008. Minor revisions have been made to the regulations of IIBE to be more explicit in referencing our Internet Safety Program.

Administrative Consideration (Rationale)

In order to prepare students to live, learn, work, and thrive in the world of the 21st century, Albemarle County Public Schools must provide access to and education in the use of the emerging technologies of the Digital Age. Digital Age Literacy--the ability to acquire, evaluate, and utilize vast amounts of information--has become the fourth basic skill needed by both present and future generations. Information literacy, global awareness, inventive thinking, teaming, collaborating, planning, and managing for results are essential skills for the 21st century

All learners believe in their power to embrace learning, to excel, and to own their future. Albemarle County Public Schools appropriately integrates technology into all aspects of curriculum, instruction, assessment, and school management to achieve the best possible outcomes. All students learn skills that will enable them to function as productive citizens in a global, technologically oriented society. Technology extends learning for all students and builds learning communities throughout the County of Albemarle.

Internet safety topics have already been imbedded in our curriculum and instructional practices. During the 2006-07 school year a committee of teachers, coordinators and technology personnel reviewed and further developed the Internet Safety Curriculum utilizing the State guidelines and the resources from the staff development offered through iSafe Internet Safety Training. This training was a required component for CTIP’s, Library Media Specialists, Guidance Counselors, Bullying Prevention Representatives and Middle and High School Health teachers during the central staff development days this year.

The curriculum developed has been mapped to the State Rubric for compliance while the committee continues to work on specific implementation strategies for the 2007-08 school year. CTIP’s,

coordinators and the Technology Advisory Committee have reviewed and provided input into the development of the document. Schools will collaborate through a team of iSafe trained teachers to implement the components and lessons for each grade level as best meets the needs of the school while assuring all students receive internet safety instruction.

Budget Implications (Short and Long Term)

The current proposed instructional budget provides support for the purchase of some supplemental iSafe materials. Additional materials identified through the implementation year of 2007-08 will be brought before the School Board for approval.

Recommendation/Future Direction/Time Line

It is recommended that the School Board review (a) the internet safety addendum to the AUP and (b) the minor revisions that have been made to the regulations of IIBE to be more explicit in referencing our Internet Safety Program for direction and future approvals at the May 24, 2007 meeting.

PREPARED: Don Vale

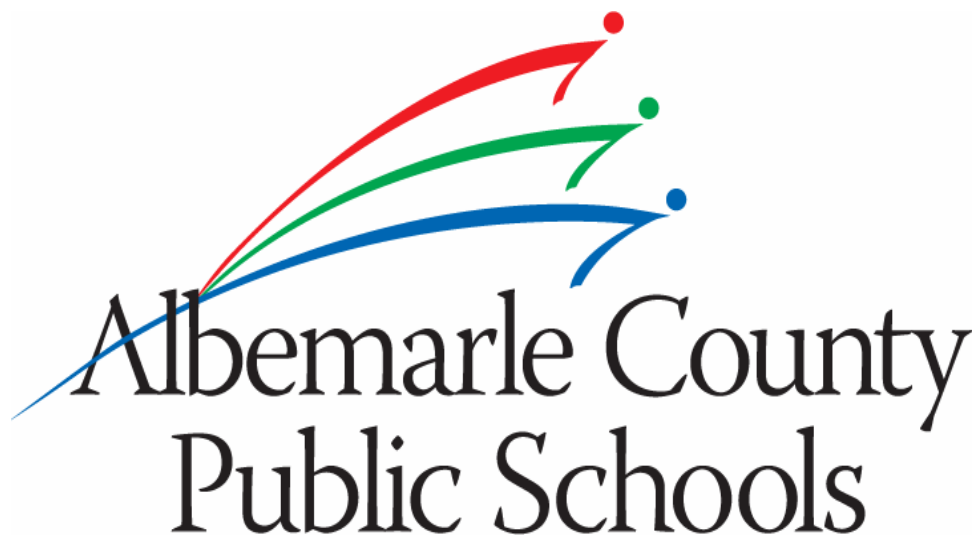
REVIEWED: _____

ITEM NUMBER:

RECOMMENDED:

Educational Technology Plan for Albemarle County Public Schools 2007-2009

Internet Safety Addendum



AUP Internet Safety Plan Overview

I. Instructional Philosophies and Strategies to be Supported by Internet Access in Schools:

Albemarle County Public Schools' philosophy on Internet use in education is to promote educational excellence by facilitating resource sharing, innovation, and telecommunications as outlined in the Technology Acceptable Use policy and applicable regulations. Internet and computer network and non-network access is available to authorized students, teachers, and other staff in the Albemarle County Public Schools.

Specific strategies supported by Internet access include but are not limited to:

- A. Staff members assigning or permitting Internet use will seek to promote a safe online environment by preventing access by students to material that the school division deems to be harmful to juveniles, and as defined in § 18.2-390 of the Code of Virginia.
- B. Staff members assigning student Internet use will recommend safe search strategies and resources which meet the curricular needs of the assignment and the developmental level of the student.
- C. Staff members assigning or permitting Internet use will provide or arrange for instruction in acceptable use of the Internet based on information or materials provided by the Office of Instruction. Topics to be addressed include:
- D. Content of the Technology Acceptable Use Policy and Regulations
- E. Generally accepted rules of network etiquette and safety
- F. Copyright guidelines
- G. Respect for use of time and resources
- H. Evaluating sites for appropriateness and validity
- I. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity.

II. Roles and responsibilities for division personnel and students with regard to Internet

safety: In the detailed Internet Safety plan below, division personnel implementation roles and responsibilities are detailed in the "Implemented By:" section of each component. Student roles and responsibilities are defined in the "Student Regulations" section of the AUP which are reviewed and signed by students and parents and kept on file at school. An overview and outline of the AUP and the Internet Safety Plan is available in electronic format for all to view through the Albemarle County Public Schools website: <http://www.k12albemarle.org/>.

III. Roles and responsibilities for community stakeholders with regard to the acceptable use of

electronic-based resources and Internet: In the detailed Internet Safety plan below, community stakeholders roles and responsibilities are detailed in the "Implemented By:" section and are further detailed in the "Community Outreach" section of each component.

IV. Safety measures in place, including filtering and monitoring procedures:

In accordance with § 22.1-70.2 of the Code of Virginia, Albemarle County Public Schools has implemented a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 of the Code of Virginia and obscenity as defined in § 18.2-372 of the Code of Virginia.

Specific strategies and guidelines include but are not limited to:

- A. Staff members assigning or permitting Internet use will seek to prevent access by students to material that the school division deems to be harmful to juveniles, and as defined in § 18.2-390 of the Code of Virginia.
- B. Staff members assigning student Internet use will recommend safe search strategies and resources which meet the curricular needs of the assignment and the developmental level of the student.
- C. School Division employees who, based upon job responsibilities, have access to monitor the technology use of students or staff must follow guidelines established by the site administrator (school

principal or administrative director). These guidelines shall be placed on file with the Office of Technology.

- D. Any Office of Technology employee monitoring the technology use of students or staff must follow established site-based or District-level guidelines, a copy of which is included in these regulations.

Measures for Future Implementation:

- A. There will be an ongoing evaluation by the Office of Technology of measures in the AUP to promote a safe environment for all school division employees and students. The action plan will be reviewed as needed.

- V. **Methods by which the division ensures data and network security:** The normal operation and maintenance of the division's technical infrastructure and services requires that general usage and activity is monitored, data and electronic communications are routinely backed up, and programs or other devices are employed to maintain the functionality, integrity, or security of the network infrastructure.

VI. Technology-based applications and hardware prohibited for employee and student use:

While ACPS does not prohibit any particular technology-based applications or hardware because of their educational implementation possibilities. There are guidelines in place as detailed in the Technology Acceptable Use Policy regarding inappropriate use including but not limited to:

- A. Some world-wide resources available on the Internet are not of educational value in a school setting and, if not filtered, should not be accessed.
- B. Students may access personal e-mail accounts and other forms of electronic communication with specific, written parental permission as provided on the Good Computer User Agreement, to the extent that access does not interfere with the educational process as determined by school staff. Student access to personal e-mail at school is intended for educational purposes and is not guaranteed to be private. No student may use Albemarle County Public Schools software or equipment to access any service for the purpose of conducting a purchase or participating in any other commercial activity.
- C. Employees should not use electronic mail for confidential matters or privileged communications, such as student education records, unless appropriate measures are taken to ensure confidentiality and to maintain the appropriate privilege. Employees shall adhere to all school, School Division, state and federal laws, policies and standards including the Family Education Rights and Privacy Act (FERPA).

Penalties:

- A. Inappropriate use will result in an immediate termination of access and other privileges relating to use and may also result in disciplinary action (up to and including suspension or expulsion, formal reprimand, or dismissal) as well as potential civil or criminal liability and prosecution.
- B. Administration, faculty, or staff may request that the systems administrator deny, revoke, or suspend specific user access in the event of violation of the Technology Acceptable Use policy.
- C. The use of computer resources is a privilege, not a right. Misuse of Internet access or a violation of this regulation may result in the account or the user's access privilege being denied, revoked, or suspended. Misuse may also subject the user to disciplinary action up to and including suspension, expulsion, formal reprimand, or dismissal as well as potential civil or criminal liability and prosecution. Any illegal activities will be reported to the appropriate agencies.

VIII. Procedures to address breaches of Internet and intranet security and safety:

- A. Administration, faculty, or staff may request that the systems administrator deny, revoke, or suspend specific user access in the event of violation of this policy.
- B. Maintaining the security of School Division computers, networks and other technology systems is of great importance and requires the cooperation and diligence of all users. Any user who identifies a security problem must notify the site administrator (principal or director) who must then notify the School Division Help Desk. The user shall not demonstrate the problem to others. Any user who

attempts or causes a breach of the system security shall have his/her privileges revoked and may be subject to any additional disciplinary and/or legal action.

Legal actions resulting from breaches:

- A. Inappropriate use will result in an immediate termination of access and other privileges relating to use and may also result in disciplinary action (up to and including suspension or expulsion, formal reprimand, or dismissal) as well as potential civil or criminal liability and prosecution.
- B. Use or transmission of any material in violation of any United States or state law is strictly prohibited. Also prohibited are the uses or transmission of the following: material protected by federal or state intellectual property laws; copyrighted material (except in accordance with School Board policy EGAAA); licensed material; threatening, harassing, or obscene material; and/or pornographic material. In addition, it shall be prohibited to access, attempt to access, use, or attempt to use the Internet or other computer network or non-network facilities for any other unauthorized purposes, including but not limited to commercial activities, introduction of viruses, and manipulation or corruption of systems, files, and other related resources.

- IX. **Ongoing professional development opportunities for each stakeholder group:** The Internet Safety plan below names all stakeholders in the “Implemented By:” section who will be provided guided ongoing professional development in the process of incorporating Internet Safety into the curriculum.
- X. **Community outreach activities that are consistent with the program’s goals:** In the detailed Internet Safety plan below, community outreach activities are detailed in the in the “Community Outreach” section of each component.
- XI. **Division procedures for the evaluation and revision of the AUP, including the Internet safety program:** The evaluation of the AUP occurs not only when mandated by the Virginia Department of Education but when determined as needed by ACPS to ensure the safety of division employees, students and network infrastructure.

TABLE OF CONTENTS

I. <u>Cyber Citizenship</u>	
A. K-2	
1. <i>Cyber Community Citizenship</i>	Page 6
B. 3-5	
1. <i>Cyber Community Citizenship</i>	Page 7
C. 6-8	
1. <i>Cyber Community Citizenship</i>	Page 10
D. 9-12	
1. <i>Security: Cyber Citizenship</i>	Page 12
2. <i>Social Issues</i>	Page 14
II. <u>Cyber Safety</u>	
A. K-2	
1. <i>Personal Safety</i>	Page 16
2. <i>Cyber Security</i>	Page 17
B. 3-5	
1. <i>Online Personal Safety</i>	Page 18
2. <i>Cyber Security</i>	Page 20
3. <i>Cyber Bullying</i>	Page 21
C. 6-8	
1. <i>Cyber Bullying and Harassment</i>	Page 22
2. <i>Predator Identification</i>	Page 24
D. 9-12	
1. <i>Privacy and the Internet</i>	Page 26
2. <i>Security: Malicious Code and Pornography on the Web</i>	Page 27
3. <i>Cyber Relationships & Harassment</i>	Page 27
III. <u>Intellectual Property</u>	
A. 3-5	
1. <i>Intellectual Property</i>	Page 29
B. 6-8	
1. <i>Intellectual Property</i>	Page 30
C. 9-12	
1. <i>Intellectual Property Theft</i>	Page 31

I. Cyber Citizenship

A. K-2

1. *Cyber Community Citizenship*

Page 6

B. 3-5

1. *Cyber Community Citizenship*

Page 7

C. 6-8

1. *Cyber Community Citizenship*

Page 10

D. 9-12

1. *Security: Cyber Citizenship*

Page 12

2. *Social Issues*

Page 14

I. Cyber Citizenship

A. K-2

1. *Cyber Community Citizenship*

a. Vocabulary

- (1) Cyberspace-Virtual Internet community in which real people interact through electronic means.
- (2) URL-Defined as Universal/Uniform Resource Locator, is another name for a Web address. The URL is located at the top of a web page and generally begins with <http://www>.
- (3) Netiquette-Blend of "network" and "etiquette" describing the informal code on Internet conduct.

b. Suggested Resources and Activities

- (1) (Grade K) iSafe: Cyber Community Citizenship-In this lesson, students will develop an understanding of the concept of community and apply it to knowledge of the Internet: compare the physical community to the abstract Cyberspace community. A discussion will take place after the song "I Got a Buddy" is played to introduce Internet safety. (Taught by CTIP, LMS when teaching the community unit, Classroom Teacher, Guidance, PE)
- (2) (Grades 1-2) iSafe: Cyber Community Citizenship-This lesson will reinforce the comparison of physical community to cyber community through discussion and in an activity mini-booklet. (Taught by CTIP, LMS, Classroom Teacher)
- (3) (Grades K-2) Website: <http://www.doe.virginia.gov/VDOE/Technology/OET/Internet-safety-guidelines.shtml> The Virginia Department of Education Office of Educational Technology Guidelines and Resources for Internet Safety in Schools; has a link at the bottom of its site to a long list of resources.

- (4) (Grades K-2) Website: www.NetSmartz.org/education Online curriculum and interactive/downloadable activities for students in K-2
- (5) (Grades K-2) Website: <http://www.safekids.com/kidsrules.htm> Printable pledge for kids to take to be safe
- (6) (Grades K-2) Website: http://www.cybersmartcurriculum.org/curr_over/ Additional curriculum ideas with scope and sequence

c. Implemented By:

- (1) 3-5 grade iMentors with Teachers teach Netiquette early in the year before or when doing a web-based activity
- (2) Additional support and instruction provided by LMS, Classroom Teacher and Guidance

d. Community Outreach

- (1) County-wide web-based resource
- (2) Coordinate a county-wide/city technology convention for parents, students and community members to include student projects, activities, robotics, resources, vendors, and Internet safety
- (3) Informative brochure created by ACPS for parents and students to review at home
- (4) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure all grade K-2 classrooms are visited by 3-5 graders

B. 3-5

1. Cyber Community Citizenship

a. Vocabulary

- (1) Cyberspace-Virtual Internet community in which real people interact through electronic means.
- (2) URL-Defined as Universal/Uniform Resource Locator, is another name for a Web address. The URL is located at the top of a web page and generally begins with <http://www>.
- (3) Bulletin Boards-Message boards, public areas on the Internet where messages or comments can be posted for other board members to read and reply to.
- (4) Posting-Placing a message or photo to an online message board or website.
- (5) Chat Room-A virtual room, or gathering place, for Internet users with shared interests to congregate and converse.
- (6) IM-Instant Messaging-Real time Internet communication. A "private chat room".
- (7) Screen name-Online name or nickname. An alias used in Cyberspace.
- (8) Buddy List-Instant message addresses of favorite users. List enabled designated users to know when their "buddy" is online so that both can easily communicate.

- (9) Flame-To send a mean or hurtful electronic message.
- (10) Mentors Club-iSafe website where Mentors exchange ideas, chat with other Mentors and learn Internet safety information to provide to their schools and communities.
- (11) Mentor "Link"-Adult in a school who helps iSafe Student Mentors organize events and activities.

b. Suggested Resources and Activities

- (1) (Grades 3-4) iSafe: Cyber Citizenship and Safety Online-This lesson compares real community to cyber community. Includes rules, community members and appropriate communications. (Taught by CTIP, LMS, classroom teacher, guidance, PE in context of classroom community and rules)
- (2) (Grade 3) iSafe: Cyber Community Citizenship-This lesson introduces terms such as URL, cyberspace, e-mail, etc. Many Internet concepts are introduced. Compares the physical community to the cyber community, and there's a folded book activity. (Taught by classroom teacher, CTIP, LMS)
- (3) (Grade 3) iSafe: Cyber Bullying-This lesson is all about being friendly vs. bullying. Delves into social interactions, feelings, compliments, etc. and, then, compares this to online treatments. (Taught by classroom teacher, guidance counselor, CTIP)
- (4) (Grade 3) iSafe: Personal Safety-This lesson uses the character iBuddy to address safety tips for the cyber community. Includes sample dialogue for the lesson as well as an FBI tips reference page and an online field trip via FBI kids' site. (Taught by Classroom teacher, CTIP, Guidance Counselor)
- (5) (Grades 3-5) iSafe: Music and Movement-This lesson includes the music for songs that can be used to teach about Internet safety. A CD can be ordered thru iSafe at a cost. Movement activities that go with lyrics and chants, etc. (Taught by music teacher, PE teacher, classroom teacher)
- (6) (Grades 3-5) iSafe: Text Messaging Safety-This lessons involves defining text messaging, IM'ing and the vocabulary that is associated with these forms of communication. It also includes personal and security consequences. (Taught by parents, any adult in the school that has to address the impact of text messaging within the educational setting)
- (7) (Grades 3-5) iSafe: Safety and Your Identity-This lesson differentiates between common information and personal information. It also allows discussions on identifying dangers and understanding consequences when personal information is shared. There's a song included that supports the objectives of this lesson. (Taught by Parents, all teachers and staff)
- (8) (Grade 4) iSafe: Personal Safety- This lesson focuses on making responsible choices while on the Internet and includes open-ended questions and activities. The lesson also includes mini-poster of tips and the link to FBI field trip. Spanish activity sheets available. (Taught by

CTIP, Guidance Counselor, classroom teacher, LMS, GRT)

- (9) (Grade 4) iSafe: Cyber Bullying-This lesson introduces netiquette. Great one-page posters that offer tips for display or home communication. Kids get a chance to edit a copy of an e-mail based on info learned in this lesson. Great integration of the OLWEUS anti-bullying model in ACPS. (Taught by Classroom teacher, CTIP, Guidance Counselor)
- (10) (Grade 5) iSafe: Cyber Community Citizenship-This lesson builds on 3rd-4th grade lessons in comparing physical community to cyber community. Students become mentors for other students, and there's an iMentor registration opportunity. There's a PowerPoint and a web activity that supports this lesson. Student activity includes comparing places of real life to cyber places and talks about appropriateness. (Taught by CTIP, LMS, Classroom Teacher, Guidance Counselor)
- (11) (Grade 5) iSafe: Cyber Bullying-This lesson builds on the 4th grade lesson and offers the same posters and tip sheets. It has a PowerPoint to support the lesson. New information includes IM'ing, and there's an IM aptitude test included. Real focus on Netiquette and what to do when bullying happens. Great integration of the OLWEUS anti-bullying model in ACPS. (Taught by CTIP, Classroom teacher, Guidance Counselor, LMS)
- (12) (Grade 5) iSafe Online Personal Safety Unit-This series of four separate lessons can be taught in a long session or in a series of shorter ones. There is a component on online predators and predator identification if this is deemed appropriate for your students. Other topics include choosing passwords, screen names, dealing with Internet strangers, reporting suspicious behaviors, etc. Includes a PowerPoint to use with lessons. (Taught by Classroom teacher, CTIP, Guidance Counselor, LMS)
- (13) (Grades 3-5) Website: An Internet Pledge for kids...
<http://www.safekids.com/kidsrules.htm>
- (14) (Grades 3-5) Website: Chart of acronyms used in text messaging, blogging, IM'ing...
<http://www.netlingo.com/e-mailsh.cfm>
- (15) (Grades 3-5) Website: Cyberethics for kids (interactive)
<http://www.cybercrime.gov/rules/kidInternet.htm>
- (16) (Grades 3-5) Website: Surf Swell Island (Disney)
http://disney.go.com/surfswell/index.html?name=ac_med6_surfSwell

c. Implemented By:

- (1) 6-8 Grade iMentors with Teachers during individual classroom visits to 3rd-5th grade classes
- (2) Guidance-in conjunction with bullying counseling
- (3) Additional support and instruction provided by LMS, GRT and Parents

d. Community Outreach

- (1) County-wide web-based resource

INTERNET SAFETY

Being educated and empowered to take control of online experiences.

- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Include in student handbook
- (4) Awareness Posters
- e. Follow-Up/Assessment
 - (1) CTIP coordinates program to be sure all grade 3-5 classrooms are visited by 6-8 graders

C. 6-8

1. *Cyber Community Citizenship*

a. Vocabulary

- (1) Chat Room-A virtual room, or gathering place, for Internet users with shared interests to congregate and converse.
- (2) IM-Instant Messaging-Real time Internet communication. A "private chat room".
- (3) Screen name-Online name or nickname. An alias used in Cyberspace.
- (4) Buddy List-Instant message addresses of favorite users. List enabled designated users to know when their "buddy" is online so that both can easily communicate.
- (5) YE-Youth Empowerment-iSafe campaign in which students take ownership of what they have learned by reaching out to others through peer-to-peer communication.
- (6) Mentors Club-iSafe website where Mentors exchange ideas, chat with other Mentors and learn Internet safety information to provide to their schools and communities.
- (7) Mentor "Link"-Adult in a school who helps iSafe Student Mentors organize events and activities.

b. Suggested Resources and Activities

- (1) (Grade 6) iSafe: Cyber Community Citizenship-Learners will be provided with reference materials to engage in an enrichment activity, which includes creating a simple awareness campaign about cyber community issue awareness at school and/or locally. (Taught by Guidance/Health Teacher/CTIP/Intervention Period Teacher/Teacher Advisory)
- (2) (Grade 6) iSafe: Integrated Literacy-Learners will review and reinforce the security concepts associated with interaction in the cyber community. Learners will then engage in an enrichment activity which involves reading developed stories to another class either inside own school or at neighboring school as appropriate. (Taught by Teacher Advisory/Facilitated in the Teacher Advisory Group in collaboration with the Classroom Teacher/CTIP/Intervention Period Teacher)
- (3) (Grade 6) iSafe: AUP's-In this lesson, learners will publicize the information found in the school's AUP, and/or, if necessary, make positive recommendations for change in the school's AUP. (Taught by CTIP/LMS/Intervention Period Teacher)
- (4) (Grade 7) iSafe: Negative Networking: A Look at Gangs Online-In this lesson, learners will

- be provided with background information to create a poster or flyer awareness campaign about online gang activity to promote safe online interaction. (Taught by Guidance/Health/CTIP/Teacher Advisory/Facilitated in the Teacher Advisory Group in collaboration with the Classroom Teacher)
- (5) (Grade 7) iSafe: Cyber Community Citizenship: Students will develop a comprehensive understanding of the concept of community and its application to the Internet. Learners will be provided with reference materials to engage in an enrichment activity, which includes writing articles for the school and/or local newspaper about what they learn regarding cyber citizenship. (Taught by Classroom Teacher/CTIP/Intervention Period Teacher/Teacher Advisory/Facilitated in the Teacher Advisory Group in collaboration with the Classroom Teacher)
- (6) (Grade 7) iSafe: AUP's: In this lesson, learners will publicize the information found in the school's AUP, and/or, if necessary, make positive recommendations for change in the school's AUP. (Taught by CTIP/LMS/Intervention Period Teacher)
- (7) (Grade 7) iSafe: Legal Trends in Cyber Safety and Security: Learners will interact in the classroom environment through group discussion and examination of current legal trends as they apply to central cyber safety and security issues. Learners will be provided with materials to engage in an enrichment activity, which involves helping to form policy by writing to an elected official concerning a legal cyber security/safety issue of their choice. Resources and information for further involvement in policy are also provided. (Taught by Health Teacher/CTIP)
- (8) (Grade 8) iSafe: Cyber Community Citizenship-Students will develop a comprehensive understanding of the concept of community and its application to the Internet. Learners will be provided with reference materials to engage in an enrichment activity, which includes creating an awareness poster campaign. (Taught by Classroom Teacher/CTIP/Intervention Period Teacher/Teacher Advisory/Facilitated in the Teacher Advisory Group in collaboration with the Classroom Teacher)
- (9) (Grade 8) iSafe: AUP's-In this lesson, learners will publicize the information found in the school's AUP, and/or, if necessary, make positive recommendations for change in the school's AUP. (Taught by CTIP/Principal/LMS/Intervention Period Teacher)
- (10) (Grade 8) iSafe: Cyber Security-Learners will become more familiar with online communication and consequences of uneducated interaction on the Internet such as virus downloading and cyber bullying. Learners will interact in the classroom environment through group discussion, and creation and presentation of skits on cyber security issues. (Taught by Health Teacher/CTIP/Intervention Period Teacher/Teacher Advisory/Facilitated in the Teacher Advisory Group in collaboration with the Classroom Teacher)

- c. Implemented By:
 - (1) Teachers (i.e. Technology Elective Teacher)-work in conjunction with CTIP on Youth Empowerment program for peer-to-peer communication
 - (2) CTIP-work in conjunction with Mentor Teacher on Youth Empowerment program for peer-to-peer communication
 - (3) Guidance-discuss in conjunction with bullying counseling
 - (4) Teacher Advisory Groups
 - (5) Additional support provided by Principal
- d. Community Outreach
 - (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Include in student handbook
 - (4) Student groups aid teachers of 3-5 students to implement iSafe program
- e. Follow-Up/Assessment
 - (1) CTIP coordinates program to be sure lessons are implemented

D. 9-12

1. Security: Cyber Citizenship

- a. Vocabulary
 - (1) YE-Youth Empowerment-iSafe campaign in which students take ownership of what they have learned by reaching out to others through peer-to-peer communication.
 - (2) PSA's (Public Service Announcements)-A TV or radio commercial that educates people on specific issues such as the need to be safe online.
- b. Suggested Resources and Activities
 - (1) (Grades 9-12) iSafe: Lesson on Legal Trends in Cyber Safety and Security-Student group discussion on current trends, writing letters to congressional leaders on the topic of their choice, and future involvement ideas
 - (2) (Grades 9-12) iSafe: Lesson on Online Freedoms and the Culture of the Internet Community-Students will take the online preassessments, students enroll in the iMentor program, teacher guides discussion about the Internet, students read an article about the cultural divide, students divide into groups and investigate Internet issues in the US and abroad and present their findings to the class, teacher leads class discussion on Internet freedoms, students host a parent/community night to inform on Internet safety
 - (3) (Grades 9-12) iSafe: Webcast Lesson on Security-Cyber Citizenship-Students take online preassessment, watch webcasts and discuss at predetermined breaks, students engage Community Leaders in a meeting to discuss issues

- (4) (Grades 9-12) iSafe: Service Learning Curriculum-Access materials to implement the iSafe program by students through service learning and using the iSafe Student Toolkit as a reference
- (5) (Grades 9-12) iSafe: Webcast Lesson on Social Issues-Watch webcasts and discuss at predetermined breaks, complete cooperative group exercises, create Internet safety message with film
- (6) (Grades 9-12) Include colleges and job impact information in lessons

c. Implemented By:

- (1) Health Teacher-teach lessons under personal safety theme
- (2) Government Teacher-teach legal trends and online freedoms
- (3) Social Studies Teacher-incorporate Internet safety into community service projects
- (4) Broadcast Studio Teacher, Leadership class, Key Club, Mentors Programs-work in conjunction with CTIP to enable Youth Empowerment program participants to create PSA's for the school
- (5) CTIP-work in conjunction with Mentor Teacher to enable Youth Empowerment program participants to create PSA's for the school and/or conduct sessions in the beginning of the year.
- (6) Guidance-discuss in conjunction with bullying counseling

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Include in student handbook
- (4) Put PSA's up on Public Access channel

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure lessons are implemented

2. *Social Issues*

a. Vocabulary

- (1) YE (Youth Empowerment)-iSafe campaign in which students take ownership of what they have learned by reaching out to others through peer-to-peer communication.
- (2) PSA's (Public Service announcements)-A TV or radio commercial that educates people on specific issues, such as the need to be safe online.

b. Suggested Resources and Activities

- (1) (Grades 9-12) iSafe: Lesson-Students take online assessments, students conduct community surveys, parents take a survey, students register in iMentor program
- (2) (Grades 9-12) iSafe: Lesson on Online Gambling-Students take online preassessment, teacher leads discussion about online gambling, students read and discuss Online

INTERNET SAFETY

Being educated and empowered to take control of online experiences.

- Gambling reference page, students debate issues of online gambling, discuss the debate as a class, iMentors conduct a Parent presentation
- (3) (Grades 9-12) iSafe: Webcast Lesson on Cyber Harassment-Bullying and Stalking Online- Students take online preassessment, watch webcasts and discuss at predetermined breaks, students start a poster/digital announcements campaign to promote anti-cyber bullying policy
 - (4) (Grades 9-12) iSafe: Webcast Lesson on Pornography on the Web-Students take online preassessment, watch webcasts and discuss at predetermined breaks, students start an iAdopt a school program to teach to lower grade levels
 - (5) (Grades 9-12) iSafe: Lesson on Online Relationships-Students take online preassessment, students enroll in the iMentors program, teachers engage students in discussion on online relationships, divide students in groups to complete an activity page to spur conversation, students present findings, teacher leads whole class discussion on online activities, students create a drop box for whole school to ask questions and express concerns about online safety
 - (6) (Grades 9-12) iSafe: Webcast Lesson on Cyber Relationships-Students take online preassessment, watch webcasts and discuss at predetermined breaks, students divide into groups and discuss cyber relationships and report back to class, an assembly experience on the topic occurs
- c. Implemented By:
- (1) Health Teacher-teach lessons under personal safety theme
 - (2) Broadcast Studio Teacher-work in conjunction with CTIP to enable Youth Empowerment program participants to create PSA's for the school
 - (3) CTIP-work in conjunction with Mentor Teacher to enable Youth Empowerment program participants to create PSA's for the school and helps to coordinate whole school presentation
 - (4) Guidance-in conjunction with bullying counseling
- d. Community Outreach
- (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Include in student handbook
 - (4) Put PSA's up on Public Access channel
- e. Follow-Up/Assessment
- (1) CTIP coordinates program to be sure lessons are implemented

II. Cyber Safety

A. K-2

- 1. *Personal Safety* Page 16
- 2. *Cyber Security* Page 17

B. 3-5

- 1. *Online Personal Safety* Page 18
- 2. *Cyber Security* Page 20
- 3. *Cyber Bullying* Page 21

C. 6-8

- 1. *Cyber Bullying and Harassment* Page 22
- 2. *Predator Identification* Page 24

D. 9-12

- 1. *Privacy and the Internet* Page 26
- 2. *Security: Malicious Code and Pornography on the Web* Page 27
- 3. *Cyber Relationships & Harassment* Page 27

II. Cyber Safety

A. K-2

1. *Personal Safety*

a. Vocabulary

(1) Internet Safety-Being educated and empowered to take control of online experiences.

b. Suggested Resources and Activities

- (1) (Grade K) iSafe: This lesson focuses on the reinforcement of the idea that it is unsafe to talk to strangers. Teachers will lead a discussion about why it is important to get help from an adult to make the Internet safe. A copy of an e-mail message is shared so students know what it looks like. The word stranger is discussed. (Taught by CTIP, LMS, Classroom Teacher, Guidance)
- (2) (Grade 1) iSafe: This lesson reinforces the discussions of strangers from (K) and discusses the importance of telling adults when the child feels uncomfortable and what to do about it. The iBuddy character is referred to again for reinforcement of what that character would do. The terms personal and permission are introduced. The FBI's 5 Internet Safety Tips are included to share. (Taught by CTIP, LMS, Classroom Teacher, Guidance, PE)
- (3) (Grade 2) iSafe: Safety and Identity- This lesson includes discussion of why everyone is special and different and focuses on the term/concept of identity. The use of the song

- “PRIVACY” from the purchased iSafe CD is available to reinforce the idea that personal identity/information is private, especially on the Internet. (Taught by CTIP, LMS, Classroom (4) teacher, Guidance, PE)
- (5) (Grades K-2) Website: <http://www.cybercrime.gov/rules/rules.htm> The U.S. Department of Justice Cybercrime site presents tips for online safety and privacy
- (6) (Grades K-2) Website: <http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/> Federal Trade Commission’s Kidz Privacy website

c. Implemented By:

- (1) Teachers-Teach in PE curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with PE teachers to implement in classroom.
- (3) Guidance in conjunction with bullying counseling
- (4) CTIP during a computer-based lesson

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure lessons are implemented

2. *Cyber Security*

a. Vocabulary

- (1) File-The specific location of data within a computer record.
- (2) Parental Controls-Special features or software packages that enable restricted access to Internet sites.

b. Suggested Resources and Activities

- (1) (Grades K-2) iSafe: This lesson develops the understanding that computers can become infected with viruses and that caution should be used when opening e-mail. The concepts of computer virus and how it can spread, and e-mail can carry viruses through attachments are discussed and are reinforced with a hands-on activity of making a mini-booklet. A discussion with open-ended questions is included. A selection from iSafe songs is a culminating activity. (Taught by CTIP, LMS, Classroom Teacher)
- (2) (Grade 1) iSafe: Safety and Identity-This lesson discusses how to differentiate between common information and personal information and what dangers lie in revealing personal information to strangers while online. Terms include: personal information, communication, Internet, online. (Taught by CTIP, LMS, Classroom Teacher, Guidance, PE)

- (3) (Grade 2) iSafe: This lesson reinforces an understanding of the need to make responsible choices to make sure students are safe while using the Internet. Dangers of Cyberspace are discussed. Posters, iBuddy e-mail and role-playing are included. (Taught by CTIP, LMS, Classroom Teacher, Guidance, PE)
 - (4) (Grades K-2) Website: <http://www.fbi.gov/fbikids.htm> Federal Bureau of Investigation
 - (5) (Grades K-2) Website: <http://www.isafe.org/> Non-profit foundation supporting online safety experiences
 - (6) (Grades K-2) Website: <http://www.getnetwise.org/> Resource for parents and children on how to keep kids and computers safe. It also has an extensive list of safe sites for kids and families
 - (7) (Grades K-2) Website: http://disney.go.com/surfswell/index.html?name=ac_med6_surfSwell Disney's interactive treasure hunt for learning how to be safe
 - (8) (Grades K-2) Website: <http://pbskids.org/license/> Official "Get Your Web License"
 - (9) (Grades K-2) Website: <http://www.kidscomjr.com/games/safety/safety.html> Iggy and Rasper's Tips for Internet Safety and Good Manners
- c. Implemented By:
- (1) Teachers-Teach in PE curriculum in conjunction with OLWEUS Committee.
 - (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with PE teachers to implement in classroom.
 - (3) Additional support and instruction provided by CTIP, LMS, Classroom Teacher, Guidance, PE
- d. Community Outreach
- (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home.
 - (3) Whole school presentation to include parents and community
 - (4) Include in student handbook
- e. Follow-Up/Assessment
- (1) CTIP coordinates program to be sure lessons are implemented

B. 3-5

1. *Online Personal Safety*

a. Vocabulary

- (1) Internet Safety-Being educated and empowered to take control of online experiences.
- (2) Identifying Information-Personal information that can be used by online predators to distinguish you from another person and possibly to find you in real life (e.g.: name, gender, age, etc.).

b. Suggested Resources and Activities

- (1) (Grades 3-5) iSafe: Spam Scam Safety-Lesson involves discussion on SPAM. (in Spanish and English) (Taught by CTIP, Classroom Teacher)
- (2) (Grades 3-5) iSafe: Spyware Risks and Acceptable Use Policies-Two lessons that offer more advanced discussions on Cybersecurity risks and the need for institutional AUP's. AUP PowerPoint available. (Taught by CTIP, LMS, Classroom Teacher)
- (3) (Grades 3-5) Website: Additional resources and easy to read scope and sequence chart. http://www.cybersmartcurriculum.org/curr_over/
- (4) (Grades 3-5) Website: More education for teachers, including publications... <http://csriu.org/index.html>
- (5) (Grades 3-5) Website: Another web resource that offers online and hard copy activities, animated characters in the lesson plans, etc. <http://www.netsmartz.org/>
- (6) (Grades 3-5) Website: An online field trip for Internet safety by FBI <http://www.fbi.gov/kids/k5th/safety2.htm>
- (7) (Grades 3-5) Website: Safety tips for various age groups and more http://www.bewebaware.ca/english/safety_tips_8_10.aspx
- (8) (Grades 3-5) Website: Additional resources on Internet Safety topics, and detailed glossary of terms <http://www.getnetwise.org/>
- (9) (Grades 3-5) Website: Printable Internet safety poster for upper elementary <http://www.cybersmart.org/for/kids.asp>
- (10) (Grades 3-5) Website: "Get Your Web License", an interactive PBS site <http://pbskids.org/license/>
- (11) (Grades 3-5) Website: Iggy and Rasper's Internet Safety Game <http://www.kidscomjr.com/games/safety/safety.html>
- (12) (Grades 3-5) Website: Online safety quiz <http://www.safekids.com/quiz/index.html>

c. Implemented By:

- (1) Teachers-Teach in PE curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.
- (3) Additional support and instruction provided by CTIP and LMS.

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook

e. Follow-Up/Assessment

INTERNET SAFETY

Being educated and empowered to take control of online experiences.

(1) CTIP coordinates program to be sure lessons are implemented

2. *Cyber Security*

a. Vocabulary

- (1) File-The specific location of data within a computer record.
- (2) File Extensions-The three or more letters at the end of a file name (e.g.: .exe, .jpg, and .doc) defining the file "type", such as a text file, executable file, database file, or graphic file.
- (3) Parental Controls-Special features or software packages that enable restricted access to Internet sites.
- (4) Firewall-Set of related hardware and software programs designed specifically to protect a computer or computer network from unauthorized external use.
- (5) Code-Written instructions in a computing language.
- (6) Malicious Code-Intentionally destructive computer program (e.g.: viruses, worms, and Trojan horses).
- (7) Anti-virus-Software that protects a computer from malicious code.
- (8) SPAM-Mass mailing or posting of messages. Also known as Internet junk mail.
- (9) Flame-To send a mean or hurtful electronic message.
- (10) FW (Forward)-Informs the recipient a redirected message has been sent to them. The sender is not the author and, therefore, is suspicious.
- (11) Phishing-Phishing attacks use "spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data (see "Spoofs/Spoofing").

b. Suggested Resources and Activities

- (1) (Grade 3) iSafe: *Cyber Security*-This lesson involves making responsible choices while using the Internet. This lesson introduces computer viruses and compares to health. Activity includes a mini-booklet to make. Spanish activity sheets available. (Taught by Classroom teacher, CTIP, LMS)
- (2) (Grade 4) iSafe: *Cyber Security*-This lesson involves all of gr. 3 lessons and builds into more in-depth vocabulary and concepts. Lesson includes a sample dialogue that the teacher can use. Introduces terms like attachment and more virus terminology. Mini-booklet available. (Taught by Classroom teacher, CTIP, Guidance Counselor, LMS)
- (3) (Grade 5) iSafe: *Cyber Security*-This lesson introduces malware, malicious, and code terms. It also involves proper e-mail protocols, etc. This lesson can be done with or without computers and involves a Handshake game that demonstrates how viruses spread, and discusses opening attachments, etc. This lesson involves the student as mentor and offers opportunity to register with iSafe. Other terms introduced: phishing, flaming, forwarding, spamming. PowerPoint and web activity available. (Taught by CTIP, Classroom Teacher, LMS)

- c. Implemented By:
 - (1) Teachers-Teach in PE curriculum in conjunction with OLWEUS Anti-Bullying Committee.
 - (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with PE teachers to implement in classroom.
 - (3) Additional support provided by CTIP, LMS and Guidance.
- d. Community Outreach
 - (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Whole school presentation to include parents and community
 - (4) Include in student handbook
- e. Follow-Up/Assessment
 - (1) CTIP coordinates program to be sure lessons are implemented

3. *Cyber Bullying*

- a. Vocabulary
 - (1) Flame-To send a mean or hurtful electronic message.
- b. Suggested Resources and Activities
 - (1) (Grade 5) iSafe: Cyber Bullying Lesson-After completing a KEWL sheet, learners will be provided with reference materials to engage in an enrichment activity, which includes creating a Pledge Wall about cyber bullying awareness at the school. (Taught by Health Teacher)
- c. Implemented By:
 - (1) Teachers-Teach in PE curriculum in conjunction with OLWEUS Anti-Bullying Committee.
 - (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with PE teachers to implement in classroom.
- d. Community Outreach
 - (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Whole school presentation to include parents and community
 - (4) Include in student handbook
- e. Follow-Up/Assessment
 - (1) CTIP coordinates program to be sure lessons are implemented

C. 6-8

1. *Cyber Bullying and Harassment*

- a. Vocabulary
 - (1) Code-Written instructions in a computing language.

- (2) Malicious Code-Intentionally destructive computer program (e.g.: viruses, worms, and Trojan horses).
- (3) Trojan Horse-A malicious code that appears harmless yet launches a virus or worm.
- (4) Virus-Executable code (computer program) that infects or attaches itself to other executable code in order to cause destructive computer events.
- (5) Worm-Self-propagating computer virus embedded in a file.
- (6) Anti-virus-Software that protects a computer from malicious code.
- (7) Firewall-Set of related hardware and software programs designed specifically to protect a computer or computer network from unauthorized external use.
- (8) Attachment-A data file sent from one computer to another along with an e-mail or an instant message.
- (9) FW (Forward)-Informs the recipient a redirected message has been sent to them. The sender is not the author and, therefore, is suspicious.

b. Suggested Resources and Activities

- (1) (Grade 6) iSafe: Negative Networking: A Look at Gangs Online Lesson-In this lesson, learners will be provided with background information to create a poster or flyer awareness campaign to promote safe online interaction. (Taught by Health Teacher)
- (2) (Grade 6) iSafe: Safety in Online Gaming Lesson-Students will understand the concept of online gaming, its safety and security risks, and develop an action plan for informing others of how to play online safely. (Taught by Health Teacher/Intervention Period/Broadcast)
- (3) (Grade 6) iSafe: Cyber Bullying Lesson-After completing a KEWL sheet, learners will be provided with reference materials to engage in an enrichment activity, which includes creating a Pledge Wall about cyber bullying awareness at the school. (Taught by Health Teacher)
- (4) (Grades 6-7) iSafe: Risks of Spyware Lesson-In this lesson, learners will develop Public Service Announcements (PSA) to inform others about spyware. The enrichment activity will provide guidance to broadcast one or more of the PSA's at school or through local news media. (Taught by CTIP/Broadcast Teacher)
- (5) (Grades 6-7) iSafe: Cyber Security Lesson-Learners will develop an understanding of proper e-mail protocol, and the necessity of using caution when opening e-mail to protect computer security and inform others about cyber security issues. (Taught by CTIP/Health Teacher)
- (6) (Grades 6-8) iSafe: Safe Website Design Lesson-Learners will design and build a website using Internet safety principles. (Taught by Health Teacher/CTIP/Exploratory Teacher)
- (7) (Grade 7) iSafe: Cyber Harassment Lesson-Learners will develop an awareness of the problems associated with cyber communication and the various aspects of cyber

- harassment including cyber bullying and cyber stalking. This awareness will lead to an understanding of safer Internet usage to minimize risks. (Taught by Health Teacher)
- (8) (Grade 7) iSafe: Cyber Harassment Lesson-The current lesson format is designed to provide an opportunity to write a story for younger children to be shared in a school setting. (Taught by Language Arts Teacher)
- (9) (Grade 7) iSafe: Cyber Security Lesson-Learners will become more familiar with online communication and consequences of uneducated interaction on the Internet such as virus downloading and cyber bullying. Learners will interact in the classroom environment through group discussion, and creation and presentation of skits on cyber security issues. (Taught by CTIP/Language Arts Teacher)
- (10) (Grade 7) iSafe: Introduction to Graphs with Internet Safety Lesson-Learners will continue developing their understanding of online dangers through a math-themed lesson aimed at reinforcing basic graphing skills. Students will be introduced to the bar graph and practice making bar graphs. (Taught by Math Teacher)
- (11) (Grade 7) iSafe: Online Shopping Risks Lesson-Learners will interact in the classroom environment through group discussion and examination of various online shopping sites using a self-created evaluation tool. Learners will develop and publicize an informational web page about safe online shopping. (Taught by Classroom Teacher/Broadcast Teacher)
- (12) (Grade 7) iSafe: Social Networking in Online Communities Lesson-Learners will become familiar with the various types of online communities, including dangers and benefits associated with online social networking, and tips for safe and secure online communication. In this lesson, learners will be provided with reference materials to develop and broadcast public service announcements to inform their peers about safe online social networking. (Taught by CTIP/Broadcast Teacher/Intervention Period Teacher)
- (13) (Grade 7) iSafe: Web Logs – A Positive Approach to Blogging Lesson-Learners will model safe and secure blogging techniques through the maintenance of a blog concerning ongoing school events and activities. (Taught by Language Arts Teacher)
- (14) (Grades 7-8) iSafe: Safety in Online Gaming Lesson-Learners will interact in the classroom environment through group discussion and the creation of an online gaming creed. (Taught by Health Teacher/Intervention Period Teacher/Broadcast)
- (15) (Grades 7-8) iSafe: Cyber Bullying Lesson-Students will practice netiquette as they communicate with others on the Internet and develop resources to cope with online bullying. (Taught by Health Teacher)
- (16) (Grade 8) iSafe: Negative Networking: A Look at Gangs Online Lesson-In this lesson, learners will be provided with background information to create a poster or flyer awareness campaign to promote safe online interaction. Learners will identify ways online communities

can be used in negative ways; become familiar with the negative ways the Internet is being used to network gangs and gang activity; identify online services designed to counteract negative online activity; discuss how online gang interaction can help authorities; identify online gang activity that needs to be reported to authorities immediately; and to know to whom to report online gang activity. (Taught by Health Teacher)

c. Implemented By:

- (1) Teachers-Teach in health curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.
- (3) Additional support and instruction provided by CTIP.

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure lessons are implemented

2. *Predator Identification*

a. Vocabulary

- (1) Identifying Information-Personal information that can be used by online predators to distinguish you from another person and possibly to find you in real life (e.g.: name, gender, age, etc.).

b. Suggested Resources and Activities

- (1) (Grade 6) iSafe: Predator Identification Lesson-Students will be able to identify the characteristics of tactics used by an online predator and make wise choices while interacting online. (Taught by Health Teacher)
- (2) (Grade 6) iSafe: Willing Participant Lesson-Learners will create a poster or bulletin board to inform others about strangers on the Internet and to provide strategies to stay safe in online communication. (Taught by Health Teacher)
- (3) (Grade 7) iSafe: Predator Identification Lesson-Learners will be provided with materials to engage their parents in an online survey about Internet safety issues. Students will be able to identify the characteristics of tactics used by an online predator and make wise choices while interacting online. (Taught by Health Teacher)
- (4) (Grade 7) iSafe: Willing Participant Lesson-Learners will create a poster or bulletin board to inform others about strangers on the Internet and to provide strategies to stay safe in online communication. Students will understand the concept of willing participation understand the

- safety risks of pursuing online relationships/friendships. (Taught by Health Teacher)
- (5) (Grade 8) iSafe: Predator Identification Lesson-Students will be able to identify the characteristics of tactics used by an online predator and make wise choices while interacting online. (Taught by Health Teacher)
- (6) (Grade 8) iSafe: Willing Participant Lesson-Students will understand the concept of willing participation and understand the safety risks of pursuing online relationships/friendships. Learners will create a poster or bulletin board to inform others about strangers on the Internet and to provide strategies to stay safe in online communication. (Taught by Health Teacher)
- c. Implemented By:
- (1) Teachers-Teach in health curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.
- d. Community Outreach
- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home.
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook
- e. Follow-Up/Assessment
- (1) CTIP coordinates program to be sure lessons are implemented

D. 9-12

1. Privacy and the Internet

- a. Vocabulary
- (1) Identity Theft-When someone uses your personal info (e.g.: Social Security #, credit card #) to steal your identity for illegal purposes. The fastest-growing crime in the U.S.
- (2) Phishing-Phishing attacks use "spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data (see "Spoofs/Spoofing").
- (3) Spoofs/Spoofing-Fake e-mail messages or web pages mimicking those of legitimate businesses in order to trick you into providing personal information (identity theft).
- b. Suggested Resources and Activities
- (1) (Grades 9-12) iSafe: Lesson on Identity Theft-Students take online preassessment, enroll in iMentors program, students discuss identity theft issues, students prepare a presentation for parents on identity theft
- (2) (Grades 9-12) iSafe: Lesson on Homeland Security-Students take online preassessment, enroll in iMentors program, teacher leads discussion on cyber issues related to homeland

security, students complete CD-ROM or paper-based activity, students share out what they learned, students take online post-assessment

(3) (Grades 9-12) iSafe: Webcast on Privacy and the Internet-Students take the online preassessment, students watch the webcast, teacher leads three directed discussion breaks during the webcast, students participate in cooperative group exercises at the conclusion of the webcast, students participate in the iAdopt a school program to share findings to lower grade levels, students take the online post-assessment

(4) (Grades 9-12) iSafe: Lesson on Online Privacy-Students take online preassessment, teacher guides discussion on online privacy, students take online privacy survey, teacher leads whole-class discussion of survey, students write a letter to the editor on this issue, students complete the online post-assessment

(5) (Grades 9-12) iSafe: Lesson on Online Shopping-Students take online preassessment, teacher leads class discussion on online shopping, in groups, students brainstorm what can go wrong in online shopping, students read and discuss an online shopping reference page, in groups, students complete an online shopping evaluation form activity and explain their findings, teacher leads whole class concluding discussion, students create a brochure to educate others, students take the online post-assessment

c. Implemented By:

(1) Teachers-Teach in health curriculum in conjunction with OLWEUS Anti-Bullying Committee.

(2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.

d. Community Outreach

(1) County-wide web-based resource

(2) Informative brochure created by ACPS for parents and students to review at home

(3) Whole school presentation to include parents and community

(4) Include in student handbook

e. Follow-Up/Assessment

(1) CTIP coordinates program to be sure lessons are implemented

2. *Security: Malicious Code and Pornography on the Web*

a. Vocabulary

(1) Looping-Website code that does not allow a visitor to exit. Feature of many adult Internet sites.

b. Suggested Resources and Activities

(1) (Grades 9-12) iSafe: Webcast Lesson on Cyber Security-Malicious Code-Student take online preassessment, students watch the webcast and participate in three teacher-facilitated student discussion breaks during the webcast, students participate in cooperative

group exercises at the conclusion of the webcast which include implementation of a plan for an Information table, students take the online or post-assessment

c. Implemented By:

- (1) Teachers-Teach in health curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure lessons are implemented

3. *Cyber Relationships & Harassment*

a. Vocabulary

- (1) SPAM-Mass mailing or posting of messages. Also known as Internet junk mail.

b. Suggested Resources and Activities

- (1) iSafe: Lesson on Online Social Networking-Students take online preassessment, teacher leads online social networking discussion, in groups or individually, students share what they have learned about online risks and create posters or webpages with safety tips, teacher leads class discussion, students help to create a student advisory board on online social networking, students take online post-assessment

c. Implemented By:

- (1) Teachers-Teach in health curriculum in conjunction with OLWEUS Anti-Bullying Committee.
- (2) OLWEUS Anti-Bullying Committee-Give whole school presentation and work with health teachers to implement in classroom.

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home.
- (3) Whole school presentation to include parents and community
- (4) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP coordinates program to be sure lessons are implemented

III. Intellectual Property

A. 3-5

1. Intellectual Property

Page 29

B. 6-8

1. Intellectual Property

Page 30

C. 9-12

1. Intellectual Property Theft

Page 31

III. Intellectual Property

A. 3-5

1. Intellectual Property

a. Vocabulary

- (1) Copyright-The exclusive rights to reproduce, publish, and sell things produced by the person who owns the copyright.
- (2) Intellectual Property-Material protected by copyright laws including songs, movies, software, and books.
- (3) Download-To copy information (data) from the Internet.
- (4) Plagiarism-Stealing someone else's work and pretending it's yours.

b. Suggested Resources and Activities

- (1) (Grade 3) iSafe: Be Responsible with Intellectual Property Lesson-Introduces the basic concept of what is intellectual property, using it from the Internet, and citing sources. Lesson provides a sample dialogue of exactly what to say. There's a "Cite your Source" activity with iBuddy worksheet. (Taught by Classroom teacher, LMS, CTIP, GRT, any other adults that work with students and conduct Internet research)
- (2) (Grade 4) iSafe: Intellectual Property Lesson-Students will learn the basic concepts of property and intellectual property and understand the basics of how to cite a source. Students will learn how to cite a source correctly. This lesson has great reference pages. Spanish pages available. (Taught by Classroom teacher, LMS, CTIP, GRT, any adult involved in research with students)
- (3) (Grade 5) iSafe: Intellectual Property-This lessons goes more in-depth on intellectual property. Provides K-W-L charts, scenarios, a PowerPoint, a web activity and reference sheets. Introduces copyright and plagiarism terms. (Taught by Classroom Teacher, LMS, CTIP, GRT and any adult that does research with students)

c. Implemented By:

- (1) LMS-in conjunction with Educational databases instruction

- (2) Teachers-providing a reference poster and/or weblink to put in all classrooms
- (3) Additional support and instruction provided by CTIP and GRT
- d. Community Outreach
 - (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Include in student handbook
- e. Follow-Up/Assessment
 - (1) CTIP follows up with LMS to be sure all classes participate

B. 6-8

1. Intellectual Property

- a. Vocabulary
 - (1) Copyright-The exclusive rights to reproduce, publish, and sell things produced by the person who owns the copyright.
 - (2) Intellectual Property-Material protected by copyright laws including songs, movies, software, and books.
 - (3) Download-To copy information (data) from the Internet.
 - (4) Plagiarism-Stealing someone else's work and pretending it's yours.
 - (5) Piracy-Theft to produce counterfeit copyrighted software and other material.
- b. Suggested Resources and Activities
 - (1) (Grade 6) iSafe: iSafe Intellectual Property Unit- Students take online preassessment, students enroll in the iMentors program, teacher/LMS guides discussion on tangible vs. intangible (intellectual) property and link copyright to the concept, students complete an activity chart with or without computers to understand why intellectual property needs to be governed leading to developing a slogan campaign on intellectual property, students take online post-assessment. There are PowerPoints to supplement discussion. (Taught by LMS/Language Arts Teacher)
 - (2) (Grade 7) iSafe: Plagiarism and the World Wide Web Lesson-Students will define plagiarism, identify how plagiarism occurs, and understand the basic guidelines for fair use of intellectual property. (Taught by LMS/Language Arts or Social Studies Teacher)
 - (3) (Grades 7-8) iSafe: Plagiarism and the World Wide Web Lesson-Students will define plagiarism, identify how plagiarism occurs, and understand the basic guidelines for fair use of intellectual property. (Taught by LMS/Language Arts or Social Studies Teacher)
 - (4) (Grades 7-8) iSafe: P2P (Peer to Peer) Networking Lesson-Students identify the safety, security risks, and legal issues surrounding P2P networks. (Taught by CTIP/Intervention Period Teacher)

- (5) (Grades 7-8) iSafe: Learn Before You Burn Lesson-Students will take a survey about their own illegal download behavior and learn about the consequences of piracy. (Taught by LMS/Intervention Period Teacher)
- (6) (Grade 7) iSafe: Donny the Downloader on All About Piracy Lesson-Students create and display a slogan poster or website banner to create awareness about piracy. (Taught by LMS/Exploratory Teacher)
- (7) (Grade 8) iSafe: Mock Trial Activity-Students act out a mock trial about intellectual property based on a provided script. (Taught by Civics Teacher/Intervention Period Teacher)
- (8) (Grade 8) iSafe: Intellectual Review PowerPoint Lesson-Students view a PowerPoint about intellectual property and have a discussion about property rights. (Taught by LMS/Intervention Period Teacher)
- c. Implemented By:
 - (a) LMS-in conjunction with educational databases instruction
 - (b) Teachers-providing a reference poster and/or weblink to put in all classrooms
- d. Community Outreach
 - (1) County-wide web-based resource
 - (2) Informative brochure created by ACPS for parents and students to review at home
 - (3) Include in student handbook
- e. Follow-Up/Assessment
 - (1) CTIP follows up with LMS to be sure all classes participate

C. 9-12

1. Intellectual Property Theft

- a. Vocabulary
 - (1) Copyright-The exclusive rights to reproduce, publish, and sell things produced by the person who owns the copyright.
 - (2) Intellectual Property-Material protected by copyright laws including songs, movies, software and books.
 - (3) Download-To copy information (data) from the Internet.
 - (4) Plagiarism-Stealing someone else's work and pretending it's yours.
 - (5) Piracy-Theft to produce counterfeit copyrighted software and other material.
- b. Suggested Resources and Activities
 - (1) (Grades 9-12) iSafe: Lesson on Copyright and Fair Use-Students take online preassessment, teacher/LMS guides copyright and fair use discussion, students read and discuss copyright reference page, students complete activity sheets by conducting research, discuss the activity as a class, students make brochures to inform others of their findings.

- (2) (Grades 9-12) iSafe: Lesson on Learn B4U Burn-Students take online preassessment, enroll in the iMentors program, teacher/LMS guides class discussion on intellectual property, divide students into groups to conduct research on intellectual property from a certain viewpoint, groups present their viewpoints to the class, students complete a free-write activity discussing impact of illegal downloading, students take online post-assessment
- (3) (Grades 9-12) iSafe: Webcast Lesson on Intellectual Property-students take the online preassessment, students watch the webcast and participate three teacher-facilitated student discussion breaks during the webcast, participate in cooperative group exercises at the conclusion of the webcast, students prepare to give a presentation on Intellectual Property to the school or lower grade-level schools, take the online post-assessment

c. Implemented By:

- (1) LMS-in conjunction with Educational databases instruction
- (2) Teachers-providing a reference poster and/or weblink to put in all classrooms

d. Community Outreach

- (1) County-wide web-based resource
- (2) Informative brochure created by ACPS for parents and students to review at home
- (3) Include in student handbook

e. Follow-Up/Assessment

- (1) CTIP follows up with LMS to be sure all classes participate

ACCEPTABLE USE OF TECHNOLOGY

Internet and computer network and non-network access is available to authorized students, teachers, and other staff in the Albemarle County Public Schools. Albemarle County Public Schools' primary goal for technology use in education is to promote educational excellence by facilitating resource sharing, innovation, and telecommunications as outlined in this policy and applicable regulations. However, some world-wide resources available on the Internet are not of educational value in a school setting.

Students and/or their parents or other legal guardians shall, prior to beginning grades K, 3, 6 and 9 or otherwise entering a school, receive and sign an acknowledgment of this Policy and return same to the appropriate individual school. The school shall maintain an accurate record of who has returned the signed acknowledgment and shall respond accordingly.

Use of the Albemarle County Public Schools' Internet and computer facilities is a privilege, not a right. Inappropriate use will result in an immediate termination of access and other privileges relating to use and may also result in disciplinary action (up to and including suspension or expulsion, formal reprimand, or dismissal) as well as potential civil or criminal liability and prosecution.

Use or transmission of any material in violation of any United States or state law is strictly prohibited. Also prohibited are the uses or transmission of the following: material protected by federal or state intellectual property laws; copyrighted material (except in accordance with School Board policy EGAAA); licensed material; threatening, harassing, or obscene material; and/or pornographic material. In addition, it shall be prohibited to access, attempt to access, use, or attempt to use the Internet or other computer network or non-network facilities for any other unauthorized purposes, including but not limited to commercial activities, introduction of viruses, and manipulation or corruption of systems, files, and other related resources.

Administration, faculty, or staff may request that the systems administrator deny, revoke, or suspend specific user access in the event of violation of this policy.

Adopted: August 26, 1996
Amended: February 22, 1999; April 22, 2004

ACCEPTABLE USE OF TECHNOLOGY

Use of the Internet

Through the Internet, students and staff in the Albemarle County Public Schools have access to a variety of resources, including but not limited to:

1. World-wide electronic mail.
2. Library catalogs from around the world, including the Library of Congress.
3. Electronic databases and encyclopedias.
4. The World-Wide Web, a collection of Internet Resources.

Liability

1. The Albemarle County Public Schools will not guarantee the availability of access to the Internet and will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties.
2. The accuracy and quality of information obtained cannot be guaranteed, nor can information sent or received be assured to be private.
3. Albemarle County Public Schools retains control, custody, and supervision of all electronic resources owned or leased by it. Any information generated, stored or sent through electronic resources is the same as any written documentation and may be subject to Freedom of Information Act inquiries, etc. The School Division reserves the right to monitor all use of electronic resources by employees and other users. There shall be no expectation of privacy of information on any equipment owned or leased by or operated within Albemarle County Public Schools.
4. In accordance with § 22.1-70.2 of the Code of Virginia, Albemarle County Public Schools has implemented a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 of the Code of Virginia and obscenity as defined in § 18.2-372 of the Code of Virginia.

Responsibilities of School Staff and Standards for Technology Use

1. Staff members assigning or permitting Internet use will seek to prevent access by students to material that the school division deems to be harmful to juveniles, and as defined in § 18.2-390 of the Code of Virginia.
2. Staff members assigning student Internet use will recommend safe search strategies and resources which meet the curricular needs of the assignment and the developmental level of the student.
3. Staff members assigning or permitting Internet use will **plan instruction utilizing materials provided through the Division's Internet Safety Program.** ~~provide or arrange for instruction in acceptable use of the Internet based on information or materials provided by the Office of Instruction.~~ Topics to be addressed include:
 - a. Content of this Policy and Regulations
 - b. Generally accepted rules of network etiquette and safety

- c. Copyright guidelines
 - d. **Internet Safety**
 - e. **Other acceptable use/safety related topics**
 - f. Respect for use of time and resources
 - g. Evaluating sites for appropriateness and validity
 - h. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity.
4. All Albemarle County employees have the opportunity to publish Internet home pages, facilitated by the school or department Web Page Coordinator (or administrator's designee). Home pages must adhere to all applicable Albemarle County Public Schools guidelines.
 5. With appropriate notification and/or permission, student projects and other material relating to individual students may be published on the school division web server. In all cases, content must be appropriate and relevant to the mission and the business of the school division. Consent is obtained when a parent signs a hard copy of the Web Publishing Permission Form included in these Regulations. In no case shall information about a student such as home phone number, personal e-mail address, etc. be published.
 6. The use of the Internet to facilitate the purchase of school supplies, instructional resource materials or other products intended for use by students or staff must follow Albemarle County purchasing guidelines and all applicable policies.
 7. Students may not use staff members' e-mail accounts. Class accounts may be used by students under the direct supervision of the person to whom the account was issued. Teachers must apply for a class account by submitting an AUTHSCHLS form to their principal for approval.
 8. Audits of account information are routinely conducted. Accounts deemed dormant are investigated and may be removed.
 9. School Division employees may not abuse their access to technology systems. Abuse may consist of either excessive or unacceptable use. Generally, a use is unacceptable if it conflicts with the School Division's or individual School's or Department's purpose, goal, or mission or with an employee's authorized job duties or responsibilities. Incidental personal use of School Division technology systems must not interfere with the employee's job performance, must not violate any of the rules contained in this policy or any other policy and must not damage any hardware, software or communications system.
 10. Staff shall report any incident of harassment or any other unauthorized or inappropriate use of technology encountered over School Division computer resources to the building or department administrator who will report it to the Assistant Director, Office of Technology as appropriate.
 11. Staff and students shall not use access to technology systems for private financial gain, including the conduct of commercial activity for any business in which there is a personal interest, or for advertising or solicitation purposes.
 12. Staff shall not use School Division technology systems for personal, non-School Division purposes to solicit, proselytize, advocate or communicate the views of an individual or of non-school sponsored organizations except through means that have been provided specifically for such purposes (e.g., County Bulletin Board). However, the School Division recognizes that employees have the right to speak out on matters of public concern, and this provision shall not be construed to restrict or prohibit the legal rights of employees to

- engage in speech that is protected under federal or state laws.
13. School Division employees who, based upon job responsibilities, have access to monitor the technology use of students or staff must follow guidelines established by the site administrator (school principal or administrative director). These guidelines shall be placed on file with the Office of Technology.
 14. Any Office of Technology employee monitoring the technology use of students or staff must follow established site-based or District-level guidelines, a copy of which is included in these regulations.
 15. Global Distribution Lists exist to facilitate communication, in the conduct of school or Division business, with specified groups of staff. Use of Global Distribution Lists is limited to the business of the School Division. Sending mass e-mails to School Division employees or outside parties for non-school purposes is prohibited.
 16. Public Folders are created to provide multiple users an efficient means of communicating information, with either specified groups of School Division employees or with all School Division employees, in order to conduct the business of the School Division. Public folders will be created if and only if they serve the purpose of facilitating such communications. Public Folders should be used only for the purposes for which they were created. They are not a forum for the expression of personal opinions and should not conflict with the School Division's purpose, goal, or mission or with an employee's authorized job duties or responsibilities. The County Bulletin Board has been established to provide a single, non-work related avenue for employees to communicate non-work related business such as advertising, promoting non-School Division sponsored events, etc. The content of items posted on the County Bulletin Board must remain within acceptable limits for employee conduct.
 17. E-mail accounts are established only upon the receipt by the Office of Technology of a valid AUTHSCHLS form. E-mail accounts should be requested if and only if an employee must have access in order to fulfill the requirements of his or her job. Employees with e-mail accounts are responsible for maintaining their accounts in a manner that promotes the conservation of School Division resources. E-mail system backups are maintained for short periods of time for the purpose of disaster recovery only. Individual users are responsible for their own backups. E-mail communications may be subject to Freedom of Information Act inquiries.
 18. E-mail attachments should be used only when necessary. File attachments should be in a format that can be opened by the recipient and of a type appropriate to the content being transmitted. Files that are platform dependent or require the user to have software that is not commonly available are often unusable and waste Division resources.
 19. The creation of, change to, or deletion of employee e-mail accounts is accomplished by the submission of an AUTHSCHLS form to the Office of Technology. Forms should be accurately completed, signed by the appropriate supervisor, and submitted in a timely manner.
 20. All technology-related purchases or product demonstrations, including consultant and development services, must comply with the guidelines presented in the Division's Comprehensive Technology Plan.

Student teachers are not eligible for e-mail accounts as their work within the School Division is conducted under the direct supervision of the cooperating teacher/counselor. However, an AUTHSCHLS form, listing a university or private e-mail address, should be submitted to the Office of Technology. Their names will then appear in the Division's Global e-mail Address Book, and may be added to school distribution lists. Administrative interns are employees of the School Division and, as such, do receive e-mail accounts.

Responsibilities of Users and Standards for Technology Use

General Guidelines for Students

1. Students will comply with the Good Computer User Agreement they have signed.
2. Students will only access the Internet using school computer resources under appropriate supervision of a staff member.

General Guidelines for Staff

1. Employees of the School Board must follow and enforce this policy and regulation.
2. Users will use school computer resources in a responsible, ethical and legal manner. All division and school codes of conduct apply. Unethical or illegal activities include, but are not limited to: knowingly spreading viruses, violating copyright laws, using unauthorized software, impersonating another user, unauthorized entry, and/or destruction of computer systems and files.

General Guidelines for All Users

1. Users shall not use, create, distribute, import or otherwise deal with illegal, offensive, obscene, libelous language, pictures, or other similar material on any computer, network or the Internet.
2. Users shall not respond to harassment encountered on any technology system and shall report any such activity to the appropriate supervisor or administrator immediately.

Network and Workstation Guidelines for All Users

1. Users will access only files and data created and maintained by them, that are publicly available within the school network, or to which they have been given authorized access. This includes but is not limited to files residing on individual workstations, servers or other storage devices.
2. User files are not private. The School Division reserves the right to review the content of all computer accounts and files. Network administrators may review files and communications to keep the network working properly and to ensure that users are using the system responsibly.
3. Users will use the network without disrupting its use by others. Network users are expected to respect all forms of password protection and use responsible file management techniques (saving, deleting, naming, etc.).
4. Maintaining the security of School Division computers, networks and other technology

systems is of great importance and requires the cooperation and diligence of all users. Any user who identifies a security problem must notify the site administrator (principal or director) who must then notify the School Division Help Desk. The user shall not demonstrate the problem to others. Any user who attempts or causes a breach of the system security shall have his/her privileges revoked and may be subject to any additional disciplinary and/or legal action.

5. Users may not share passwords with others. Employee passwords, necessary for access to e-mail and systems that contain confidential information, must be changed at least quarterly to protect the security of the network. Periodic password changes may be enforced by the systems administrator. It is recommended that for personal security all users choose a password unique to their Albemarle County account(s).
6. Any user who desires to access School Division network resources or services on a personally owned computer or other device while on county property must obtain permission from the Office of Technology prior to accessing School Division network resources or services.

Internet Guidelines

Guidelines for Students

1. Students may access personal e-mail accounts and other forms of electronic communication with specific, written parental permission as provided on the Good Computer User Agreement, to the extent that access does not interfere with the educational process as determined by school staff. Student access to personal e-mail at school is intended for educational purposes and is not guaranteed to be private. No student may use Albemarle County Public Schools software or equipment to access any service for the purpose of conducting a purchase or participating in any other commercial activity.
2. Best practices for online safety require that students shall only use their first name and last initial unless participating in a moderated learning activity which requires full names. Home phone numbers, addresses, or other personal information shall not be revealed without parental and teacher permission.

Guidelines for Staff

1. Users may not share confidential information on students or employees with users who are not authorized to have such information. Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Employees should not use electronic mail for confidential matters or privileged communications, such as student education records, unless appropriate measures are taken to ensure confidentiality and to maintain the appropriate privilege. Employees shall adhere to all school, School Division, state and federal laws, policies and standards including the Family Education Rights and Privacy Act (FERPA).
2. Account access to systems containing confidential data will only be granted to individuals who meet the conditions of School Board Policy JO – Student Records, School Board

Policy GBL - Personal Records and other School Board policies, local, state and federal laws as applicable to the particular system. The use of such accounts must comply with all applicable laws and policies.

Guidelines for All Users

1. Users may not participate in any form of on-line mass e-mails, "chain letters" or thelike.
2. Users will follow general rules of communication etiquette.
3. Users may not create, open or forward any e-mail attachments that are known or suspected to contain viruses.

Consequences of Unacceptable Use

The use of computer resources is a privilege, not a right. Misuse of Internet access or a violation of this regulation may result in the account or the user's access privilege being denied, revoked, or suspended. Misuse may also subject the user to disciplinary action up to and including suspension, expulsion, formal reprimand, or dismissal as well as potential civil or criminal liability and prosecution. Any illegal activities will be reported to the appropriate agencies.

Internet Web Site Management Rules and Guidelines

All use of Albemarle County Schools Web server and resources shall promote educational excellence by facilitating resource sharing, innovation and communication for the enhancement of the School Division's mission.

Items published on the Albemarle County Schools Internet server shall be in accordance with applicable web site management rules and guidelines. The Web Page Coordinator within each school or department shall be responsible for ensuring that all pages published within the school or department's directory comply with this policy and applicable rules and guidelines. Each principal or director will assign the Web Page Coordinator duties to a staff member or staff members as appropriate. The Web Page Coordinator activities are managed by the Division Web Analyst.

Schools and departments must develop and use templates that meet the requirements for Division web pages and use navigational strategies common to those used by effective web sites. The templates should provide a common, professional "look and feel" to the Division's web site and sub-sites as appropriate. For example, the Division template would apply to all pages linked from the site home page. As another "site" begins, so may another template. These templates must be approved by the Division Web Analyst.

All School or Department home pages must include the following basic, current information:

- Name of school or department
- Name of principal or director
- Address
- Phone number
- Fax number

- Link to staff directory page containing names, current assignments, and school e-mail addresses for all professional staff (staff may substitute personal e-mail address if desired)
- Link to Division's home page
- Link to Division's Internet Privacy Statement
- Name and e-mail address of Web Page Coordinator (in case there are errors)

All web pages posted to the Division's web site must:

- contain only content appropriate and relevant to the business of the school division
- provide no more than limited personal information on "About the Teacher" pages, similar to introductory remarks that would be appropriate comments at a "Back to School Night" or similar function
- promote educational excellence by facilitating resource sharing and/or innovation
- comply with school and division "Web Site Management Rules and Guidelines"
- be technically sound and work properly
- protect the rights and privacy of students and staff. School and department web sites should include a faculty/staff directory with individual names, e-mail addresses and current assignments listed. In addition, the following statement should appear on school directory pages:

Notice: E-mail communication is not guaranteed to be immediate. If you have a message that requires immediate attention or must be communicated to your child in a timely manner, please phone the school office.

- adhere to all applicable Albemarle County guidelines and School Board policies. The web site may not be used to transmit or otherwise deal with illegal, offensive, obscene, libelous language, pictures, or other similar material, any material protected by federal or state intellectual property laws; copyrighted or licensed material, for which permissions have not been obtained; private, commercial links or materials; threatening or harassing language or material; and/or pornographic material.
- include name and e-mail address of web page owner (in case there are errors)
- include link to parent page
- include link to school's or department's home page
- include date of last update
- include appropriate title header that associates the page with the school or department

Web Page Coordinators should refer to the Yale Web Style Guide, currently located at <http://info.med.yale.edu/caim/manual/contents.html> for information regarding web page design and style or contact the Division Web Analyst for guidance.

Pages should be grammatically correct without spelling errors.

The author of the web page should review all pages for typographical errors, grammatical errors, content errors and similar problems before posting them to the web server.

Graphics should be used with a thoughtful purpose.

Graphics should provide useful, visual clues about the information provided and not distract from the purpose of the web page. Consideration should be given for the many different browsers that will be displaying the page. It is recommended that web page designs accommodate the common screen resolution of 800 X 600 pixels.

Information should be as current and accurate as possible.

In addition, all links to Internet resources should be checked regularly as appropriate and revised as necessary by the author of the web page. Any page that includes external links must include the following warning, informing the user that they are leaving www.k12albemarle.org.

<p><u>WARNING!</u> This page contains hyperlinks to one or more external web sites. Accuracy and quality of information obtained from either internal or external sources cannot be guaranteed.</p>
--

Each page must include the date of last revision. Each page should include an appropriate title. Standard web site management and page creation tools must be utilized. Additional technical standards may be obtained from the Office of Technology.

Guidelines for Monitoring Student or Staff use of Technology

Albemarle County Public Schools does not routinely monitor an individual's usage of the Division's technology resources. However, as stated in the Acceptable Use Policy (School Board policy IIBE), there is no guarantee of privacy granted to the user of these resources. The normal operation and maintenance of the Division's technical infrastructure and services requires that general usage and activity is monitored, data and electronic communications are routinely backed up, and programs or other devices are employed to maintain the functionality, integrity, or security of the network infrastructure.

Albemarle County Public Schools reserves the right to monitor any activity, communication, or file creation or storage that utilizes Division resources. An individual user's account or activity may be monitored, without notice, under specific conditions, including but not limited to the following:

- 1) The user has posted the material to the Division's web server.
- 2) Routine monitoring reveals excessive traffic (file downloads/uploads, e-mail generation, etc.) or violations of the Acceptable Use Policy (School Board policy IIBE) associated with a particular account.
- 3) It is determined that the activity associated with a particular account threatens the functionality or security of the Division's technical infrastructure.
- 4) There is a legal requirement to do so.
- 5) An employee's supervisor, or a student's principal or designee requests such monitoring to ensure compliance with the Acceptable Use Policy (School Board policy IIBE). All requests must be approved by the Executive Director of Administrative Services.

Monitoring of any individual user's account must conform to written procedures established by the Assistant Director, Office of Technology.

**Grades K-2 Student Regulations
Albemarle County School Board Policy IIBE**

A Good Computer User:

1. Uses the computer with good intentions. Does not use a computer to hurt people or their work.
2. Respects the computer as our school's property. Does not break or hurt the computer.
3. Practices good computer citizenship. Does not look at, send, or print bad or mean messages or pictures.
4. Respects the environment. Does not waste paper by printing too much.
5. Respects the rights of others. Does not go into another person's folders, work, or files without permission.
6. Acts responsibly. Immediately tells an adult if his/her computer shows bad or inappropriate things.
7. Accepts responsibility. If you do something wrong, expect to be disciplined.

I agree to be a good computer user!

_____	_____
Student Name	School
_____	_____
Student Signature	Date

I expect my student to be a good computer user as defined by this document and the Albemarle County School Board Policy IIBE, *Acceptable Use of Technology*.

_____	_____
Parent's/Legal Guardian's Signature	Date

For a full copy of the Albemarle County School Board Policy IIBE, *Acceptable Use of Technology* and accompanying regulations, please contact your child's principal.

**Grades 3-5 Student Regulations
Albemarle County School Board Policy IIBE**

A Good Computer User:

1. Uses the computer with good intentions. Does not use a computer to hurt people or their work.
2. Respects the computer as our school's property. Does not damage the computer or other school community property.
3. Respects the law. Does not download and/or install software, shareware, or freeware unless approved by a teacher and does not violate copyright laws.
4. Practices good computer citizenship. Does not look at, send, or print inappropriate messages or pictures.
5. Respects the environment. Does not waste paper by printing too much.
6. Respects privacy rights. Does not share or use passwords that are not his/her own without a teacher's permission.
7. Respects the rights of others. Does not go into another person's folders, work, or files without permission.
8. Acts responsibly. Tells an adult if his/her computer displays inappropriate material.
9. Accepts responsibility for proper computer use. Misuse of the computer can result in loss of computer privileges and other punishments.

I agree to be a good computer user!

Student Name

School

Student Signature

Date

I expect my student to be a good computer user as defined by this document and the Albemarle County School Board Policy IIBE, *Acceptable Use of Technology*.

Parent's/Legal Guardian's Signature

Date

For a full copy of the Albemarle County School Board Policy IIBE, *Acceptable Use of Technology* and accompanying regulations, please contact your child's principal.

Secondary Student Regulations
Albemarle County School Board Policy IIBE

Secondary students are expected to:

1. Use the computer for educational purposes only.
2. Use the computer in a manner which does not harm
 - a. People
 - b. Physical equipment, hardware
 - c. Software, operating systems, folders, and files
3. Protect the privacy of self and others by
 - a. Keeping passwords secret
 - b. Respecting the privacy of other student's, teacher's, and the school system's files.
4. Access Internet sites that are appropriate and avoid sites that
 - a. Are offensive, obscene, libelous, or disruptive or contain inflammatory language or pictures
 - b. Require a fee for access (unless authorized by the school and teacher permission is granted).
5. Use computer resources responsibly by
 - a. Self-limiting use of disk space
 - b. Self-limiting use of printing paper
6. Download materials from the Internet, or copy materials from the network, only as approved by a teacher.
7. Protect the use of the computer for others by never
 - a. Knowingly loading or creating viruses
 - b. Violating copyright laws
 - c. Destroying or deleting other's files, folders or programs.
 - d. Deliberately causing harm to any computer, system, or network
8. Use e-mail responsibly by
 - a. Accessing personal e-mail, and other forms of electronic communication, during the school day for educational purposes only
 - b. Respecting the privacy of letters: letters will not be re-posted without a sender's permission
 - c. Ignoring and refusing to re-send "chain letters" and the like
 - d. Using appropriate language and subject matter
9. Protect, for personal safety reasons, your own privacy on the Internet by using first name and last initial unless the teacher-approved activity requires full names. Home telephone numbers, addresses, and other personal information may not be released unless written parental permission is granted.
10. Accept the consequences of improper use of computers that may include loss of computer privileges and other disciplinary actions.

**Acceptable Use of Technology Policy
Acknowledgment**

I have read the Albemarle County Public Schools' Secondary Student Regulations based on Albemarle County School Board Policy IIBE and state that I fully understand and agree to abide by its requirements in all respects. Should I violate any aspect of this Policy, I specifically agree that I shall accept and be subject to all ramifications, including but not limited to the loss of access and other privileges.

Student Name	Student Signature
School	Parent's/Legal Guardian's signature
Date	

If the above-named student does not have a personal e-mail account I give her/him permission to apply for a free Internet-based e-mail account from school if deemed necessary for educational purposes by school staff. Furthermore, I give the above-named student permission to access his/her personal e-mail account from school if deemed necessary for educational purposes by school staff.

Parent's/Legal Guardian's signature	Date
-------------------------------------	------

NOTE: Your signature on this acknowledgment is binding and establishes that you understand the terms and conditions of this policy and their significance.

For a full copy of the Albemarle County School Board Policy IIBE, *Acceptable Use of Technology* and accompanying regulations, please contact your child's principal.

**Albemarle County Public Schools
Web Publishing Permission Form**

Dear Parent/Guardian,

Each school in Albemarle County maintains school web pages that often highlight events or student accomplishments and work. Your child may be featured in some of these pictures, or may complete work our staff deems worthy of being posted on the Internet. In order to ensure the privacy and safety of all students, Albemarle County Schools requires parental consent before publishing student photographs and student work to these web sites. Albemarle County Schools will not associate names with student pictures on the web and will only associate first name with student work.

Please fill out the form below and return it to school as soon as possible.

I give permission for my child's photograph to be used on the school web pages.

Please check one: Yes No

(In order to ensure safety and privacy, Albemarle County Schools will not associate names with student pictures on the web*)

I give permission for my child's school work to be posted on the school's web pages.

Please check one: Yes No

(In order to ensure safety and still allow for proper credit and recognition, Albemarle County Schools will associate first name only with student work on the web*)

Student's Name: _____ School: _____

Teacher's Name: _____ Grade: _____

Parent's/Legal Guardian's Signature: _____ Date: _____

* In certain circumstances, when posting additional student information to the web may be appropriate (ex. sports, academic recognition, etc), special permission will be requested.

**Albemarle County Public Schools
Web Publishing Special Permission Form**

Dear Parent/Guardian, Visitor, or Staff:

To ensure the safety and privacy of all students, visitors, and staff, Albemarle County Schools does not associate names with student or other photographs on our website. First name only may be associated with student work. In some cases, it may be appropriate to step outside these guidelines to provide proper recognition in a certain area. The form below describes the special circumstance and asks for permission to publish specific student information to a school web page. This form should also be used for granting permission to publish staff or visitor photographs or other information to the school's web page.

Special Circumstance (please describe):

Student, Visitor, or Staff Information to be Published:

I give permission for this information to be published on the school's web page for this special circumstance:

Please check one: Yes No

Student's Name _____ School _____

Teacher's Name _____ Grade _____

Parent's/Legal Guardian's Signature _____ Date _____

If adult visitor or staff permission granted, please sign below:

Name _____ Signature _____ Date _____