PROTECTING CHILDREN IN CYBERSPACE: A HIGHER EDUCATION CASE STUDY

by

James Earl Lantzy
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Arts
Community College Education

Committee:

Victoria N Salmon ________ Director

____

____

John Oconnor ________ Program Director

________ Dean, College of Humanities and Social Sciences

Date: December 2, 2008 ________ Fall Semester 2008
George Mason University
Fairfax, VA

Protecting Children in Cyberspace: A Higher Education Case Study

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Arts at George Mason University

By

James Earl Lantzy
Master of Arts
Industrial Relations
Saint Francis University, 1990

Director: Dr. Victoria N. Salmon
Higher Education Program

Fall Semester 2008
George Mason University
Fairfax, VA

DEDICATION

I dedicate this dissertation first and foremost to my wife Lisa. Your understanding, resolve, and commitment have provided me with the strength to put this vision in motion. You inspire me to improve as a person every day and I am thankful that we are making this life journey together—you are my best friend and I love ya, buddy! To my daughters Abby, Katie, Jaimee, and Claire who are the love of my life and daily reminders that miracles can happen and love conquers all: I am where I am today because of your encouragement and belief in me. You girls are not only my inspiration but the reason I chose to reach out and accomplish a grassroots effort uniting K-12 and higher education in an effort to affect change via protecting children in cyberspace. You are all my best friends and I love you so much—I did this for you.

To my parents who have been so supportive throughout my entire life. My Dad taught me so much about common sense and always doing the right thing; you definitely have served as my moral compass in life. To my Mom, who is my role model for how to always treat everyone with kindness and compassion—when I grow up, I want to be just like you, Mom! To my sister Anne, thanks for being a good listener and always filling me with the belief that I could accomplish this almost insurmountable task.

My family: You have educated me your whole life. Thank you for teaching me the importance of being a good person, pursuing your dreams, believing in oneself, and most importantly—embracing the love of family and the blessings that come free with each day.

ACKNOWLEDGEMENTS

I would like to thank Dr. Victoria Salmon. Without you I would not be completing this dissertation. Your support throughout the entire program has been tremendous. Your leadership and guidance for me through these sometimes challenging 10 years and dissertation process is remarkable. Thanks for stepping in as my chairperson when I needed one. I appreciate your patience, leadership, encouragement and friendship. I consider myself very fortunate to have had the privilege of working with you on this project.

Thanks to Dr. Muir and Dr. McCarron for your drive, guidance, and resolve in making not only this product and exercise worthwhile, but also helping me to develop myself to be a more serious student of education; I am ever grateful.

Special thanks to James Madison University, Ms. Cheryl Elliott, Ms. Tammy McGraw and the Virginia Department of Education, Office of Educational Technology, and the entire K-12 community of Rockingham County and Harrisonburg City school districts whose cooperation made this study possible. You have shown your class, style and commitment to education at all levels by giving of your time and sharing your experiences with me. Thanks to the search consultants, retired superintendents, and the six superintendents who gave me your time for interviews. It is a privilege to have worked this project with you.

Special thanks to Colleen Spears for her dedication, patience and time keeping me on the straight and narrow path to completion! I couldn’t have done this without your help and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

PROTECTING CHILDREN IN CYBERSPACE: A HIGHER EDUCATION CASE STUDY

James E. Lantzy, D.A.

George Mason University, 2008

Dissertation Director: Dr. Victoria N. Salmon

The Internet provides students with a multitude of resources for learning, communicating, and entertainment. Children should develop skills to identify not only good information but biases, misinformation, and safety and security threats. All children should understand how to protect themselves online, their personal information when engaging with others online, and the potential consequences of their actions in online information sharing through social networking sites, e-mail, gaming, and instant messaging to name a few. To this end, the Virginia Department of Education, Office of Educational Technology produced *Guidelines and Resources for Internet Safety in Schools* (October 10, 2006) which requires all K-12 schools to integrate an Internet safety component into each school division's instructional program.

This case study reviewed the collaboration efforts of one higher education institution's effectiveness in assisting the middle school education community in Rockingham County and Harrisonburg City schools through a community partnership with the Virginia Department of Education's Office of Educational Technology, James Madison University (JMU), and the Harrisonburg City and Rockingham County school districts. This collaboration centered on whether higher education (with JMU serving as a subject matter expert in information security education), and its K-12 resource *Cyber Citizenship for Kids Guide,* could lead a grassroots community-centered campaign for Internet safety and provide a solution which met the requirements of these *Guidelines and Resources for Internet Safety in Schools* as outlined by the Commonwealth for their K-12 community.

To achieve this end, middle school teachers, school administrators, instructional technology resource teachers (ITRT), counselors, resource officers, school media specialists, JMU staff, and Virginia Department of Education's Office of Educational Technology staff participated in a combination of surveys, interview questionnaires, and telephone and personal interviews.

This research determined that this community partnership on cyber safety education between higher education and K-12 institutions in Rockingham County and Harrisonburg was perceived by stakeholders as feasible and effective. Several aspects of this county-wide community partnership effort to enhance K-12 cyber safety awareness can serve as a credible statewide model in providing Internet safety education to K-12 throughout the Commonwealth.

I. INTRODUCTION

The opportunities to expand educational experiences, develop creativity, and foster communication in a global context are among computer technology's exciting potential applications; however, these benefits are accompanied by challenges. Most significant among the difficulties are the online risks to children's safety and emotional wellbeing. Children typically are naive regarding dangers in cyberspace, and parents/guardians often lack familiarity with mechanisms to address these concerns (Berson, Berson, & Ferron, 2002). Consequently, educators have an important role to play in addressing the lapse in students' at-home preventative intervention to create and maintain awareness and safety for young people online.

Children's safety and wellbeing are of paramount importance to educators; however, in practice few professionals are prepared for their role as children's cyber protectors and advocates. Teachers' careful guidance may assist students in making informed decisions and allow them to demonstrate an ability to apply online critical thinking skills and productive social participation. Although many young people have some awareness of cyber safety as a result of initial discussions with adults, there appears to be a paucity of ongoing communication, leaving adults generally unaware of the online behaviors of children in their care. This is described by Young (1998) as a benign neglect of children's Internet activity. Adults' distance from youth as a result of a communication gap and technological divide highlights the shared responsibility of educators and parents/guardians in making sure that children have access to, and are safely guided through, the Internet. Educators' roles in promoting awareness of potential harm online and the importance of safe and ethical conduct online are an essential preventative mechanism to counter cyber misconduct. The lack of instruction on these soft-skills in the curriculum has many experts worried about the propagating culture of young Internet users (Lewandowski, 2002).

An adequate number of studies on the safety of children while using the Internet have been published (Adelman, 2004; Berrier, 2007; Berson, 2000; Berson, Berson, & Ralston, 1999; Cho & Cheon, 2005; Finkelhor et al., 2000; Wolak et al., 2002, 2003), and an extensive list of organizations providing Internet safety awareness solutions to the K-12 community. In contrast, there appears to be little to no scholarly research depicting appropriate K-12 teaching practices for cyber security. However, the National Cyber Security Alliance (NCSA), which serves as the overarching collaborator for these organizations in promoting Internet safety awareness to the K-12 community, issued a new study conducted online, the *2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study*, which reveals that "K-12 teachers and students are not prepared to Protect Against Cyber-Crime" (Educational Technology, Policy Research, and Outreach - National Cyber Security Alliance (ETPRO-NCSA), 2008a). This ETPRO-NCSA study was to baseline and explore educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S. public and private K-12 educational settings;

1,569 public and private U.S. K-12 educators and 94 technology coordinators took the survey, while 219 educators local and state technology coordinators, and state technology directors participated in focus groups for the survey (ETPRO-NCSA, 2008b). Some key findings of this ETPRO-NCSA *2008 National Cyberethics* baseline study include the following regarding teacher preparedness:

- “More than 60%” of study participants “don’t feel comfortable discussing how to detect and minimize computer viruses” (2008b).
- “75% don’t feel comfortable discussing cyber-bullying and less than 32% are comfortable giving guidance on how to be safe in an online environment, including social networking and cyber predators” (2008b).
- “Only 23% percent feel prepared to teach students how to protect their personal information online” (2008b).

Ron Teixeira, Executive Director of the NCSA, stated in an interview to *Education Week’s Digital Directions*, “We haven’t done a good job of teaching kids that there are consequences for what they do on the Internet” (McCann, 2008). Students are now becoming creators of web content themselves through collaborative sites like MySpace and Facebook. While much of their online time may occur outside the school environment, K-12 still has a responsibility to address the underlying values (cyber ethics) and responsible behaviors expected of students.

As society’s needs change, so too must our educational system adopt new efforts to meet its mission’s needs both nationally and locally. Adopting new partnerships in local communities surrounding higher education, which can then enable K-12 to broaden its resource base in educational offerings, and access varied rich sources of technology-related education requirements, proved itself a critical strategy through this research.

In this case study, James Madison University's (JMU) Institute for Infrastructure and Information Assurance, led by Ms. Cheryl Elliott, Marketing Director, developed an informal and community-based partnership with the Virginia Department of Education, Rockingham County, and Harrisonburg City public middle schools in an effort to model an effective strategy to help these Virginia communities address a new Virginia K-12 educational requirement to teach Internet safety in all Virginia K-12 public schools. Collectively, this trinity incorporates the technical expertise of higher education (JMU), educational standards and governance of the Virginia Department of Education (VA DOE), and the classroom connections and communication element of Rockingham County and Harrisonburg City Middle School officials.

This informal outreach model's potential for effectiveness lies within its student/customer-centered approach. JMU views the middle school students as the middle school teachers' customers; middle schools teachers are the VA DOE's customers; the VA DOE is JMU's customer. The Internet safety education model for middle school students used in the case study was the *Cyber Citizenship for Kids Guide* (Institute for Infrastructure and Information Assurance at James Madison University [IIIA], 2007). This *Kids' Guide* is organized around the ways a middle school student uses the Internet, with sections on e-mail, surfing, chat rooms, cell phones, and gaming (see Appendix A – Definitions). Thus, the *Cyber Citizenship for Kids Guide* includes general safety tips on:

- instant communication (instant messaging (IM), chat rooms, text messaging, cell phones),
- surfing the Web safely,
- e-mail,
- gaming, and
- protecting your identity.

Case Study Participants

The key participants in this case study included representation from both levels of education in the Rockingham County community: Higher education is represented via JMU, K-12 is represented in the middle school communities of Harrisonburg City schools and Rockingham County schools.

Rockingham County

The population in Rockingham County is approximately 68,000 with the county seat for government located in Harrisonburg, Virginia. As of the census of 2000, there were 67,725 people, 25,355 households, and 18,889 families residing in the county (as cited in Wikipedia, n.d.). In contrast, as an independent city, Harrisonburg is not a part of Rockingham County, despite its status as the county seat. Therefore, Harrisonburg City schools has its own educational body which is peer to Rockingham County schools. According to the Virginia Department of Education's *2003-2009 Educational Technology Plan for Virginia* (2006a), for the 2007-2008 school year Rockingham County had a student population of roughly 11,850 students within 20 schools in 3 school districts: Broadway, Spotswood, and Turner Ashby. Harrisonburg City schools had a total enrollment of nearly 4,500 students throughout 6 schools in the city.

James Madison University (JMU)

JMU is a public coeducational research university located in Harrisonburg, Virginia. JMU was founded in 1908 as the State Normal and Industrial School for Women at Harrisonburg. The university underwent four name changes until settling with James Madison University. It became the State Teachers College at Harrisonburg in 1924 and continued under that name until 1938, when it was named Madison College in honor of the fourth president of the United States (Wikipedia, n.d.). The school is nationally recognized for its academics. *U.S. News & World Report* has ranked JMU as the top public (4th overall), masters-level university in the South for 14 consecutive years (as cited in JMU Office of Media Relations, n.d.). And according to *BusinessWeek* magazine in its 2008 ranking of undergraduate colleges of business, JMU's undergraduate business school is ranked 54th in the nation, and 4th in Virginia (as cited in JMU Office of Media Relations, n.d.). Currently, James Madison University offers more than 100 degree programs on the bachelor's, master's, educational specialist, and doctoral levels. JMU was selected for this study as the higher education representative because of their strong credentials in having subject matter expertise in information security. The university is comprised of seven colleges and 78 academic programs. According to IIIA (2007), JMU was

> named as one of the original Centers of Academic Excellence for Information Security Education by the National Security Agency and is recognized throughout

academia, industry and the government, as a subject matter expert on homeland security and cyber security related issues.

Statement of the Problem

Based on discussions with EDUCAUSE’s Rodney Peterson (personal communication, June 15, 2006), National Internet Safety Alliance Executive Director Ron Teixeira (personal communication, June 15, 2006), and the National School Boards Association Manager of Education Technology Programs Colleen O’Brien (personal communication, June 15, 2006), there appears to be a lack of a hands-on community-focused effort between the K-12 educational environment and higher education to address Internet safety, cyber safety, and cyber ethics issues for today’s K-12 students. All three leaders explained that the current methodology being employed nationally through their programs is a top-down approach which leaves the K-12 administrators and educators carrying the burden of applying the program solutions, and no alternative means for providing the message to students. These national cyber awareness programs do provide valuable resources to the K-12 community; however, no one program provides a facilitating mechanism to integrate any of these best Internet safety practices into existing Virginia Standards of Learning, nor advises educators on how best to integrate the practices into their existing K-12 curricula.

By opening dialogue between higher education and the K-12 environment, K-12 teachers may be better able to prepare students to understand appropriate technology use, and explore and educate students about issues that will continue to unfold. Unfortunately, many educators are not equipped with the tools or understanding to integrate Internet safety best practices into their classroom lessons (ETPRO-NCSA, 2008a, 2008b. Consequently, in order to maximize the benefits of online access, educators have an important role in empowering students with cyber literacy skills and extending training to families as well. As a result, the initial focus of creating a framework for Internet safety, according to the Virginia DOE's *Guidelines and Resources for Internet Safety in Schools* (2006), is to emphasize the role of the schools, parents or guardians, and administrators. Instruction on Internet safety and responsibility is needed to accompany schools' rapid saturation by technology and Internet access (VA DOE, 2006). Educators are in an important position to identify appropriate Internet safety resources to assist them with sharing what are appropriate online behaviors for safe and rewarding Internet use for children. Higher education, with its technological expertise and experience, can serve as a catalyst; therefore, as the subject of this study. Helping to address community needs, provide expertise, and help leverage best practices throughout industry and the government is not a new phenomenon for higher education. Higher education, in many ways, can serve as a catalyst not only in communities but throughout the world. For example, Australia's National Centre for Vocational Education Research (Karmel & Maclean, 2007) recently provided technical and vocational education to what they called an "aging society." For this case study, JMU provided Internet safety learning awareness and education tools to the Virginia middle school students and their community through its partnership with VA DOE, Rockingham County and Harrisonburg City schools, and its *Cyber Citizenship for Kids Guide*.

In middle school settings in particular, the need to educate about behaviors in cyberspace and minimize potential and actual risks to children has brought on national programs and campaigns sponsored by the National Cyber Security Alliance through programs like iSafe, NetKids, and CyberSmart, which provide educators across-the-board programs and resources. As mentioned above, although educators play an integral role in this process, they tend to lack confidence in their own technology skills and their ability to provide appropriate prevention information to children and their families. Consequently, as society struggles to address the serious social problems associated with Internet use, educators often find themselves inadequately prepared to assist children in the classroom. Since teachers are key individuals in helping students develop essential capabilities as responsible technology users, providing these educators with comfortable instructional guidelines to meet the Virginia Educational Standards is critical to fostering students' positive social and ethical behaviors in a digital society. Technology education standards such as the National Educational Technology Standards for Teachers (NETS) developed by the International Society for Technology in Education (ISTE) (ISTE, 2002a; see also http://www.iste.org), establish expectations for teachers to prepare technology-capable youth. This preparation requires a commitment to ensure that students stay safe from harm, understand their responsibilities as citizens, and use their time online productively and effectively.

Purpose

This study supported the research and development of JMU's *Cyber Citizenship for Kids Guide* (IIIA, 2007), for which the researcher authored and developed text. When the *Cyber Citizenship for Kids Guide* was released July 11, 2007, it was expected to serve as a model for the Fall 2007 school year release of the new VA DOE *Guidelines and Resources for Internet Safety in Schools* (2006b) in print and electronically via the VA DOE, Office of Educational Technology website. In addition, with collaboration from Harrisonburg City schools, JMU focused this *Kids Guide* into a web-based electronic version to provide the middle school community with a more readily integrated resource. This case study explored this informal and triangulated cooperative approach to Internet safety awareness and education for middle school children between higher education in Rockingham County (JMU), the Virginia Department of Education (VA DOE), and Rockingham and Harrisonburg City middle school officials. A qualitative case study and analysis to determine whether this strategic alliance and community partnership was perceived as effective in responding to Virginia's K-12 2007 Internet safety awareness and education needs at the middle school level.

Research Questions

The study's goal was to evaluate one higher education institution's (JMU's) effectiveness in assisting the middle school education community through its community partnership with the VA DOE, Rockingham County, and Harrisonburg City middle school educators in meeting Virginia's Internet safety awareness and education requirements for middle school children in 2007. Meeting these requirements was achieved through JMU's development and delivery of its *Cyber Citizenship for Kids Guide* (IIIA, 2007) in both hard copy and electronic version. These tools were to serve as an Internet safety handbook for Virginia middle school children. Once this *Kids Guide* was distributed in the Fall of 2007, this research pursued the following questions to achieve this study's goal:

- Was JMU's grassroots approach, as a subject matter expert in information security education, and through its community-based partnership with VA DOE and middle school teachers in Virginia, *perceived as being effective* in helping Virginia educators meet the requirements set forth by the VA DOE's *Guidelines and Resources for Internet Safety in Schools* (2006) with its *Cyber Citizenship for Kids Guide* (IIIA, 2007) for Internet safety awareness and best practices?
- Was this community partnership on cyber safety between higher education and K-12 institutions perceived by the educational stakeholders as feasible and effective?
- Finally, what aspects of this county-wide community partnership effort to enhance K-12 cyber safety awareness can serve as a credible delivery model for Virginia statewide and federal efforts in this area?

Limitations and Delimitations

Some limitations and delimitations existed. The first limitation was the unknown level of participation by Rockingham County and Harrisonburg City middle schools in using the *Kids Guide*. Another limitation was the level of interest by the VA DOE in doing follow-up surveys of the effectiveness of the JMU Internet safety and awareness instrument in its *Kids Guide,* and the overall effectiveness of the community-based partnership between VA DOE and higher education. It was possible that these school districts and/or VA DOE may choose not to participate. Another limitation was the timely publishing process for this *Kids Guide* by James Madison University, which was expected to occur in July 14, 2007. However, JMU did not publish its draft copy until November 1, 2007. This occurred in conjunction with this study's the follow-up survey. What was realized was that the participants were interested in an electronic version of the *Kids Guide* in addition to the hard copy to better afford the middle schools a more viable channel for integration into their curriculum.

This study's major delimitation was that it focused on middle schools in Virginia. It does account for grades 6 - 8, but does not take into account the high school and elementary education environments. Recent literature suggests that students initially start using the Internet as a tool in education starting around the third grade (National Cyber Security Alliance, 2007a; EDUCAUSE, 2005). Also, the study is centered on Virginia education requirements and Virginia Standards of Learning to meet the requirements set forth in the VA DOE's 2006 *Guidelines and Resources for Internet Safety in Schools* agenda; therefore, the study does not take into account other states or countries. Finally, this study does not address all Virginia middle schools, only a representative sample in Rockingham County and Harrisonburg City—the areas surrounding JMU—in order to narrow the scope and shorten the timeline.

Background on Cyber Safety for Children

Education has historically enjoyed a culture of open access to information. The free flow of information in today's technologically rich environment—with cell phones surfing the net and receiving and sending e-mail, personal digital assistants (PDAs) and iPods/MP3 players turned into portable hard drives for storing potentially sensitive or proprietary information, as well as viewing podcasts for the day’s lesson—represents how computers and technology intertwine in the education landscape.

To balance the increase and demand for technology in schools and provide a framework for children’s safety in learning, many national programs sponsored through not-for-profit organizations focus on the appropriate technology use—i.e., the elements of Internet safety. National programs such as StaySafeOnline.org, iKeepSafe.org, and CyberSmart.org, with support of grants from the National Science Foundation and visibility from EDUCAUSE and Congress, help play a vital role in the overall cyber awareness and education of K-12 students. Through public service announcements and other media sources, they try to reach the needs of the K-12 environment, its students and educators.

Many middle schools have constructed standards or acceptable use policies concerning how to use technology appropriately inside the schools, but how students behave as members of a cyber society has become a critical issue for technology leaders, educators, and district administrators, as well as higher education.

Internet safety, as defined by Kansas State University’s (KSU) *Study on Digital Citizenship for Education* (Ribble, Bailey, & Ross, 2004), encompasses the norms of behavior regarding computer technology use. This research study’s *Cyber Citizenship for Kids Guide* is meant to be an “Internet safety awareness model” for middle school students to include cyber ethics, cyber safety, and Internet safety awareness materials (C. Elliott, JMU, personal communication, March 15, 2007).

Why are K-12 schools not fully utilizing national cyber awareness programs? This study demonstrates that creating a statewide Virginia middle school student resource such as the *Kids Guide* can successfully address a national-level concern at the community level for the Commonwealth of Virginia. This JMU *Cyber Citizenship for Kids Guide* is intended to serve as an educational model for Internet safety for middle school students by the Virginia Department of Education, and meet the requirements of the Virginia 2006 *Guidelines and Resources for Internet Safety in Schools* set forth for all Virginia K-12 schools. Although this personalized, statewide higher education effort and gathering of community resources is not effectively occurring relating to Internet safety with the national programs at present, this research demonstrates that this community partnership model between higher education, the K-12 education community in Rockingham County and Harrisonburg City, and the VA Department of Education can prove successful for addressing an immediate local and statewide need to educate middle school students regarding Internet safety.

According to IIIA (2007), "The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) was founded in August 2002 as an interdisciplinary research center focusing on homeland and national security issues." In addition, IIIA (2007) states,

> Named as one of the original seven Centers of Academic Excellence for Information Security Education by the National Security Agency, JMU has established online educational programs through a Master's of Computer Science

in Information Security and Master's of Business Administration with a concentration in Information Security.

JMU's Institute for Infrastructure and Information Assurance (IIIA) outreach program produced the *Cyber Citizenship for Kids Guide* (2007). This outreach effort symbolizes a major contribution wherein higher education played a critical role in supporting the efforts of middle school elements within their region—an important step to bridging the gap and sharing expert knowledge between postsecondary education and lower education levels.

JMU adopted this collaborative approach to specifically address Virginia-wide Internet safety education requirements mandated for all Virginia K-12 public schools. JMU sought to develop a Rockingham County community of teachers, technologists, learners, and community leaders who combine talents to advance rapidly changing technologies for education purposes (C. Elliott, JMU, personal communication, March 15, 2007). IIIA and JMU have provided similar community-based collaborative guides in the past, including *A Rural Citizens Guide for Emergency Preparedness* (May 2005) and *A Guide for the Hispanic Community* (June 2006).

IIIA and JMU produced the *Kids Guide* in collaboration with JMU's Colleges of Education and Integrated Science and Technology; Congressman Good Latte's (R) office where the Congressman serves as Chairman of the House Republican High Technology Working Group, and Co-Chair of the Congressional Internet Caucus; Senator Mark Obenshain (R) who was elected to the Virginia State Senate for the 26th District; the

Virginia Attorney General’s office; Virginia Department of Education’s Office of Educational Technology; and the Rockingham County and Harrisonburg City schools.

As noted above, this study explored and evaluated the effectiveness of the informal community-based partnership representing all elements of education: JMU, Virginia’s K-12 school community, the Office of Educational Technology at the Virginia Department of Education, and community resources, to assist middle school teachers in imparting Internet safety awareness and education to middle school children in Rockingham and Harrisonburg City middle schools. This study researched, analyzed, and validated the effectiveness of this triangulated union—and determined this collaborative community partnership afforded higher education the access it needed to produce a solution for the Virginia K-12 community regarding middle school students’ awareness and understanding of Internet safety.

JMU’s resulting *Cyber Citizenship for Kids Guide* is meant to provide Virginia middle school students with Internet safety best practices and awareness education which meets the Virginia Department of Education *Guidelines and Resources for Internet Safety in Schools* (2006b) and the *Commonwealth of Virginia Computer Technology Standards of Learning for Virginia’s Public Schools* (VA Board of Education, 2005) for grades 6 - 8.

With the U.S. Department of Education count of almost 54 million children (K-12) in our nation’s public and private schools (EDUCAUSE, 2005), today’s students will be the first generation to use the Internet for their entire lives. This unprecedented access to resources can allow them to enhance their learning, research, communications, explorations for new ideas, and expressions of creativity. Unfortunately, this remarkable resource has become susceptible to abuse that often targets young people.

The *National Strategy to Secure Cyberspace* (President's Critical Infrastructure Protection Board, 2002) calls on individuals and industries to improve national security by securing the part of cyberspace they can influence or control. Cyber awareness for children is generally weak or missing in implementations of this national agenda. There are ongoing efforts to structure a similar type vehicle through the National Internet Safety Alliance's *Cyber Security, Safety, and Ethics* Roundtable Series (2006). Its supporting partners, including the Internet Safety Industry Alliance (CSIA) and Department of Homeland Security (DHS), are focusing on developing a "National Internet Safety, Safety and Ethics Awareness Campaign" to decrease and eventually eradicate cyber crimes against children and teenagers and increase national awareness about proper Internet safety, safety and ethical uses of computer technology and the Internet in today's environment (R. Trexteria, NCSA Director, personal communication, April 16, 2006). The results of this dissertation will be presented to the Director of the National Cyber Security Alliance (NCSA) as one possible solution for meeting the local K-12 community needs for Internet safety, applying a higher education community-infused approach which leverages local/community expertise and resources to address a national problem in Internet safety for today's youth.

At a Congressional Hearing on "Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen" (April 21, 2004), EDUCAUSE highlighted the need for higher education institutions to advance and promote Internet safety leadership and outreach activities among the higher education and civil communities (Peterson, 2004). EDUCAUSE states that “colleges and universities have long been interested in supporting the efforts of elementary and secondary schools to improve the awareness of students on issues like cyber ethics and security” (as cited in Peterson, 2004).

Information security is a growing concern for K-12 schools, since most schools now use information technology to organize and access data as well as to facilitate learning. Information security incidents are pervasive; according to the Computer Security Institute/Federal Bureau of Investigation’s *2002 CSI/FBI Computer Crime and Security Survey*, 56% of the respondents detected security incidents within one year’s time (Computer Security Institute, 2002). Information security incidents adversely affect society on four levels, according to the Computer Security Institute (2002):

- Individual: “Security incidents adversely affect individuals, who lose valuable, sensitive information and services.”
- Organizational: “Security incidents affect organizations, who spend valuable resources preventing, detecting, and responding to incidents, and which suffer lost revenue and opportunity.”
- National: “Information security incidents also have the potential to affect the nation’s security, whose critical infrastructure depends on telecommunications and the Internet for core business and functional services.”
- Global: “Security incidents affect the Internet for core business and functional services worldwide.”

Therefore, “the security of cyberspace rests on the security of all its components” (President’s Critical Infrastructure Protection Board, 2002). Unfortunately, K-12 students, educators, and support staff are largely information security illiterate; that is, they are unaware of the threats, vulnerabilities, and issues associated with the information systems they use.

Electronic and wireless devices like iPods, cell phones, and handheld devices with remotely controlled technology (e.g. Bluetooth) are being integrated into all facets of society—which includes all levels of education—at an alarming rate. While these tools present a wealth of opportunities never before seen in the educational community, they are also becoming a source of abuse and misuse by students. As educators, parents, and concerned citizens, we should be proactive and effectively engage our children and students in a consistent manner regarding using these tools in our schools. While there are many underlying causes, one of the reasons for technology misbehavior can be attributed to lack of education or training and/or lack of cyber ethics awareness in schools.

Technology leaders throughout the United States have attempted to minimize technological abuse and misuse by creating rules, regulations, and policies called Acceptable Use Policies (AUPs). While the presence of AUPs appears to minimize in-school misbehavior, this research proposes that they have had limited impact on technology misuse and abuse outside the school. Students—as well as educators and administrators—appear to have a very limited understanding of the issues related to appropriate and inappropriate technology use. A mounting concern in growing proportion is the increasing body of knowledge related to technological misuse and abuse of children by adults (see StaySafeOnline.org).

Children use PCs to learn traditional subjects, do homework and study, and for entertainment. Few could argue that the high-speed Internet has not had a profound influence on education, including an unprecedented access to resources, opportunities for collaboration across geographic and temporal barriers, and engagement in global communities. As pervasive as the Internet and technology have become, it is vital that America's children learn the ramifications that are possible through electronic commerce and transmissions. E-mail, instant messaging, and text messaging connect them with friends, parents, and other family, but they are also susceptible to stalking and predatory behavior. The Internet provides means for obtaining music, sharing digital photographs, playing games, and blogging about personal life, yet this research sees fewer boundaries or legal borders being placed on them at home or in school (e.g. MySpace.com). These experiences are useful and important, but children need training in broader dimensions of cyber awareness in order to create a more educated, secure community as the Information Age sweeps through society. Just as we teach our children "right from wrong" in the physical world, we must ensure that the same lessons are taught in the cyber world as well. As reported through the Virginia DOE's *Guidelines for Internet Safety in Schools* (2006b), "children need to develop a good immune system through gradual exposure to the unfiltered Internet. Meanwhile, parents and teachers must help children learn appropriate responses to potentially harmful online experiences."

A Kansas State University (KSU) study, *Recommendations for Digital Citizenship in Schools* (Ribble & Bailey, 2004a), identifies a few examples of how cyber awareness education for children should include “survival skills” such as understanding harassment, copyright violations, chatting, cell phone etiquette, and appropriate use. Results of their study include the following alarming examples:

- Using e-mail or websites to intimidate students (also known as cyber bullying) has become an epidemic in many schools. Cyber blackmailers threatened to delete computer files or install pornographic images on the computers of a British school if it did not pay $25 (Reuters article, 2004, as cited in Ribble & Bailey, 2004a).
- The Business Software Alliance (BSA) reported in 2004 that software piracy alone cost the United States $1.9 billion in 2002. Downloading programs and music illegally from the Internet has become a serious concern for educators (Ribble & Bailey, 2004a).
- Text chatting with PDAs and computers while classes are being held has been reported to be a major distraction to students and teachers in technology-infused schools. A survey by Blue Coat System in 2003 found that 65% of United Kingdom and 39% of United States students in their study found occurrences of instant messaging for personal conversations during school hours (Ribble & Bailey, 2004a).
- Students using cell phones before, during, and after class has been reported to be a major teacher concern. Use of cell phones in schools has caused problems

regarding when and where cell phones can be used. A 2003 study performed by Cingular Wireless states that 39% of those surveyed would answer a phone while having face-to-face conversations (Ribble & Bailey, 2004a).

Defining Internet Safety

After a detailed literature search, it was clear that Internet safety is still being formally defined in educational and other technology-related literature. Through this research, several key themes began to emerge, including (a) Internet use etiquette, sometimes referred to as “Netiquette,” (b) Cyber Communication, (c) Cyber Education, (d) Cyber Access, (e) Cyber Commerce, (f) Cyber Responsibility, (g) Cyber Rights, (h) Cyber Safety, and (i) Internet Safety (Self-Protection).

The theme that was further developed in JMU’s higher education model was that Internet safety encourages membership and acceptance of a globally connected community—which includes exercising certain social behaviors just like regular citizens who have rights, duties, and privileges to make informed decisions every day. Not a day goes by where technology in some capacity is not used; therefore, an online world of citizenship is necessary. This project demonstrated the linkage and collaboration of a number of professional communities working together to achieve a specific desired result for Rockingham County higher education and middle school needs that is a component of cyber citizenship. A true “one-team” attitude for successful collaboration in delivering a proper Internet safety resource for the middle school community was shared by all participants.

Identifying and categorizing Internet safety topics are complex and ongoing tasks. This is the reason that technology leaders require specific and rich resources to help them understand Internet safety and develop programs for their school districts. JMU's *Kids Guide* provides technology leaders with materials and resources that affords them the ability to develop comprehensive Internet safety programs for today and in the future. There are many programs and alliances developed through allegiances between industry, state and federal government interests, and experts in the field, to educate the public about risks associated with inadequate Internet safety and to offer tips to help enhance Internet safety. For example, the CyberSmart program is designed to help K-12 educators, administrators, and professionals as well as university professors, executives, and IT administrators develop programs that help empower students, faculty, and school administrators to take personal responsibility for keeping personal and public computers secure (CyberSmart Education Company, 2005b; see CyberSmart.org).

An academic or educator vision for *Internet safety* includes the following qualities, which encompass the basis for JMU's *Kids Guide:*

- **Internet Safety—**Protecting a child's PC and personal information.
- **Cyber Ethics—**Teaching children proper modes of behavior online.
- **Cyber Safety—**Protecting children from predators who initiate contact online.

Computer technology touches almost every aspect of our lives—from home to academia, from professional life to recreation. The Venn diagram created by the researcher, Figure 1, highlights the importance of three interrelated disciplines which must come together to capture the educational essence of cyber citizenship practice, as supported by the literature review (Chapter II). This research is not trying to quantify this case study's theory with this Venn diagram; the figure merely suggests that the circles' intersections define a territory of particular complexity and significance. *In fact, it locates the heart of the matter***.** In this instance, the heart is where Internet safety, cyber safety, and cyber ethics meet to form ***cyber citizenry***.

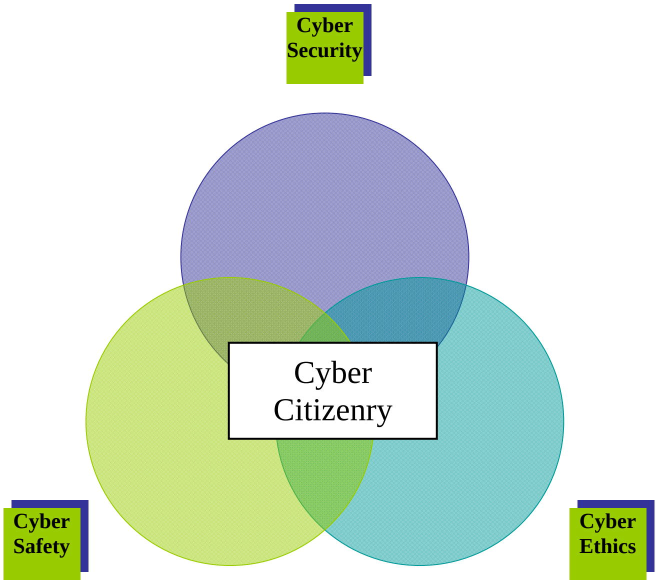


Figure 1. Internet safety: Cyber security, cyber safety, and cyber ethics overlap to form cyber citizenry.

The U.S. Congress has encouraged schools to implement policies and protection technology to filter and block obscene content. The Children's Internet Protection Act of 2002 (American Library Association, 2006) requires those steps to qualify for E-rate discounts and certain federal funding. Some schools teach cyber safety, but not as part of any federal- or state-mandated curricula. Some websites offer educators sample lesson plans, advice, resources and training on cyber safety (e.g. iSafe and CyberSmart). Content often includes lists, articles, and links to other resources. Similar material is offered to parents and for self-learning by children. But in 2002 most self-learning games were appropriate only for a very young audience. A few sites offered games that taught cyber safety to various ages of children, but the games' presentation was usually well below the sophisticated animation seen on television, in motion pictures, and in video games. Most content was free of charge. However, a common characteristic was the assumption that users had a lot of time to read through articles on a myriad of websites.

The advancement of technology and innovation since 2002 (e.g. better use of streaming video and more Web-friendly applications) has afforded organizations an opportunity to improve their website content, increase their outreach, and not limit themselves and what they can share online in an effort to improve their Internet safety programs. For example, one organization that is leading the way with cutting-edge technology via video representations of their cyber safety awareness campaign is Web Wise Kids (webwisekids.org). This sites does an extraordinary job in connecting the student to real-life examples in an entertaining way that appears to fit the target audience's age group interest levels. One of its applications is the "Missing" game (Web

Wise Kids, n.d.), which tells the story of child who forms an online friendship with a social network user. This anonymous user has an online magazine and sends the child cool stuff, like graphic arts and software. Little does the child user know that this other guy is actually a predator. After the child agrees to meet this predator, and unbeknown to the child), players work with a detective to find and rescue the child and arrest the predator. This is just one wonderful example of how technology advances in the past few years have allowed better capabilities for organizations to share their Internet safety messages with children, adults, and schools.

All technology users need to realize that technology is a tool—and to control a tool, one must know how to use it appropriately. It is the individual’s role to know what is acceptable and what is not. Acceptable Use Policies, rules and laws exist that are established for Virginia education institutions; technology leaders need to begin to understand the issues and disseminate the information to those who can make the largest impact on the future: educators. JMU’s *Cyber Citizenship for Kids Guide* (IIIA, 2007) is an attempt by a well-known and respected higher education institution to share the importance of their expert knowledge in teaching and learning with the K-12 and middle school community.

Cyber safety includes teaching children how to protect themselves from unscrupulous people who operate Web sites, contact them online, or attempt unsupervised meetings in person. Widespread opportunities for unsupervised Internet use have created a demand that parents and teachers train children in cyber safety skills. Children must learn a healthy respect for the positive and negative actions presented via a computer screen. Unlike the controllable, passive experience of television, Internet access presents real opportunities for luring children into unsafe situations, bullying, or scaring them, and inflicting psychological or personal injury, abduction, or death.

Cyber ethics includes teaching children proper modes of behavior online. Children must be taught what behaviors are appropriate or inappropriate for interacting with other people online. Cyber ethics includes avoiding behavior such as hacking, writing, or spreading viruses; stealing content and lying about its authorship by copying and pasting into a writing assignment; downloading copyrighted music or videos; copying CDs and software; or pulling online pranks such as smearing another student’s reputation. Some children may succumb to temptation because the Internet seems anonymous and free of the risk of being caught. Children also must be taught the legal consequences of inappropriate online behavior.

According to the *American Heritage Dictionary*, “ethics” refers to the set of principles of right conduct (2001). Ethics is “concerned with what we consider to be ‘right’ or ‘just’ behavior” (Gibney, 1999, p. 19). Ethics refers to the guiding principles or ideals of good versus evil. They are not based in law, religion, or standardized beliefs; rather, ethics refer to a general conception of right and wrong which transcend both religion and law (*Webster’s Dictionary*, 2001). “Cyber ethics” refers to applying ethics into the online or virtual environment (Consortium For School Networking (COSN), 2004).

Internet safety entails teaching children about protecting their PC and their personal identity while using the Internet. Most of the responsibility for installing and maintaining technical systems for Internet safety appropriately rests with parents for home PCs and with educational administrators for schools. However, children must be taught the consequences of actions such as widespread downloading of music, videos, graphics, and other content from Web sites that may be sources of viruses or software that infect their PC. Another simple action with potential for major damage is opening attachments to e-mail from unknown senders—an action that can trigger cyber attacks on the initial PC and spread to many other PCs over the Internet. Children also must be taught to restrict offering their personal information over the Internet. See Appendix A for definitions of other terms used in this study.

Summary

This study's purpose was to research, evaluate, and analyze whether a higher education institution with expert knowledge in information security, like JMU through its community outreach programs in IIIA, effectively formed a community-wide partnership approach to responded to its local K-12 educational requirements and needs regarding Internet safety education for middle school children in Rockingham and Harrisonburg City schools in 2007.

The production of JMU's *Cyber Citizenship for Kids Guide* (IIIA, 2007) was to provide Internet safety awareness and education to middle school students in Rockingham County and Harrisonburg City middle schools. If this higher education partnership was to be successful in Rockingham County and Harrisonburg City middle schools, it was expected that this higher education and K-12 community based partnership (developed around producing Internet safety awareness educational material) could represent a Commonwealth model for implementing Internet safety awareness through higher education at other communities in Virginia.

With the rate of technology growth in the classroom, it is imperative for students to learn how to become citizens of cyberspace (The Regional Network for the Exchange of Information and Experience in Science and Technology (ASINFO), 1999). JMU raised concerns about issues confronting their university and lessons learned that could be shared with the K-12 community of schools in Rockingham County. Some of the issues confronting technology-rich education include plagiarism, copyright infringement, fair use law, safety, security, identify theft, and privacy. These concerns are also noted nationally in education every day (Lewandowski, 2002; Ribble, Bailey, & Ross, 2004).

The JMU *Cyber Citizenship for Kids Guide* (IIIA, 2007) addresses a local void in Rockingham County, Virginia, where these national standards are being developed and not always effectively known or used in their entirety—as stated in an interview with Cheryl Elliott from IIIA at JMU (personal communication, July 12, 2006). This JMU *Kids Guide* also addressed the then-newly released *Guidelines and Resources for Internet Safety in Schools* Virginia-wide initiative and law (VA DOE, 2006b). Since then, Virginia K-12 schools must teach Internet safety throughout K-12 to meet the *Commonwealth of Virginia Computer Technology Standards of Learning for Virginia's Public Schools* (VA DOE, 2006b; VA Board of Education, 2005).

All Virginia school divisions currently have Internet Acceptable Use Policies and employ filtering software. These policies and filters are necessary but cannot prevent all risks to students. Since Internet threats change constantly, schools and divisions must take additional steps to safeguard students.

The Virginia Department of Education published *Guidelines and Resources for Internet Safety in Schools* (2006b) to assist school divisions in three areas:

- writing an Internet safety component as part of an acceptable use policy,
- integrating Internet safety into the curriculum, and
- fostering responsibility among all stakeholders to help protect young people from online dangers.

In response, this case study examined: (a) the mission success of JMU’s higher education partnership in trying to meet K-12 community Internet safety education needs and (b) the potential of this higher education collaboration to become a model Commonwealth solution for Internet safety awareness throughout Virginia as mandated by the Virginia Department of Education for completion in the 2007 school year.

II. LITERATURE REVIEW

Introduction

The following is a review of the literature that supports this research. To evaluate whether a program like JMU’s higher education community partnership can become a model for Virginia middle school communities addressing the Virginia state requirement for Internet safety education via JMU’s *Cyber Citizenship for Kids Guide* (IIIA, 2007), a sample of Virginia higher education partnerships was reviewed to gain an understanding of higher education’s historical perspective on assisting with K-12 issues.

Before beginning to evaluate the effectiveness of this higher education community partnership in meeting Rockingham and Harrisonburg City middle school teachers’ needs, it is important to first understand existing nationwide Internet safety coalitions and professional organizations addressing this requirement nationwide, as well as understand Internet safety and students’ risk issues, middle school teacher practices on Internet safety, and Virginia legislation and governance on Internet safety awareness and education for 2006-2008.

Higher Education Community Partnerships

Higher Education Fostering K-12 Community Partnerships

Thomas Jefferson stated the following regarding one's civic duty: "Private charities as well as contributions to public purposes in proportion to everyone's circumstances are certainly among the duties we owe to society" (Moore, 2004). Outreach efforts exist at most universities throughout this country. There are many variations on how each institution defines its level and capacity for outreach, but those definitions that were reviewed at the University of Virginia, Virginia Polytechnic Institute, and James Madison University, as examples, all focus on the following core message: "applying academic expertise to the direct benefit of others in support of University missions" (C. Elliott, JMU, personal communication, March 15, 2007; Moore, VA Tech, as cited in EDUCAUSE, 1998; Payne, UVA, as cited in EDUCAUSE, 2004). Dr. Judith Rodin, President of the University of Pennsylvania, states that "community outreach occurs when the following conditions are met at the university level":

- Link with significant human needs and societal problems, issues or concerns,
- Direct application of knowledge to significant human needs and societal issues or concerns,
- Utilization of the university's academic expertise,
- The ultimate purpose is for the public or common good,
- New knowledge is generated for the discipline and/or for another audience, and

> There is a clear relationship between the program and the university's academic units mission. (Rodin, 2004)

Higher education that wishes to engage in meaningful, significant, and relevant community outreach can form strategic alliances and partnerships. Dr. David Wilson is the Vice President for University Outreach, Auburn University, and states that the landscape is changing with university involvement in community in a very positive regard: "Residents of communities are no longer receptive to academicians as lone rangers who come into communities and prescribe solutions to social, economic and educational needs and conditions without involving the communities in the solution" (Wilson, 2005).

Some literature suggests that from a systems perspective, the K-12 education system can be considered an important highway to the university. All things equal, the better the quality of students in K-12, the better these students are entering higher education, and in the future by representing the university in its scholarship activities: "For public universities, there is an expectation from the community that higher education will help address pressing social and economic problems, and K-12 education is considered to be a major issue in most communities" (Lassner, 2006).

Sample Set of Virginia Universities' Successful Partnerships

Higher education's model in conducting its business relationships and finding mission success for its constituents and community is no different than many government agencies, nor private industry. The researcher's professional experiences in several government agencies has led to understanding the sensitivity in sharing information—

which has often been a sticking point for efforts to move ahead as an organization or common community of interest. Virginia public universities are finding that the only way to success is through collaborative environments and partnerships to help them leverage each other's resources, unique talents, and levels of expertise, and to provide opportunities for new funding, marketing, and support services statewide. Without these three components—"external forces, internal pressures for change, and resources for change—piecemeal, incremental adjustments to the status quo will be the order of the day" (Toffler, 1985). The following samples show some recent higher education partnership efforts at Virginia Polytechnic Institute and the University of Virginia, to better understand their localized motivations and strategies for forming successful partnerships with their communities of interest in Virginia.

Virginia Polytechnic Institute. Virginia Polytechnic Institute's (Virginia Tech or VT) collaboration with state and local governments, private business, and K-12 schools in Southside Virginia is transforming Danville's distressed economic community into a center of innovation and high tech opportunities with new-found growth. Virginia Tech viewed the opportunity to extend its own technology integration and implementation processes to this distressed region as a logical next step. The project involved complex relationships among local governments, K-12 and higher education, and a local foundation in Southside's Dan River regions (Moore, 2004). A K-12 roadmap was drawn and with the cooperation of VT, the Department of Education and the Danville community, a new magnet high school focusing on biotechnology was on the drawing board (eCorridors, 1999). VT, through its eCorridors program, has positively impacted its educational communities. This carries forward to 2008 where VT has developed a “real world” large and scalable infrastructure with the community in mind. This community-oriented network provides a high-tech sandbox where K-12, private sector partners, municipalities, and non-profit partners all have a unique opportunity to collaborate on a set of common theme programs to support the Blacksburg community at large (eCorridors, 2002).

Higher education institutions have long histories of community outreach activities. In recent years, the Kellogg Commission and concerned leaders have called for institutions to migrate their activities from one-way outreach to two-way engagement partnerships with their surrounding communities (Hirshhorn, 2002). As Virginia Tech works toward an engagement model for the 21st century, many of the university’s strategies in the Dan River region could function as proof-of-concept initiatives for models useful in other communities.

University of Virginia. Scholars such as Peter Senge, Arie De Geus, and Meghan Wheatley stress the power that lies in ownership of participation and inclusion: “For collaboration and partnership to be successful, there must be ownership at all levels” (De Geus, 1997). Partnerships often happen between higher education and large corporations as well. Such was the case of an example with International Business Machines, Inc. (IBM) and University of Virginia (UVA). In this example, IBM helped UVA establish an Institute for Advanced Technology in the Humanities, which helped change the way faculty in the humanities interacted with peers, students, and research labs (Payne, 1999). While this partnership was project-based, it offered IBM an opportunity to increase its share of the higher education marketplace, as well as the ability to create new environments for research, enhance new products and services, and improve the quality of the current workforce. In return, higher education, through its students and scholarship efforts, potentially returns the knowledge investment back to IBM through future employment opportunities for graduating UVA students.

Change may be motivated by external factors, but rarely occurs unless enough citizens inside of the community want change, are willing to work for it, and know how to secure or leverage the resources required for it to occur. Much of the literature on substantive change suggests that external factors may either inspire or force people to think about the need for change, perhaps even moving them to the point of proposing new directions (Wheatley & Kellner-Rogers, 1998; De Geus, 1997; Senge, 1994). The literature on constructivist, experiential, and organizational learning suggests viable options for engaging in community-based activities. Boyte explained that successful civic learning organizations stress learning as productive work aimed at community problem-solving and capacity-building. He further suggested that an empowering, people-oriented process will build public relationships across rigid boundaries of old (2002).

At the heart of community change lies developing human relationships focused on change, human capital that responds to new challenges, new and sustained alliances that cross traditional community boundaries, and other kinds of relationship-building activities. Sherry Turkle, in an interview with *Harvard Business Review,* suggested that "computer software changes how architects think about buildings, surgeons about bodies, and CEOs about business. It also changes how teachers think about teaching and how their students think about learning" (Coutu, 2003, p. 44).

Higher education has historically been a vehicle for our nation's and communities' progress; yet, some argue that the social conditions in which education has traditionally occurred are changing beyond recognition.

In examining the forces of change in society today, Jarvis, Holford, and Griffin suggested that

> the risks, illusions, and ambiguities of a postmodern world call for replacing traditional notions about education, a vestige of modern societies where stability, confidence, and progress were the social order of the day, with a new concept of learning over a lifetime. (2003)

Internet Safety in Schools

Internet Learning Experience

Adolescents view cyber communication as a natural extension of peer socialization; systematically extending cooperative/collaborative learning to these types of media could provide teachers with additional means for motivating student inquiry, as well as building fluency and confidence with reading and writing. What remains to be understood are the ways in which these principles inform the pedagogies of practicing teachers and teacher–educators, whether the conditions for developing successful experiences with online communications are present in many classrooms, and a statistical analysis of teachers who do or do not introduce such activities in their classrooms. If pedagogy and practice include integrating such technologies in classroom activities, is there a corresponding improvement in literate behaviors on the students' part? If little integration is taking place, are there ideological, technological, or political barriers that make it difficult for teachers to include such activities in their instructional methods?

One study indicates that Web logs (blogs) can provide a means to help struggling students authentically engage with text by providing a multi-genre, multimedia reading and writing space (Kajder & Bull, 2003). The authors argue that blogs encourage creativity by providing the means of entry into work with visual and print text, indicating that their work "is just a start at defining best practice [and] a glimpse of the possibilities and an invitation for [educators] to examine, invent, reinvent, and ultimately join in the conversation" (p. 35).

Another study focused specifically on Instant Messaging (IM), in particular AOL Buddy Chat, finding that engaging in such technologies enables students to express with immediacy something they have to say that they feel is worth hearing. This is, of course, predicated on the impression they have just read something worth reading. According to Beach and Bruce (2002), chat rooms and IM require cognitive processes that are consistent with Dewey's definition of the four primary interests of a learner in an inquiry-based learning environment: investigation, communication, construction, and expression. Internet-based communication can "create contexts that allow participants to share their opinions, beliefs, and ideas" and experiment with different voices and audiences (p. 150-151). This allows students to position themselves to authentically construct meaning from various textual situations with an authority and greater prior knowledgebase than they might with traditional texts. "The ability to frame or contextualize topics or issues in terms of different components operating in social worlds or systems is central to inquiry learning" (Beach & Bruce, 2002, p. 157). Educators, particularly those charged with developing literacy instruction for adolescents, can capitalize on adolescent engagement with, and knowledge of, literate behaviors in these contexts: "framing instruction in this manner mirrors adolescents' attempts to cope with the complex, ill-defined problems, issues, and dilemmas in their everyday lives" (Beach & Bruce, 2002, p. 155).

The Center for Education and Research in Information Security (CERIAS) conducted a pilot study of vulnerabilities in K-12 systems in the state of Indiana. This study showed that the IT systems of K-12 schools are vulnerable; for example, 40% of the participating schools were easily penetrated from the Internet, 100% of the schools' Children's Internet Protection Act CIPA protection measures were easily circumvented using basic tools and techniques well within the grasp of an average student, and payroll and grade systems were relatively easily penetrated in 90% of the schools (CERIAS K-12 Outreach Program, 2003, p. 3). These vulnerabilities have potential downstream implications for misusing data, misusing system services, personal safety, crimes against children, and public embarrassment to schools. For example, confidential and sensitive information can be stolen, lost, and exposed to the public. The threats and vulnerabilities associated with school information systems are especially pertinent to K-12 educators and support staff, who are obligated to protect sensitive information such as assessment data under the Family Educational Rights and Privacy Act (FERPA), one of the nation's strongest privacy protection laws.

Virginia State Legislation on Internet Safety in Schools

Until recently, applicable legislation has not been able to keep pace with technological developments, and the constitutionality of many legal solutions has been challenged. Nonetheless, many states have crafted statutes which address child pornography and computers. Federal and state law also has evolved to ban computers as a means of soliciting children for sexual activity, and additional proposed legislation may lead to future statutes designed to safeguard youth. Currently, legal solutions provide a reactive rather than proactive intervention to counter cyber victimization of youth.

The Virginia Department of Education presented House Bill 58 and its process for developing guidelines for schools to implement the mandates of this law at a National Internet Safety Alliance meeting on July 14, 2006 (“Virginia’s Internet Safety Law,” 2006). Virginia is the first state to enact legislation and a process for developing guidelines for schools regarding Internet safety. Virginia’s Internet Safety Law H.B. 58, sponsored by Delegate William Fralin, Jr., and passed by the 2006 General Assembly, requires that school divisions’ Acceptable Use Policies “include a component on Internet safety for students that is integrated in a division’s instructional program” (“Virginia’s Internet Safety Law,” 2006). This legislation also requires the Superintendent of Public Instruction to issue guidelines to school divisions regarding instructional programs related to Internet safety.

Virginia’s Governor Kaine signed this bill into law with no amendments on March 7, 2006. These *Guidelines for Internet Safety* and/or *Guidelines and Resources for*

Internet Safety in School (2006b) were published on October 10, 2006, and went into effect for all Virginia schools starting with the 2006-2007 school year.

Internet Safety and Student Risks at Home

A critical component of Internet safety addresses the fact that students have unprecedented access to information without regard to geographic boundary lines or jurisdictions. The perceived anonymity of cyberspace can lead to irresponsible behavior. When children cannot validate the physical location or identity of an individual on the other end of the message, they may believe that their activity causes no perceptible harm and there is limited chance for detection and punishment. In the context of cyberspace identity deception is commonplace, diminishing self-regulation and contributing to disconnected behavior. But in conjunction with early preparatory experiences which engage a child in assessing risky situations, developing appropriate coping techniques, and practicing responses to problematic situations, children can be adequately prepared for potential risks on the Internet (National Internet Safety Alliance, 2006). Avoidance techniques, de-escalation skills, and protection strategies are additional safety mechanisms children need on the Internet (National Internet Safety Alliance, 2006).

Safety is paramount when students go online. Children need to feel competent to safely manage their online experiences, to know how to deal with uncomfortable situations, and to know when to seek adult help. Brief presentations and handouts with online safety tips are not sufficient. These issues need to be integrated into an ongoing dialogue. Netiquette, or online manners, define acceptable conduct when engaged in an interchange with people in cyberspace. Netiquette represents guidelines for relating in a courteous and respectful manner and emphasizes awareness that computers are merely a mechanism for communicating with other individuals. Applying rules which assist young people in making informed decisions and allow them to demonstrate an ability to apply online critical thinking skills facilitates productive social participation (National Internet Safety Alliance, 2006).

Moreover, Netiquette counters the threat of potential disengagement of young people from positive social interactions, especially when the guidelines include limits on the time spent on the computer (EDUCAUSE, 2005).

Cyberspace Communication

Online chat rooms are a popular venue to initiate exchanges between youth and individuals who are threats to their safety and wellbeing. In this virtual world, children assume new identities through their nicknames and then are expected to manage control over their private information while trying to build relationships, engage in self-expression, explore their own identities, and find validation. This process has been referred to as “a complicated juggling act which requires sophisticated skill in performing chameleon-like behaviors and attitudes” (O’Connell, 2001). Existing knowledge on psychosocial implications for sexual exploitation provide an initial frame of reference to understand the impact of deception and online interactions.

Although cyberspace mirrors some aspects of other experiences, there are major differences which may mediate behavior. For example, it is difficult to merely classify the online enticement of a child as “acquaintance abduction” versus “stranger abduction” since it has dynamics of both. After months of forging an online relationship with someone, a child no longer perceives this individual as an outsider. Additionally, the defenses against strangers often are not triggered when a youth perceives that he or she is interacting with a peer. In cyberspace, mutually anonymous interactions lead to developing close relations with others without benefit of visual cues which are typically important in socially categorizing others and subsequent interaction. Online identities are self-constructed and can be repeatedly modified to recreate one's online persona. Usually one's self identity is relatively static and strongly associated with physical characteristics (gender, age, weight, race). Identity construction on the Internet allows experimentation with various possible selves. The usual constraints of particular roles are nonexistent and identity can be fluid (Gurak, 2001; McKenna & Bargh, 2000). The adult can manipulate the child's initial interpretations of their interactions and continue to present himself or herself as a child so that when the contradictions become apparent, children will attempt to reinterpret the actions rather than disbelieve the adult's original identification of being a child (O'Connell, 2001). Identity deception is an inherent part of online communication, and transformations can have positive and negative repercussions for youth—who also experiment with their online personas.

Berson, Berson, and Ferron (2002) noted that many adolescents describe online interactions which are characteristic of a culture of deception in which students' primary activities involve exchanging verbally harassing or sexually suggestive chat. In e-mails and chatrooms where respondents describe spending the majority of their online time, young people report insulting each other, exchanging sexual quips, attacking others' opinions, and engaging in generally outrageous behavior. Young people often perceive that there is little chance of detection for misconduct online, minimize the potential harm to others that may result from their actions, and equate a behavior's legality with its ethics (Willard, 2002). Computer crimes, such as computer hacking, also are increasing in frequency, despite their serious offline legal consequences (Aftab, 2000). Since computer activities appear to be victimless and faceless crimes, their true repercussions may not be discernible to a young person in comparison to the potential and/or perceived benefits.

Education Guidelines

Professional organizations' guidelines for using technology in K-12 education are part of the framework for learning Internet safety in middle schools. In the Integrating Literacy and Technology in the Curriculum summary by The International Reading Association (2001) there is one item on appropriate use of technology: "Opportunities to learn safe and responsible use of information and communication technologies." The National Science Teachers Association (1999) developed a position statement on using computers in science and within it, there are two statements concerning issues related to technology use: "Exemplify the ethical use of computers and software," and "Seek to provide equitable computer access for all students." Two recommendations within the technology guidelines by National Council of Teachers of Mathematics (2003) are "to strive to instill dispositions of openness to experimentation with ever-evolving technological tools and their pervasive impact on mathematics education," and "to make informed decisions about the appropriate implementation of technologies in a coherent instructional program." The National Council for the Social Studies continues to adopt guidelines at this time (2008), and the focus is on curriculum and instruction in middle school. In addition, Bennett (2005) developed technology guidelines in the Social Studies classroom based on students' rights, responsibilities and respect.

While these guidelines are available for review by all educators, the potential for change within the K-12 school system may not occur until a team of middle school teachers analyzes the guidelines and develops a school or team plan that is consistent with the school's own behavioral guide; then middle school teachers can be prepared to infuse Internet safety into instruction. This step can be achieved with resources such as the *Cyber Citizenship for Kids Guide* created with the cooperation of James Madison University, the Virginia Department of Education, and a sample of Virginia middle school teachers.

Middle School Education Audience

Middle school education around the country usually requires students to be proficient in using technology, but does not always provide clear guidelines for being a "good cyber citizen." Along with including technology in the classroom, it is ethically imperative for students to learn how to become citizens of cyberspace (The Regional Network for the Exchange of Information and Experience in Science and Technology (ASINFO), 1999). Courses incorporate technology tools appropriate to the disciplines, but there may not be a concerted effort to incorporate ethical, legal, or social studies issues related to using technology.

As new technologies are rapidly added to schools, issues are emerging that confront education. Plagiarism, safety, copyright laws, fair use, security, and privacy plague education every day (Burbules & Callister, 1996; Willard, 2002; Swain & Gilmore, 2001; Ribble, Bailey, & Ross, 2004). Guidelines, rules and laws to govern technology use in schools are being developed to address these issues, such as those currently enacted in Virginia through the Virginia Department of Education ("Virginia Internet Safety Law," 2006).

Responsible, respectful, and acceptable behaviors while using technology are concerns in mathematics, science, English, and social studies classrooms. Whether using an online primary source document on a current political campaign, or online submission of a research paper on the pros and cons of a current health care issue, middle school students are learning behaviors related to using technology in each discipline. In addition, every teacher in a school shares the responsibility of teaching "good Internet safety"—so using technology in learning is part of each teachers' responsibility.

A missing yet vital component in middle school education is the fact that teachers in subject area courses not only need to incorporate acceptable technology practices into their instruction, but also need to be able to handle emerging technologies proficiently. Middle school teachers need the knowledge and skills to address the issues related to using technology within disciplines and to infuse appropriate Netiquette into instructional practices in middle school education. Teachers need guidelines to understand using technology in specific disciplines. Currently, teachers can incorporate technology guidelines developed by professional organizations for mathematics, science, literacy, social studies, and the middle level association. In addition, the National Education Technology Standards for first year teachers (NETS-T) (International Society for

Technology in Education, (2002b) require teachers to be technologically literate about the issues concerning technology use, and National Education Technology Standards for Students (NETS-S) technology standards provide requirements for students to master computer technology concepts (International Society for Technology in Education, (2002a). These categories provide a framework to link performance indicators within the Profiles for Technology Literate Students to the standards. Teachers can use these standards and profiles as guidelines to plan technology-based activities in which students achieve success in learning, communication, and life skills.

While it is valuable to have a framework, it is just as critical that middle school teachers incorporate Internet safety as it is to teach middle school students how to be “good” citizens of the school or community. Therefore, the hardest part is to find discipline-specific instructional strategies for middle school students. The *Kids Guide* (IIIA, 2007), which was developed in collaboration with Rockingham County and Harrisonburg City middle schools and was tied directly to the Virginia Standards of Learning for various disciplines, is an exception. Internet safety creates a unique challenge for teachers to integrate Netiquette into their pedagogical practices in subject area courses. Some issues include privacy of student information, online identification of minors, abuses of online communication tools, responsible use of online research tools, and using socially acceptable manners while communicating online. As new technologies become everyday tools for middle school students, teachers need to be informed citizens on appropriate technology uses in the classroom.

Internet Safety Learning Models for Teachers

Integrating the ethical, legal, and social issues related to technology is a significant challenge because middle school teachers may not have participated in professional development related to the topic. This section focuses on what teachers can incorporate into curriculum and instruction.

One way to infuse the technology standards into a course is by requiring students to use the technology standards within lessons. The CyberSmart curriculum includes numerous lessons for middle-level students on responsible use of technology, and each lesson aligns to the National Education Technology Standards for Students (NETS-S) standards (CyberSmart Education Company, 2005a). CyberSmart lessons integrate literacy, social studies and science through units on manners, advertising, safety, research, and technology (2005a). A valuable activity for a middle-level class is to participate in blogs, chat rooms, or instant messaging about a specific topic.

Beyond the mathematics, literature, social studies, or science curricula in middle school, Internet safety courses can focus on promoting the welfare of the online community or using technology to take action for the common good within the online community. For the welfare of the online community within a course, teachers need written guidelines for consequences when a student’s social, moral, or ethical behavior is not acceptable. For active online citizenship, teachers can write letters to political or civic leaders, solicit support for a local or global environmental concern, or discuss current or controversial issues in middle level classrooms with an international community. Infusing these ideas into the courses can promote Internet safety by opening communication lanes with students on safe and responsible Internet usage, and how to recognize the relevance of issues such as online privacy, online predation, cyber security, and intellectual-property use to actual Internet behaviors.

Another method is for teachers to model whom to contact when issues arise outside of the teacher's experiences, abilities, or typical responsibilities. A few cyber "crimes" include piracy, hacking, copyright laws, pornography, fair use, security, and privacy. When issues arise, educators can teach more about the topic, contact an expert, problem solve, and then develop a plan for the future. Along with curriculum and instruction, these are legitimate issues to incorporate into courses.

According to the National Education Technology Standards for Students (NETS-S) (International Society for Technology in Education, 2002a), students in the sixth through eighth grades should be able to "use content-specific tools, software, and simulations (e.g., environmental probes, graphing calculators, exploratory environments, Web tools) to support learning and research and apply productivity/multimedia tools and peripherals to support personal productivity, group collaboration, and learning throughout the curriculum." Middle-level students use technology to communicate and research, so this is an ideal time to include instruction on proper technology use.

One factor in understanding how to include Internet safety in the middle school classroom is to recognize the developmental needs and interests of the 11- to 13-year-olds. Middle-level students are looking for social interactions with peers and more independence in selecting activities. Teachers need skills to guide students on what is responsible and respectful behavior in the online global community. A few basic guidelines are to develop cyber citizen rules for the classroom, to be observant and monitor what students do on computers, and to keep track of who uses the computers.

Computer Technology Standards of Learning for Virginia's Public Schools

The current Commonwealth of Virginia Computer Technology Standards of Learning (VA Board of Education, 2005), developed by the Virginia Department of Education, identify and define the progressive development of essential knowledge and skills necessary for students to access, evaluate, use, and create information using technology. These standards provide a framework for technology literacy and demonstrate a progression from physical manipulation skills for using technology, to intellectual skills necessary for information use, to skills needed for working responsibly and productively within groups. Computer/technology proficiency is not an end in itself, but lays the foundation for continuous learning. The focus is on learning using technology rather than learning about technology. The Virginia Department of Education defines "technology literate" as possessing technology skills that support learning, personal productivity, decision making, and daily life decisions (VA DOE, Office of Educational Technology, *2003-2009 Educational Technology Plan for Virginia*, 2006).

To become "technologically proficient," the student must develop skills through integrated activities in all content areas K-12, rather than through one specific course. These skills should be introduced and refined collaboratively by all K-12 teachers as an integral part of the learning process. Teachers can use the *Commonwealth of Virginia Computer Technology Standards of Learning* (VA Board of Education, 2005) as guidelines to plan technology-based activities in which students achieve success in learning and communication, and are prepared to meet the challenges of today's technology-rich working world.

The following excerpts are from the Virginia Department of Education's *Guidelines and Resources for Internet Safety in Schools* (2006b).

Grades 6-8 Technology Standards of Learning

Basic Operations and Concepts

1. The student will demonstrate knowledge of the nature and operation of technology systems.
2. The student will demonstrate proficiency in the use of technology.

Social and Ethical Issues

1. The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.
2. The student will practice responsible use of technology systems, information, and software.
3. The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.

Technology Research Tools

1. The student will use technology to locate, evaluate, and collect information from a variety of sources.
2. The student will evaluate and select new information resources and technological innovations based on the appropriateness for specific tasks.

Problem-Solving and Decision-Making Tools

The student will use technology resources for solving problems and making informed decisions.

Technology Communication Tools

The student will use a variety of media and formats to communicate information and ideas effectively to multiple audiences. (VA DOE, *Guidelines and Resources for Internet Safety in Schools*, 2006b)

Significance of the Study Based on the Literature Review

Internet safety awareness and education for the cyber citizen are relatively new. Testimony was previously provided by EDUCAUSE (Peterson, 2004) before the 2004 Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census Committee on Government Reform to the United States House of Representatives relating to a hearing on “Protecting Our Nation’s Cyber Space: Educational Awareness for the Cyber Citizen.” That testimony revealed the importance of education and awareness for cyber citizens—both in the educational systems including K-12 through college, and in preparing citizens who will be contributors to our information economy. “The present challenges of cyber security require the establishment of a life long culture of security from the cradle to grave” (Peterson, 2004).

Improving Internet safety is a national priority; organizations were identified by the Presidential National Strategy to Secure Cyberspace to improve a diverse need and infusion of resources from public and private sources (e.g. EDUCAUSE, Internet2, and Network Security Task Force). These organizations received a grant from the National

Science Foundation (NSF) to identify and implement a coordinated strategy for higher education. EDUCAUSE is a nonprofit association with a mission to advance higher education by promoting intelligent technology use with roughly 1900 colleges, universities, and organizations, including more than 170 corporations (EDUCAUSE, 2005). Internet2 (2007, see http://www.Internet2.edu) develops and deploys advanced network applications and technologies for research in higher education. Its leadership consists of more than 200 universities working collaboratively with industry and government to foster behaviors and attitudes for the Internet today (2007).

This National Security Task Force is coordinating its efforts on behalf of higher education institutions with the support of the Higher Education Information Technology Alliance (http://www.heitalliance.org) whose members include the American Council on Education, Association of American Universities, National Association of State Universities and Land Grant Colleges, American Association of State Colleges and Universities, National Association of Independent Colleges and Universities, and the American Association of Community Colleges.

What appears missing is a focused and organized national effort to teach children Internet safety, cyber ethics, and cyber safety with national security in mind. These elements of cyber awareness are vital because pervasive use of the Internet also poses risks that may harm children’s emotional and personal safety. The technology, unfortunately, enables devious and unethical behavior toward people, organizations, or information technology underpinning critical infrastructure. The cyber education our children receive sometimes does not go far beyond how to turn on the computer and use a mouse**.** It is alarming that we are not more effectively teaching Internet safety, ethics, and safety at an early age. Poor awareness by children about Internet safety may cause inadvertent damage to their own PC, other electronic devices, or personal information, and could ultimately threaten the fabric of our nation's critical cyber infrastructure.

A key issue is the question of "Who does the teaching?" Some assume this kind of education should occur in school by teachers following authorized curricula. Perhaps it should. There is a need for guidelines and lesson plans to help teachers address cyber awareness as children use PCs and the Internet. But teachers' plates are already full with the challenging requirements of *No Child Left Behind* (EDUCAUSE, 2005). Adding sole responsibility to teachers for cyber awareness education could backfire. The Reagan-era national anti-drug message *Just Say No* was underpinned by the omnipresence of public service announcements, and has produced a much more aware citizenry. In cyber awareness education, there has been a national effort to standardize expectations and methodologies for the teacher's role. A national cyber awareness program could provide the vital infrastructure for securing the country's technological-based fabric and develop awareness for future generations.

However, as the literature review demonstrates, there has been little community focus on this national concern. Therefore, school districts have gained little or no momentum in implementing responsible use efforts; while the resulting messages of these existing national cyber awareness programs is positive, the process they applied has been a "top-down" approach from the national level to the state level and appears to be missing the target of getting into the K-12 schools to effectuate their desired program result.

Parental involvement is critical to the success of any national canvass relating to our youth and could augment efforts made by teachers. Parents are responsible because they pay family Internet service fees for the PC, the mobile phone or PDA, instant messaging, digital music services, and photo uploads. The parental responsibility for children’s cyber awareness is fairly straightforward: Parents should teach and enforce proper behavior.

Summary

This literature review demonstrates that Internet safety education and awareness is a fast-moving priority for educators at all levels of K-12, and educators cannot and should not take on this responsibility by themselves. To be successful, educators need support from their community through partnerships, resource assistance from subject matter expert institutions, and guidance from their state-level authority on educational best practices.

The NSTA recommends that middle school science teachers “provide numerous opportunities for professional development experiences to bolster their knowledge of science content and enhance their skills in working with the middle level age group” (NSTA 2003). To this end, if educators are to teach Internet safety, there is strong evidence they will need the full support of their community to include their leadership team, the community at large for subject matter expertise and resource support, and their state’s board of education. In Virginia, these key players in this new paradigm of educating students on Internet safety best practices must shape efforts to integrate Internet safety education with Virginia's guidelines and standards for education, promote further collaboration among higher education and the K-12 community, provide teachers with exemplary Internet safety curriculum materials, and work time into the school day for high-quality professional development programs relating to Internet safety.

When higher education serves as a leader in its community, it can gain a better understanding of the realities faced within its region—and can become a catalyst and innovator in leading technology insertion and learning development strategies. Moreover, higher education gains practical insight through hands-on activities and practical application of its own education and awareness models such as the *Cyber Citizenship for Kids Guide* (IIIA, 2007) aimed at cyber safety awareness for middle school-age students. As will be shown in the following chapters, this JMU-led cyber safety awareness campaign for middle school students in its Rockingham County and Harrisonburg community includes fieldwork, partnership, and teamwork with the VA Department of Education and K-12 education community. JMU, like its sister universities in Virginia, exemplifies citizenry in cultivating community awareness and information awareness among citizens of cyberspace.

III. METHODOLOGY

Research Methodology

The purpose of this research was to conduct a case study on how a higher education institution in Virginia (JMU) developed and led a community-wide partnership with the Virginia Department of Education and the Rockingham County and Harrisonburg City middle schools to address a state-mandated effort for the K-12 community regarding mandatory cyber safety education for their students. Specifically, this study evaluated whether a higher education community partnership through JMU's interpretation of the state's new requirement for Internet safety education via its development and delivery of a *Cyber Citizenship Kids Guide* (IIIA, 2007) was effective. To achieve this end, middle school teachers, school administrators, instructional technology resource teachers (ITRT), counselors, resource officers, school media specialists, JMU staff, and Virginia Department of Education's Office of Educational Technology staff participated in a combination of surveys, interview questionnaires, and personal interviews.

The objective was to answer the following three research questions:

1. Was JMU's grassroots approach, as a subject matter expert in information security education, and through its community-based partnership with VA

DOE and middle school teachers in Virginia, perceived as being effective in helping Virginia educators meet the requirements set forth by the VA DOE's *Guidelines and Resources for Internet Safety in Schools* (2006b) with its *Cyber Citizenship for Kids Guide* (IIIA, 2007) for Internet safety awareness and best practices?

2. Was this community partnership on cyber safety between higher education and K-12 institutions perceived by the educational stakeholders as feasible and effective?
3. Finally, what aspects of this county-wide community partnership effort to enhance K-12 cyber safety awareness can serve as a credible delivery model for Virginia Commonwealth and federal efforts in this area?

To answer the research questions, the following instruments were created for this study and provided to participants as described in this chapter. Responses were collected anonymously.

- Survey 1: Understanding the Current (Initial) State of Collaboration Between Higher Education and the K-12 Community, October 9, 2007 - November 15, 2007 (Appendix B).
- Survey 2: Understanding the Collaboration, December 1, 2007 - January 15, 2008 (Appendix C).
- Stakeholder Questionnaire/Interviews, October 9, 2007 - February 15, 2008 (Appendix D).

This research focused on qualitative research that was specific to Virginia middle schools, as well as existing national programs promoting Internet safety best practices and curriculum for K-12 schools.

Researching and validating the perceptions of this community partnership and its derived “best practices” were achieved through a case study in selected middle schools in 1) Rockingham County and 2) Harrisonburg City, which surround JMU. Although participants near JMU—part of its community—were desired, the particular middle schools that participated were chosen at random for this case study, and all constituents who would be involved with this qualitative research at these particular schools voluntarily agreed to participate. Therefore, the research included a number of middle school teachers, instructional technology resource teachers (ITRT), counselors, resource officers, school media specialists, JMU staff, and Virginia Department of Education, Office of Educational Technology staff participated in a combination of surveys (Appendices B and C) and stakeholder interviews (Appendix D). Middle school staff participants were not chosen by this research, but volunteered for this research case study through their respective liaison school official.

This research was approved by the Director level for both Rockingham County and Harrisonburg City schools, and it was requested that these senior oversight policymakers for these school districts provide a liaison or advocate to aid in recruiting and administering the research tools (surveys and questionnaires) electronically to their middle school communities. It was hoped that having the liaisons be the internal advocates for the study (rather than the researcher, an external advocate) could lead to greater and/or more enthusiastic participation. The directors agreed to select the liaisons.

These two liaisons for their respective school communities posted this study's surveys and questionnaires via a link which was provided electronically by their respective school web sites (internal) for the teachers, ITRT's, resource officers, and administrators to access and complete. In addition, an electronic George Mason University Human Subjects Review Board participation agreement was posted which all participants were asked to complete, sign, and provide back in hard copy to their respective school liaison. These agreements were collected in person during one of the follow-up meetings with these schools. These approval forms were then sealed in an envelope and secured by lock in a cabinet to protect participants' identities.

There were no initial limitations placed on participating with this study other than the participants be currently employed by their respective schools/agencies.

Through the use of the online service and third-party survey tool Survey Monkey, all survey responses were collected anonymously for the first two survey tools. The questionnaires and online electronic interviews conducted with this third-party software were targeted at two categories of participants: The questionnaire was directed toward the two liaison participants to forward to the respective middle schools since these individuals were hands-on and directly involved with the collaboration exercise with JMU in producing the *Kids Guide*. Interviews could be conducted online via Survey Monkey, in person, or via telephone to better accommodate participants' schedules and comfort levels for participation. Participants who were selected for the interview and stakeholder questionnaires were chosen by the liaisons because they worked hands-on with JMU in this collaboration exercise. Potential interviewees included the Rockingham County and Harrisonburg City liaisons; VA Department of Education, Office of Educational Technology officials who collaborated directly with JMU and the liaisons; and the JMU official.

Research Methodology Collection Guidelines

This case study employed interviews and surveys to collect responses anonymously from the participants. While JMU had interest in the individuals regarding how their *Kids Guide* could best be integrated and received in Rockingham County middle schools, this study conducted surveys and interviews to better understand the perceived effectiveness of the community-wide collaboration and partnership's effectiveness between higher education and the K-12 community stakeholders. The focus of this case study, then, was on the relationships and what worked well when these separate educational communities, higher education and K-12, united to accomplish a community-wide goal of fulfilling state requirements for cyber safety awareness. Pseudonyms for participants and their associated schools were used in reporting the results of these interviews (see Findings and Analysis, Chapter IV) to ensure the data in this study remains confidential and participant anonymity is retained.

First, re-examination of NCSA-approved Internet safety education and awareness best-practices at the K-12 level (National Cyber Security Alliance, 2002b) was conducted to baseline resources for Internet safety education nationwide to K-12 communities and in particular, middle schools (grades 6 - 8).

Second, a series of surveys was administered to individuals from selected Rockingham County Virginia middle schools was administered to (a) determine perceptions of this collaborative environment in Rockingham County between higher education, K-12 institutions, and the Virginia Department of Education, Office of Educational Technology (see the survey in Appendix B); (b) gain an understanding of the perception of this JMU and K-12 community partnership with the delivery of the *Cyber Citizenship for Kids Guide* (IIIA, 2007) in select Rockingham County and Harrisonburg city middle schools and its overall feasibility for meeting the Virginia commonwealth's requirements for Internet safety (Appendix C). Finally, interviews of the "key stakeholders" in K-12, JMU, and the Virginia Department of Education, Office of Educational Technology were conducted relating to the governance, management, accomplishment of objectives, communications, and outcomes of this community collaborative, and whether this case study is transferable and a "collaborative delivery model" to all of the Commonwealth.

The surveys were administered as follows.

Survey 1 (Appendix B) was used to baseline the perception of the existing collaborative environment, if any, in Rockingham County and Harrisonburg City between higher education and the K-12 community. In addition, the survey was designed to track the current acceptability and role of national cyber safety and other higher education programs and collaboration efforts in the middle school landscape. A number of Rockingham County and Harrisonburg City public middle school teachers, instructional technology resource teachers (ITRT), counselors, resource officers, and school media specialists received the survey via an anonymous third-party survey instrument which was posted to their respective schools' internal websites via Survey Monkey. The URL and link to the survey were delivered to participants from their respective instructional technology supervisor and Director of Technology Services who served as the liaisons for the Rockingham and Harrisonburg City school community with this study and JMU. These third-party survey tools were provided on each school's internal web pages from October 2007 through November 2007 for the prospective respondents to access and complete. A total of 40 respondents participated in this initial survey from Rockingham and Harrisonburg City schools.

Survey 2 (Appendix C), the "follow up survey" was administered approximately one year after the collaboration had started, and helped to delineate the participants' perception of the community partnership between higher education and K-12 schools, its perceived effectiveness, and its overall feasibility in meeting the cyber safety requirements for selected middle schools in Rockingham County and Harrisonburg City. Additionally, participants were asked what aspects of this county-wide partnership effort to enhance cyber safety awareness can serve as a credible model for Virginia commonwealth-wide and/or federal efforts in cyber safety.

This second survey instrument was provided on both schools' websites from December 1, 2007, through January 30, 2008, for the respondents to access and complete anonymously. These two months allowed for JMU to provide its higher education resource on Internet safety (*Kids's Guide*, IIIA, 2007) to the respondents and interact on ways to incorporate this into their classrooms and lesson plans in order to empower the teachers to be well-equipped for meeting the Commonwealth mandate on Internet safety education according to the VA *Guidelines and Resources for Internet Safety in Schools* (VA Department of Education, 2006b). A total of 27 respondents participated in this follow-up survey from Rockingham and Harrisonburg City schools.

A stakeholder questionnaire (Appendix D) was provided via a link to the Survey Monkey website to the two primary contacts the researcher collaborated with during this case study, one liaison each at Rockingham County Public Schools and Harrisonburg City Schools. The purpose was to evaluate whether this community partnership on cyber safety education between higher education and K-12 institutions in Rockingham County and Harrisonburg City schools, as perceived by these two stakeholders, was effective, feasible, and could serve as a credible model for the commonwealth.

Theory

The study's theoretical framework incorporates both the academic and professional fields of education. The framework is diverse and draws from a number of different sources in comparing national educational programs on Internet safety, cyber safety, and cyber ethics, such as electronic and written works, journal articles and professional journals.

This study incorporated qualitative research, which was appropriate for the K-12 educational systems focused on this study, and because the nature of this research was expected to be more subjective than analytical. Qualitatively, this study investigated the best practices of Internet safety-type educational resources that existed at that time and their delivery model for integration into Virginia's middle school system. Therefore, this qualitative method elaborated on whether this JMU higher education and K-12 partnership delivered a perceived successful cyber safety model for middle schools in Rockingham County and Harrisonburg City middle schools.

Research Population

As noted above, a sample of individuals including middle school teachers, instructional technology resource teachers (ITRT), counselors, resource officers, school media specialists, JMU staff, and Virginia Department of Education, Office of Educational Technology staff participated in a combination of surveys and stakeholder interviews to help determine whether this higher education and K-12 community partnership met the perceived objectives of the Rockingham County and Harrisonburg City middle schools intentions on cyber safety awareness—and furthermore, what aspects of this community wide approach could be applied throughout the Commonwealth.

This study's research community specifically included: JMU as the higher education constituent; VA Department of Education, Office of Educational Technology, which is responsible for producing the VA *Resources and Guidelines for Internet Safety in Schools* (VA Department of Education, 2006b) that each school had to comply with by September 2008; and the communities of Rockingham County and Harrisonburg City schools. ITRT professionals are the instructional technology specialists within these schools and serve the entire K-12 school population regarding Internet safety awareness and education. Also included were teachers and administrators from select middle schools in both Rockingham County and Harrisonburg City schools. Initially, when the first (entrance) survey was introduced to the participants online, there were one high school and one pre-kindergarten teacher participating. Their scores were not captured since the focus was middle-school-age students.

Data Collection Methods and Analysis

This case study served as the primary data source. It explored views and perceptions on the effectiveness, or not, of a higher education and K-12 community-based partnership to meet the state-mandated cyber safety awareness needs of the Rockingham County and Harrisonburg City middle schools. The survey instruments provided an overview of educator and administrator experiences with existing national cyber safety educational programs for K-12, other experiences with higher education partnerships in the community, and overall expectations for success and lessons learned from this partnership experience. Follow-up qualitative interviews of key stakeholders with the Virginia Department of Education, Office of Educational Technology; JMU IIIA officers; and technology integrators in Rockingham County and Harrisonburg City middle schools were conducted to determine best practices from this case study and whether or not this community-based partnership approach could be an effective instrument for cyber safety awareness campaigns on the state and federal level.

To protect the identities of individuals participating in this study, they were not required to identify themselves throughout the surveys; however, they were required to complete a Rights of Human Subjects form administered by George Mason University (GMU) who also oversaw this study. All questionnaire respondents, targeted experts, and main field participants also agreed to the consent requirements in accordance with George Mason University's Human Subjects Review Board's research policies and practices prior to their involvement with the study. Therefore, the following specifics applied to the survey phase:

Risk and Benefits of Participation in This Case Study: There are no physical, psychological, social, or medical risks associated with the survey instrument and one’s participation. The potential benefit will be derived “best practices” for higher education and K-12 community collaboration that potentially could be applied to a statewide or federal model.

Compensation: There is no compensation for participation in this study.

Confidentiality: The records of this study will be kept confidential and research records will be stored securely. In any report that JMU or the researcher may publish, no information will be included to make it possible to identify a subject.

Selection of Subjects: Will be up to the direction of the Rockingham County and Harrisonburg City liaisons for their schools.

Voluntary Nature of Study: Participation is wholly voluntary; if subjects decide to participate, they will be free to answer all or none of the required questions and may withdraw at any time from this case study and individuals without affecting their relationship with JMU.

Summary

The research procedures allowed this study to obtain necessary data and information to be effectively utilized in this case study. By allowing the respondents to provide information in a number of different ways (e.g., Survey Monkey surveys and questionnaires, personal and telephone interviews), this study developed a customer-centered approach which allowed this assessment instrument to maintain a high level of integrity with participants. The data was protected in order to ensure candid and truthful responses from the participants.

IV. FINDINGS AND ANALYSIS

Findings

This section details participants' responses to this study's surveys, questionnaires, and interviews.

There were no incentives offered for completing these surveys, questionnaires, or interviews, except for the understanding that their participation could directly benefit the collaboration that was occurring between the middle schools and JMU in producing an Internet safety resource to better the middle school's needs in meeting the state-mandated Internet safety goals.

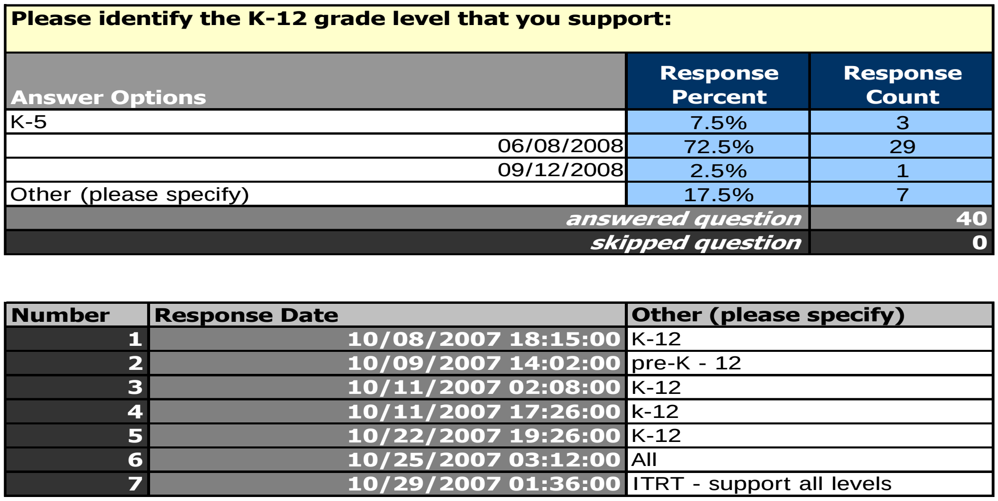
Survey 1: Understanding the Current State of Collaboration

Forty respondents took part in this entry survey, of which 23 completed the entire survey (57.5%), 11 (27.5%) completed part of the survey, and 6 (15%) did not complete it. Of those 40 total respondents, 29 were middle school educators, 1 was a high school educator, 3 were K-5 educators, and 7 were ITRT specialists who supported all levels of education within K-12. The surveys were filled out anonymously via an online third-party software tool, Survey Monkey, and focused on teachers, administrators, and ITRT specialists who supported the middle-school-age student. Reponses collected for those two respondents who supported Pre-K and high school (identified in the "other" column) (Figure 2) were considered minimal and not material to this study as it was targeted at middle school education; therefore, there responses were not considered with the rest of the data.

Question 1: Please Identify the K-12 Grade Level That You Support

As shown in Figure 2, the 40 total respondents in this initial (entry) survey responded as follows:

- 3 respondents supported grades K-5,
- 29 respondents supported grades 6-8,
- 1 respondent supported grades 9-12, and
- 7 respondents supported all grade levels.



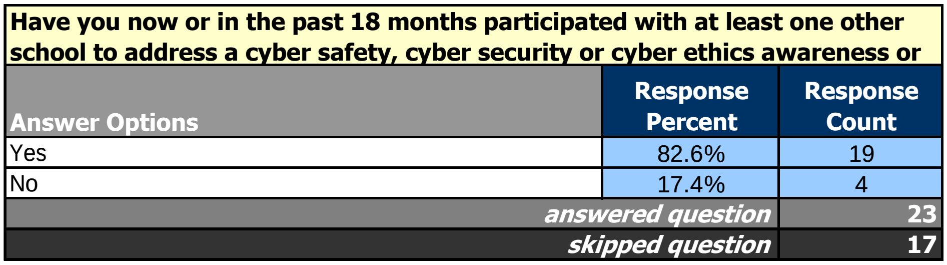
Please identify the K-12 grade level that you support:		
Answer Options	Response Percent	Response Count
K-5	7.5%	3
06/08/2008	72.5%	29
09/12/2008	2.5%	1
Other (please specify)	17.5%	7
answered question		40
skipped question		0

Number	Response Date	Other (please specify)
1	10/08/2007 18:15:00	K-12
2	10/09/2007 14:02:00	pre-K - 12
3	10/11/2007 02:08:00	K-12
4	10/11/2007 17:26:00	k-12
5	10/22/2007 19:26:00	K-12
6	10/25/2007 03:12:00	All
7	10/29/2007 01:36:00	ITRT - support all levels

Figure 2. Initial Survey, Question 1.

Question 2: Have You Now or in the Past 18 Months Participated With at Least One Other School to Address Cyber Safety, Cyber Security, or Cyber Ethics Awareness or Educational Programs – Either Nationally or Locally?

Figure 3 shows that of 23 respondents who answered this question, 19 stated that they had participated in such a program, and 4 respondents had not participated with at least one other school.



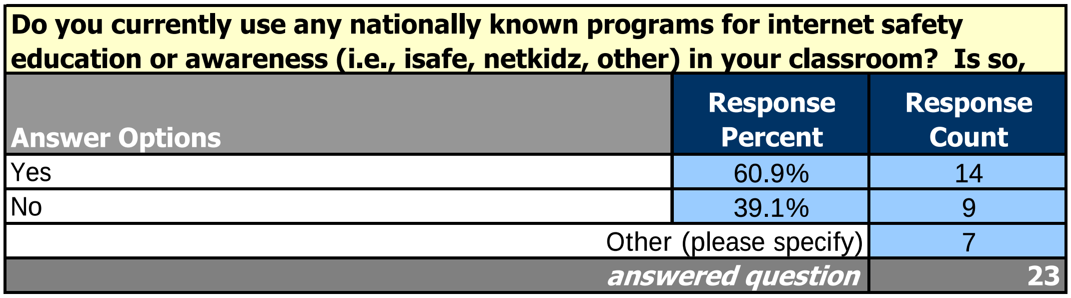
Have you now or in the past 18 months participated with at least one other school to address a cyber safety, cyber security or cyber ethics awareness or

Answer Options	Response Percent	Response Count
Yes	82.6%	19
No	17.4%	4
	answered question	23
	skipped question	17

Figure 3. Initial Survey, Question 2.

Question 3: Do You Currently Use Any Nationally Known Programs for Internet Safety Education or Awareness (i.e., iSafe, Netkidz, Other) in Your Classroom? If So, Why? If Not, Why?

As shown in Figure 4, of the 23 respondents who answered the question,14 stated yes they do use nationally known programs; 9 respondents stated that they do not.



Do you currently use any nationally known programs for internet safety education or awareness (i.e., isafe, netkidz, other) in your classroom? Is so,

Answer Options	Response Percent	Response Count
Yes	60.9%	14
No	39.1%	9
Other (please specify)		7
answered question		**23**

Figure 4. Initial Survey, Question 3.

Of those who specified "other," the responses were as listed in Table 1.

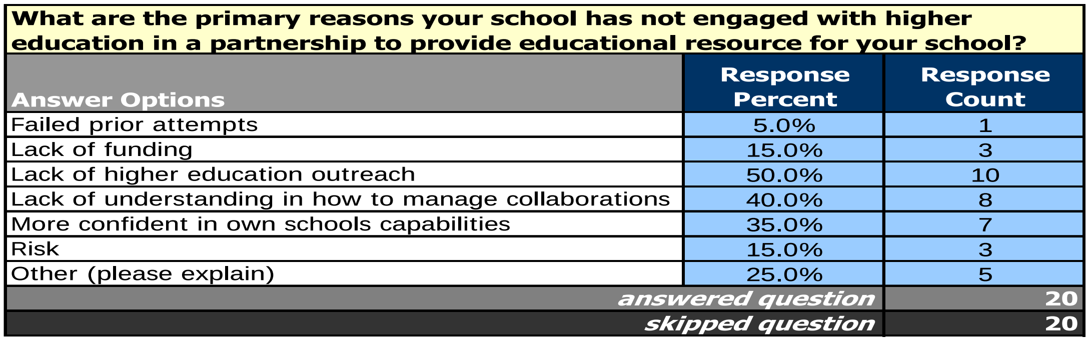
Table 1

Initial Survey, Question 3: Do You Currently Use Any Nationally Known Programs for Internet Safety Education or Awareness (i.e., Isafe, Netkidz, Other) in Your Classroom? Responses in "Other" Category

Number	**Response Date/Time**	**Other (Please Specify)**
1	**10/09/2007 23:02:00**	We just got isafe in our school
2	**10/11/2007 12:30:00**	Have used some sites to help teach Internet safety.
3	**10/11/2007 17:33:00**	we use our own material with the support of other programs
4	**10/12/2007 16:16:00**	I have my own lesson
5	**10/12/2007 17:28:00**	I am an ITRT...have used with some classes.
6	**10/17/2007 17:25:00**	We do not use the internet in my class at this time.
7	**10/25/2007 18:31:00**	Not a "unit" in my class

Question 4: What Are the Primary Reasons Your School Has Not Engaged With Higher Education in a Partnership to Provide Educational Resources to Your School? Please Select as Many as Are Applicable.

As shown in Figure 5, half of the respondents answered this question. One respondent indicated that it was attributable to failed prior attempts; 3 respondents indicated that it was due to lack of funding; 10 respondents indicated that it was due to lack of understanding in how to manage collaborations; 7 respondents indicated that they were more confident in their own school's capabilities; 3 indicated that it was risky. Of the 5 who answered "Other," Table 2 shows 1 stated that they do not use partnerships; 2 stated that it was due to time constraints; 1 stated they did not know because they were new to this environment; and 1 stated that it was due to disinterest on behalf of the university.



What are the primary reasons your school has not engaged with higher education in a partnership to provide educational resource for your school?

Answer Options	Response Percent	Response Count
Failed prior attempts	5.0%	1
Lack of funding	15.0%	3
Lack of higher education outreach	50.0%	10
Lack of understanding in how to manage collaborations	40.0%	8
More confident in own schools capabilities	35.0%	7
Risk	15.0%	3
Other (please explain)	25.0%	5
	answered question	20
	skipped question	20

Figure 5. Initial Survey, Question 4.

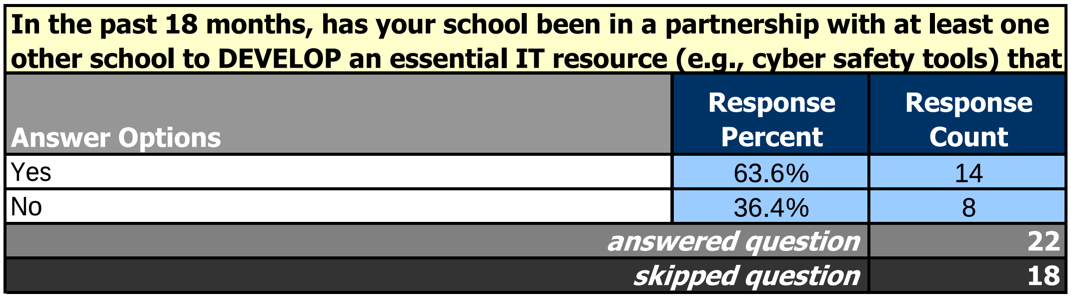
Table 2

Initial Survey, Question 5: What Are the Primary Reasons Your School Has Not Engaged With Higher Education in a Partnership to Provide Educational Resources to Your School? Responses in "Other" Category

Number	Response Date	Other (please explain)
1	10/10/2007 12:43:00	WE DO USE partnerships
2	10/12/2007 17:22:00	time
3	10/12/2007 17:24:00	lack of time
4	10/17/2007 17:25:00	Do not know...this is my first year at this school.
5	10/25/2007 03:20:00	disinterest on the part of the university

Question 5: In the Past 18 Months, Has Your School Been in a Partnership With at Least One Other School to DEVELOP an Essential IT Resource (e.g. Cyber Safety Tools) That Involved Sharing Risk, Resources, and/or Management Control?

Figure 6 shows that of the 22 respondents who answered the question, 14 stated yes; 8 respondents stated no. Eighteen respondents did not complete the question.



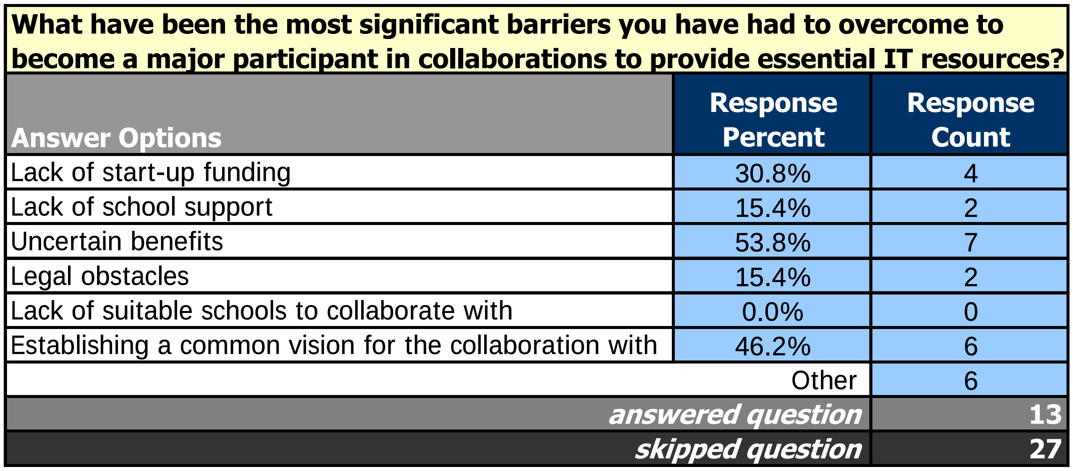
In the past 18 months, has your school been in a partnership with at least one other school to DEVELOP an essential IT resource (e.g., cyber safety tools) that

Answer Options	Response Percent	Response Count
Yes	63.6%	14
No	36.4%	8
	answered question	22
	skipped question	18

Figure 6. Initial Survey, Question 5.

Question 6: What Have Been the Most Significant Barriers You Have Had to Overcome to Become a Major Participant in Collaboration to Provide Essential IT Resources? Select as Many as Apply.

As shown in Figure 7, of the 13 respondents who answered the question, 4 indicated lack of start up funding; 2 respondents indicated lack of school support; 7 respondents indicated they were uncertain of the benefits; 2 respondents indicated legal obstacles; 6 respondents indicated "establishing a common vision for the collaboration with other participating schools." Of the 6 who answered "Other," Table 3 reveals that 4 respondents stated they had no time; 1 respondent stated they had no knowledge of the program; and 1 respondent did not know. 27 respondents did not answer this question.



What have been the most significant barriers you have had to overcome to become a major participant in collaborations to provide essential IT resources?

Answer Options	Response Percent	Response Count
Lack of start-up funding	30.8%	4
Lack of school support	15.4%	2
Uncertain benefits	53.8%	7
Legal obstacles	15.4%	2
Lack of suitable schools to collaborate with	0.0%	0
Establishing a common vision for the collaboration with	46.2%	6
	Other	6
	answered question	13
	skipped question	27

Figure 7. Initial Survey, Question 6.

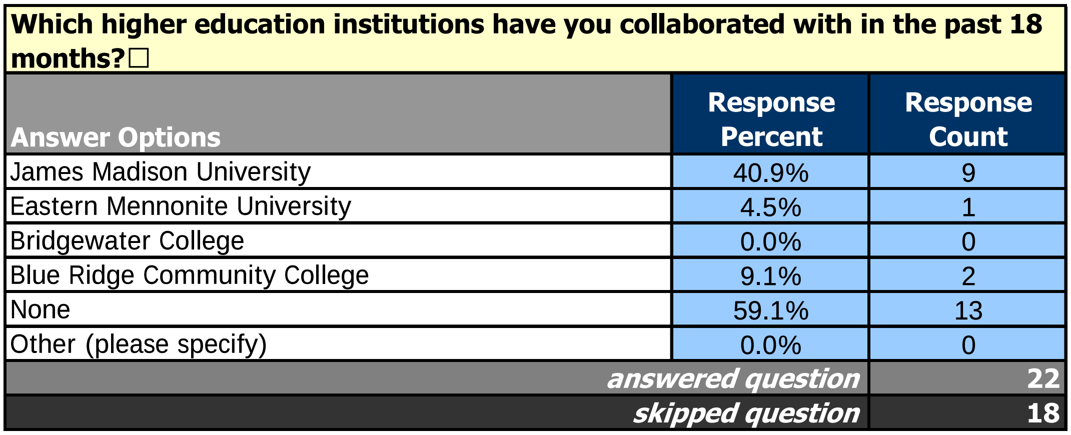
Table 3

Initial Survey, Question 6: What Have Been the Most Significant Barriers You Have Had to Overcome to Become a Major Participant in Collaboration to Provide Essential IT Resources? Responses in "Other" Category

Number	Response Date	Other
1	10/09/2007 13:42:00	understaffed and overworked- TIME!
2	10/09/2007 23:02:00	Not enough time in the school day
3	10/11/2007 12:30:00	Had no knowledge of the program
4	10/12/2007 17:22:00	time
5	10/15/2007 14:25:00	time
6	10/17/2007 17:25:00	unknown... does not pertain

Question 7: Which Higher Education Institutions Have You Collaborated With in the Past 18 Months?

Figure 8 reveals that of the 22 respondents who answered the question, 9 indicated James Madison University; 1 indicated Eastern Mennonite University; 2 indicated Blue Ridge Community College; 13 indicated “none” and 18 respondents did not answer this question.

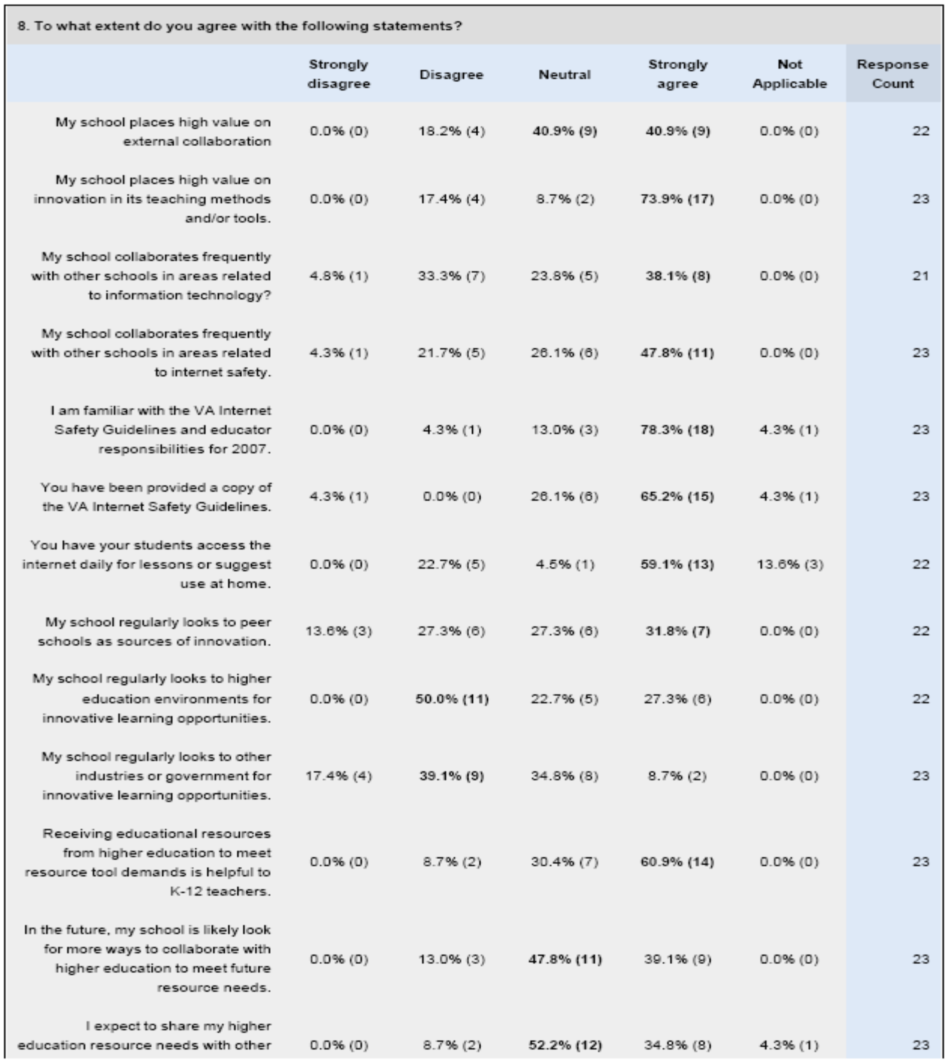


Which higher education institutions have you collaborated with in the past 18 months?□		
Answer Options	Response Percent	Response Count
James Madison University	40.9%	9
Eastern Mennonite University	4.5%	1
Bridgewater College	0.0%	0
Blue Ridge Community College	9.1%	2
None	59.1%	13
Other (please specify)	0.0%	0
answered question		22
skipped question		18

Figure 8. Initial Survey, Question 7.

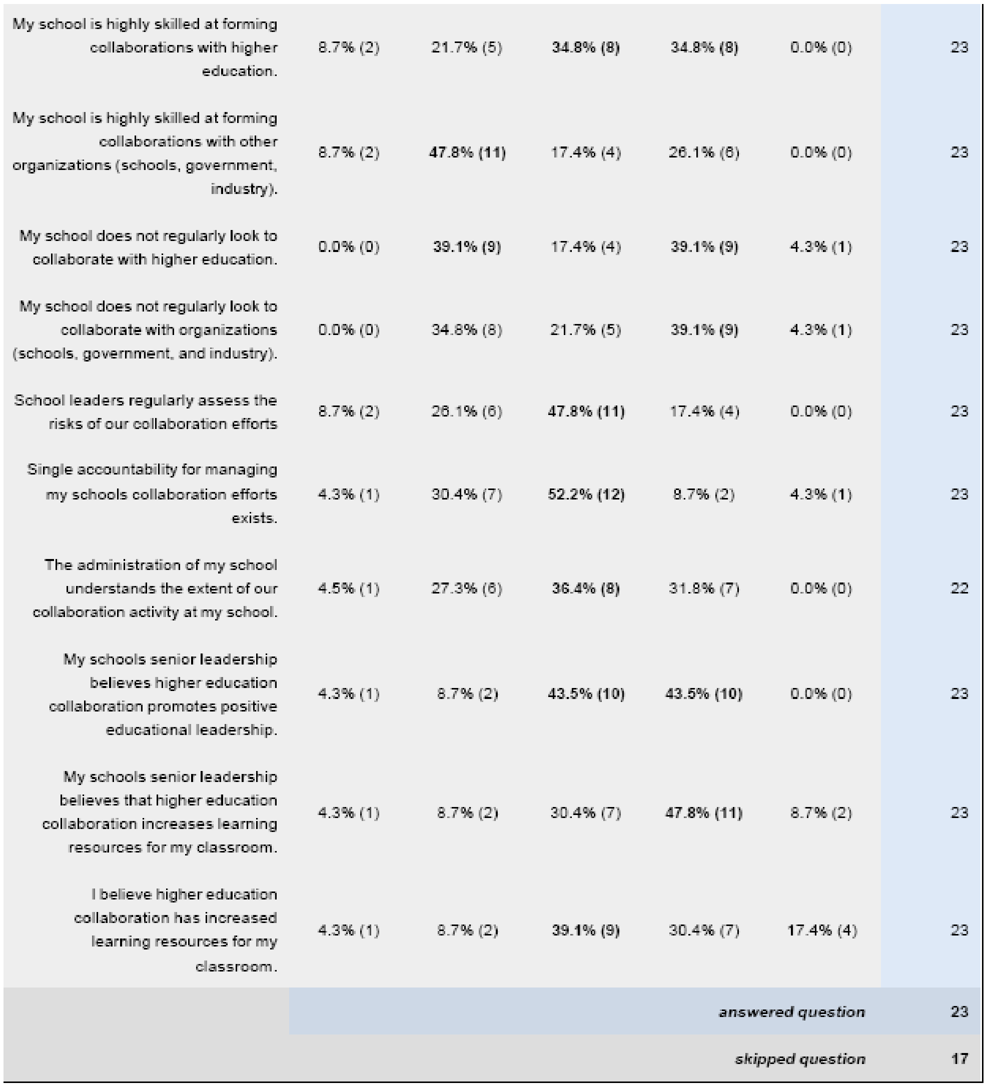
Question 8: To What Extent Do You Agree With the Following Statements?

Figure 9 best depicts the respondents' level of agreement or not. Of the 23 respondents who answered the question, 73.9% strongly agreed that their school places high value on innovation in teaching methods and/or tools; and 50% disagreed that their school regularly looks to higher education environments for innovative learning opportunities.



8. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
My school places high value on external collaboration	0.0% (0)	18.2% (4)	**40.9% (9)**	**40.9% (9)**	0.0% (0)	22
My school places high value on innovation in its teaching methods and/or tools.	0.0% (0)	17.4% (4)	8.7% (2)	**73.9% (17)**	0.0% (0)	23
My school collaborates frequently with other schools in areas related to information technology?	4.8% (1)	33.3% (7)	23.8% (5)	**38.1% (8)**	0.0% (0)	21
My school collaborates frequently with other schools in areas related to internet safety.	4.3% (1)	21.7% (5)	26.1% (6)	**47.8% (11)**	0.0% (0)	23
I am familiar with the VA Internet Safety Guidelines and educator responsibilities for 2007.	0.0% (0)	4.3% (1)	13.0% (3)	**78.3% (18)**	4.3% (1)	23
You have been provided a copy of the VA Internet Safety Guidelines.	4.3% (1)	0.0% (0)	26.1% (6)	**65.2% (15)**	4.3% (1)	23
You have your students access the internet daily for lessons or suggest use at home.	0.0% (0)	22.7% (5)	4.5% (1)	**59.1% (13)**	13.6% (3)	22
My school regularly looks to peer schools as sources of innovation.	13.6% (3)	27.3% (6)	27.3% (6)	**31.8% (7)**	0.0% (0)	22
My school regularly looks to higher education environments for innovative learning opportunities.	0.0% (0)	**50.0% (11)**	22.7% (5)	27.3% (6)	0.0% (0)	22
My school regularly looks to other industries or government for innovative learning opportunities.	17.4% (4)	**39.1% (9)**	34.8% (8)	8.7% (2)	0.0% (0)	23
Receiving educational resources from higher education to meet resource tool demands is helpful to K-12 teachers.	0.0% (0)	8.7% (2)	30.4% (7)	**60.9% (14)**	0.0% (0)	23
In the future, my school is likely look for more ways to collaborate with higher education to meet future resource needs.	0.0% (0)	13.0% (3)	**47.8% (11)**	39.1% (9)	0.0% (0)	23
I expect to share my higher education resource needs with other	0.0% (0)	8.7% (2)	**52.2% (12)**	34.8% (8)	4.3% (1)	23



My school is highly skilled at forming collaborations with higher education.	8.7% (2)	21.7% (5)	**34.8% (8)**	**34.8% (8)**	0.0% (0)	23
My school is highly skilled at forming collaborations with other organizations (schools, government, industry).	8.7% (2)	**47.8% (11)**	17.4% (4)	26.1% (6)	0.0% (0)	23
My school does not regularly look to collaborate with higher education.	0.0% (0)	**39.1% (9)**	17.4% (4)	**39.1% (9)**	4.3% (1)	23
My school does not regularly look to collaborate with organizations (schools, government, and industry).	0.0% (0)	34.8% (8)	21.7% (5)	**39.1% (9)**	4.3% (1)	23
School leaders regularly assess the risks of our collaboration efforts	8.7% (2)	26.1% (6)	**47.8% (11)**	17.4% (4)	0.0% (0)	23
Single accountability for managing my schools collaboration efforts exists.	4.3% (1)	30.4% (7)	**52.2% (12)**	8.7% (2)	4.3% (1)	23
The administration of my school understands the extent of our collaboration activity at my school.	4.5% (1)	27.3% (6)	**36.4% (8)**	31.8% (7)	0.0% (0)	22
My schools senior leadership believes higher education collaboration promotes positive educational leadership.	4.3% (1)	8.7% (2)	**43.5% (10)**	**43.5% (10)**	0.0% (0)	23
My schools senior leadership believes that higher education collaboration increases learning resources for my classroom.	4.3% (1)	8.7% (2)	30.4% (7)	**47.8% (11)**	8.7% (2)	23
I believe higher education collaboration has increased learning resources for my classroom.	4.3% (1)	8.7% (2)	**39.1% (9)**	30.4% (7)	17.4% (4)	23
					answered question	23
					skipped question	**17**

Figure 9. Initial Survey, Question 8.

Question 9: What is the Major Reason Your School has Elected to Collaborate With Higher Education to Provide Internet/Cyber Safety Resources to Students?

Table 4 reveals that the 17 respondents who provided feedback provided a mix of varying responses as to why they thought their school was participating with JMU. There was no defining collective response. In addition, 23 respondents did not answer this question.

Table 4

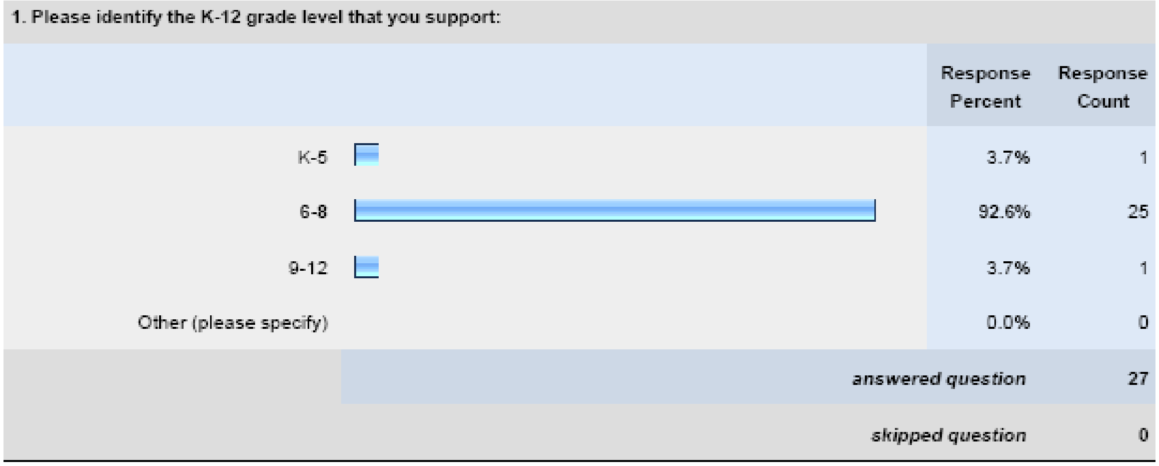
Initial Survey, Question 9: What is the Major Reason Your School has Elected to Collaborate With Higher Education to Profice Internet/Cyber Safety Resources to Students?

Number	Response Date	Response Text
1	10/09/2007 13:42:00	I have no idea
2	10/09/2007 15:41:00	law
3	10/09/2007 23:02:00	To stay current with the changing technologies
4	10/10/2007 12:43:00	it is an important issue
5	10/10/2007 17:09:00	Closeness of higher learning facilities
6	10/11/2007 17:33:00	I don't know that "my school" has.
7	10/12/2007 16:16:00	to educate them on safety issues
8	10/12/2007 17:22:00	when the opportunity is provided, it is easier to accept, then to initiate
9	10/12/2007 17:24:00	lack of time
10	10/12/2007 17:28:00	This is a new area that we are trying to provide resources for staff, students, and parents and we are looking at all possible resources.
11	10/12/2007 17:38:00	more resources
12	10/15/2007 14:25:00	not applicable
13	10/17/2007 17:25:00	To keep students safe while using the Internet and to stay on top of current trends in Cyber-Issues.
14	10/18/2007 17:46:00	neutral
15	10/22/2007 12:35:00	We learn from each other
16	10/25/2007 03:20:00	N/A
17	10/25/2007 18:31:00	I don't know if it has

Survey 2: Understanding the Affect of Higher Education Interaction

Question 1: Please Identify the K-12 Grade Level That You Support

As shown in Figure 10, 1 respondent was from grades K-5; 25 respondents supported grades 6-8; and 1 respondent supported grades 9-12. As noted above, the responses for the 2 who identified themselves as supporting Pre-K and high school were considered minimal and not material to this study as it was targeted at middle school education; therefore, their responses were not considered with the rest of the data.



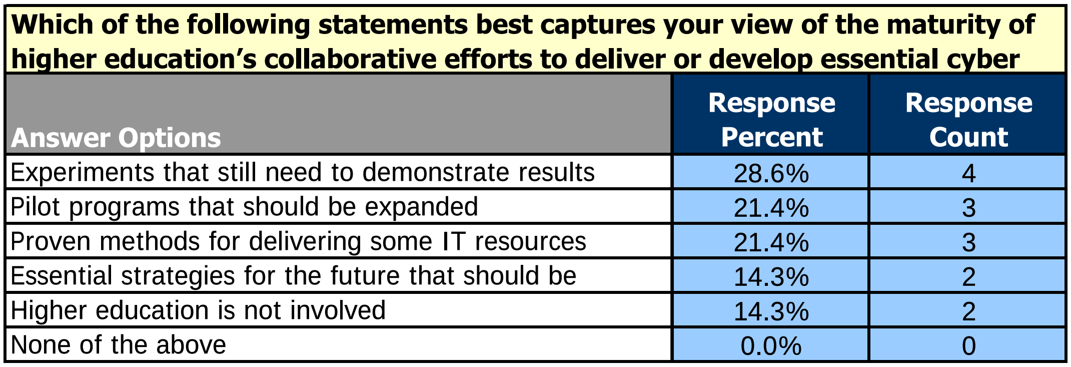
1. Please identify the K-12 grade level that you support:

	Response Percent	Response Count
K-5	3.7%	1
6-8	92.6%	25
9-12	3.7%	1
Other (please specify)	0.0%	0
answered question		27
skipped question		0

Figure 10. Survey 2, Question 1.

Question 2. Which of the Following Statements Best Captures Your View of the Maturity of Higher Education's Collaborative Efforts to Deliver or Develop Essential Cyber Safety Learning Resources for K-12?

Figure 11 reveals 4 respondents indicated that experiments still need to demonstrate results; 3 respondents indicated that collaboration pilot programs should be expanded; 3 respondents indicated that collaboration can be a proven method for delivering some IT resources; 2 respondents indicated that essential strategies for the future that should be implemented; 2 more respondents indicated that higher education is not involved in collaboration to develop essential cyber safety learning resources for K-12. Thirteen respondents did not answer this question.



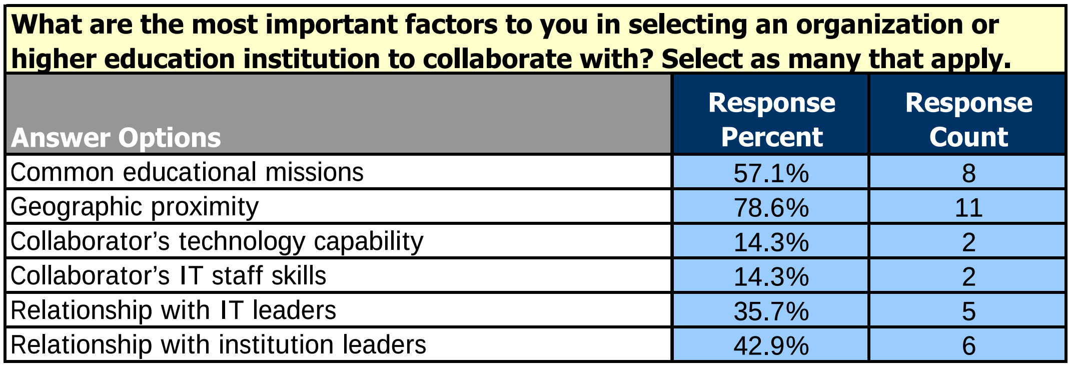
Which of the following statements best captures your view of the maturity of higher education's collaborative efforts to deliver or develop essential cyber

Answer Options	Response Percent	Response Count
Experiments that still need to demonstrate results	28.6%	4
Pilot programs that should be expanded	21.4%	3
Proven methods for delivering some IT resources	21.4%	3
Essential strategies for the future that should be	14.3%	2
Higher education is not involved	14.3%	2
None of the above	0.0%	0

Figure 11. Survey 2, Question 2.

Question 3: What Are the Most Important Factors to You in Selecting an Organization or Higher Education Institution to Collaborate With? Please Select as Many as Apply.

As shown in Figure 12, 8 responses were tallied for “common education missions”; 11 responses were collected for “geographic proximity”; 2 responses each for “collaborator’s technology capability and IT staff skills”; 5 responses for “relationship with IT leaders”; 6 for “relationship with institution leaders”; 10 respondents selected “common objectives for the collaboration” and 3 respondents selected “collaborator’s willingness to share risk.”



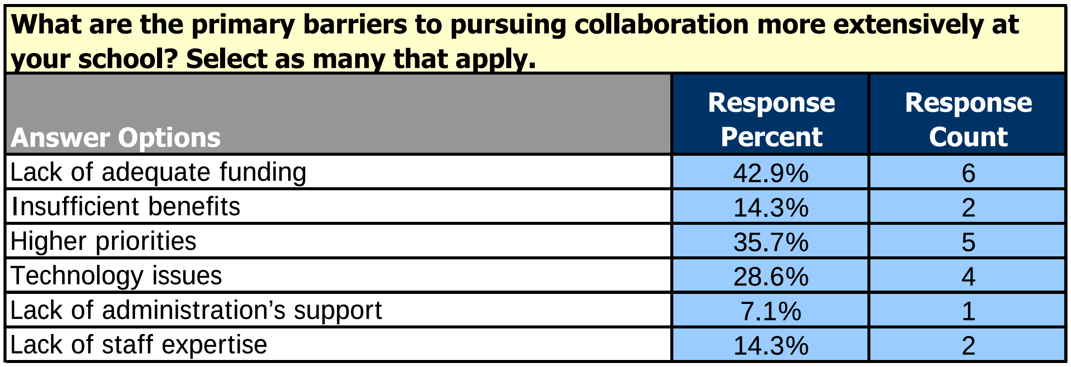
What are the most important factors to you in selecting an organization or higher education institution to collaborate with? Select as many that apply.

Answer Options	Response Percent	Response Count
Common educational missions	57.1%	8
Geographic proximity	78.6%	11
Collaborator’s technology capability	14.3%	2
Collaborator’s IT staff skills	14.3%	2
Relationship with IT leaders	35.7%	5
Relationship with institution leaders	42.9%	6

Figure 12. Survey 2, Question 3.

Question 4: What Are the Primary Barriers to Pursuing Collaboration More Extensively at Your School? Select as Many as Apply.

As depicted in Figure 13, 6 respondents indicated “lack of funding”; 2 indicated “perception of insufficient benefits”; 5 selected “other higher priorities”; 4 indicated “technology issues existed”; 1 respondent indicated “lack of administration’s support”; 2 indicated “lack of staff expertise.” Table 5 shows that of those who selected “Other,” 2 selected “lack of alignment with school’s priorities”; and 4 respondents stated they had no “extra time” and “other responsibilities.”



What are the primary barriers to pursuing collaboration more extensively at your school? Select as many that apply.

Answer Options	Response Percent	Response Count
Lack of adequate funding	42.9%	6
Insufficient benefits	14.3%	2
Higher priorities	35.7%	5
Technology issues	28.6%	4
Lack of administration’s support	7.1%	1
Lack of staff expertise	14.3%	2

Figure 13. Survey 2, Question 4.

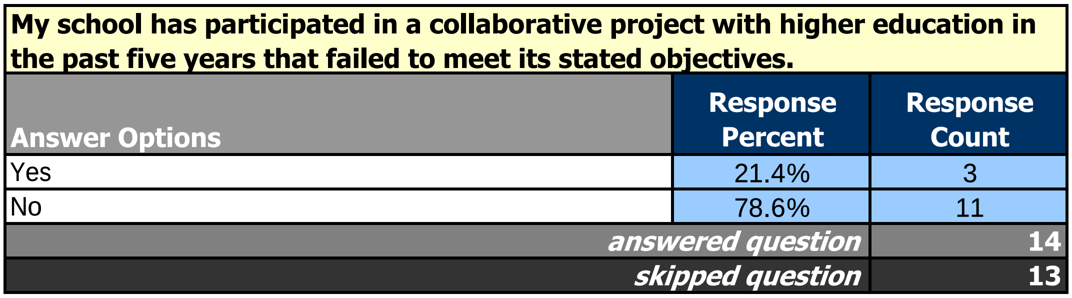
Table 5

Survey 2, Question 4: What Are the Primary Barriers to Pursuing Collaboration More Extensively at Your School? Responses in “Other” Category

Number	Response Date	Other (please specify)
1	12/10/2007 17:24:00	lack of time to initiate and follow through
2	12/12/2007 20:12:00	time, effort involved
3	12/29/2007 17:30:00	Time
4	01/03/2008 17:48:00	too many other responsibilities (AYP, NCLB, VLGA, IEP), etc...

Question 5: My School has Participated in a Collaborative Project With Higher Education in the Past Five Years That Failed to Meet its Stated Objectives.

Figure 14 shows that 3 respondents indicated “yes” to this question and 11 indicated “no.” Thirteen respondents did not answer this question.

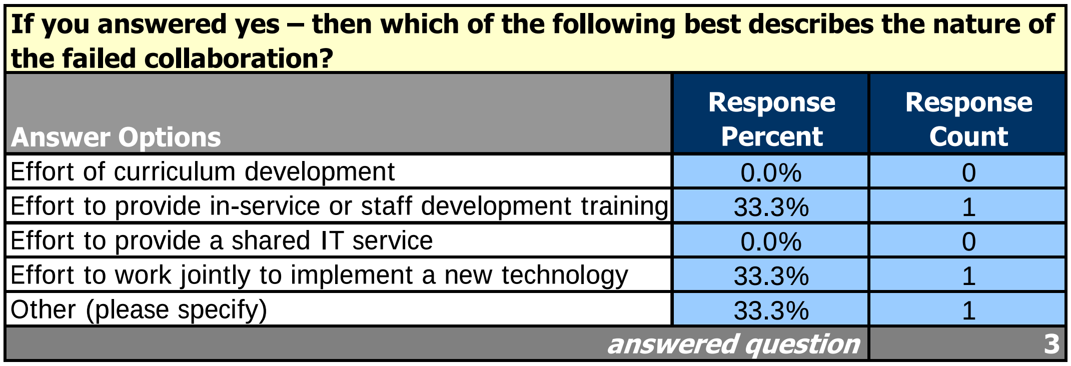


My school has participated in a collaborative project with higher education in the past five years that failed to meet its stated objectives.		
Answer Options	Response Percent	Response Count
Yes	21.4%	3
No	78.6%	11
	answered question	14
	skipped question	13

Figure 14. Survey 2, Question 5.

Question 6: If You Answered “Yes” to Question 5 Then Which of the Following Situations Best Describes the Nature of the Failed Collaboration?

As noted in Figure 15, the 3 respondents who answered “yes” to Question 5 selected the following failed situations: “effort to provide in-service or staff development training”; “effort to work jointly to implement a new technology” and “Other.” Table 6 shows the “Other” response was detailed as “tutors.”

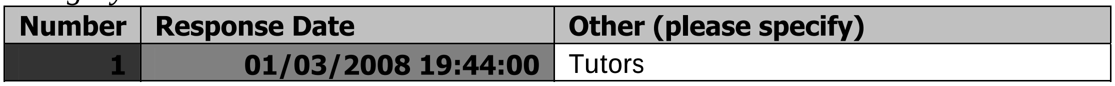


If you answered yes – then which of the following best describes the nature of the failed collaboration?		
Answer Options	**Response Percent**	**Response Count**
Effort of curriculum development	0.0%	0
Effort to provide in-service or staff development training	33.3%	1
Effort to provide a shared IT service	0.0%	0
Effort to work jointly to implement a new technology	33.3%	1
Other (please specify)	33.3%	1
	answered question	**3**

Figure 15. Survey 2, Question 6.

Table 6

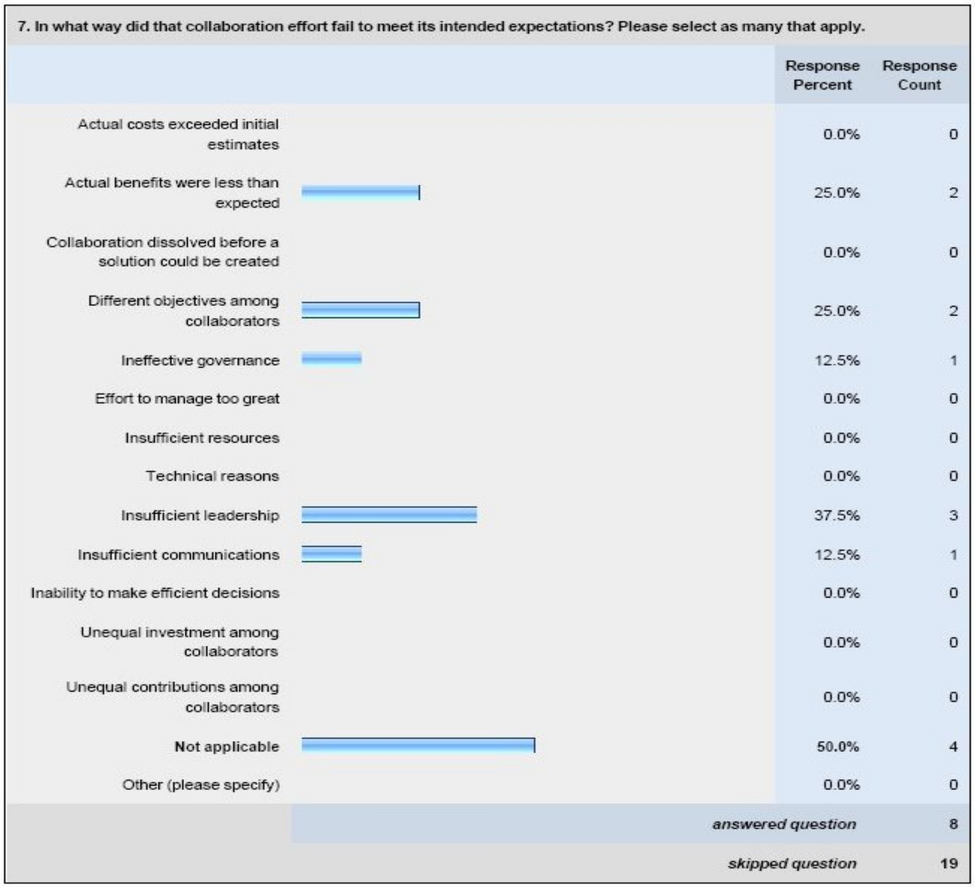
Survey 2, Question 6: If You Answered “Yes” to Question 5 Then Which of the Following Situations Best Describes the Nature of the Failed Collaboration? Reponses to “Other” Category



Number	**Response Date**	**Other (please specify)**
1	**01/03/2008 19:44:00**	Tutors

Question 7: In What Way Did That Collaboration Effort Fail to Meet Its Intended Expectations? Please Select as Many as Apply.

Figure 16 reveals that 2 responses indicated that “actual benefits were less than expected”; 2 responses indicated “different objectives among collaborators”; 1 response indicated “ineffective governance”; 3 responses identified “ineffective leadership”; 1 response indicated “ineffective communications”; and 4 respondents chose “not applicable.” Nineteen respondents did not answer this question.



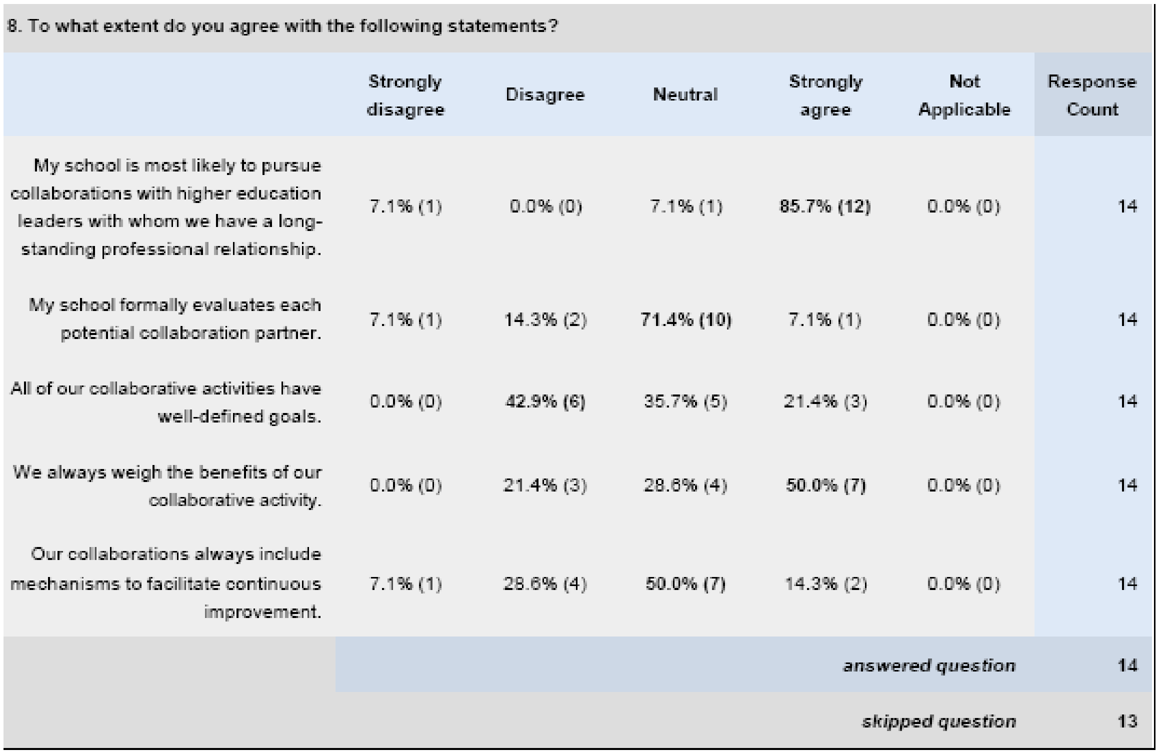
7. In what way did that collaboration effort fail to meet its intended expectations? Please select as many that apply.

	Response Percent	Response Count
Actual costs exceeded initial estimates	0.0%	0
Actual benefits were less than expected	25.0%	2
Collaboration dissolved before a solution could be created	0.0%	0
Different objectives among collaborators	25.0%	2
Ineffective governance	12.5%	1
Effort to manage too great	0.0%	0
Insufficient resources	0.0%	0
Technical reasons	0.0%	0
Insufficient leadership	37.5%	3
Insufficient communications	12.5%	1
Inability to make efficient decisions	0.0%	0
Unequal investment among collaborators	0.0%	0
Unequal contributions among collaborators	0.0%	0
Not applicable	50.0%	4
Other (please specify)	0.0%	0
	answered question	8
	skipped question	19

Figure 16. Survey 2, Question 7.

Question 8: To What Extent Do You Agree With the Following Statements?

Figure 17 encapsulates the respondent's level of agreement or disagreement with the applicable question as posed. Of the respondents, 85.7% strongly agreed that they would pursue collaborations with higher education leaders with whom they had a longstanding relationship. There was 42.9% percent disagreement that all collaboration activities had well-defined goals. Thirteen respondents did not answer this question.



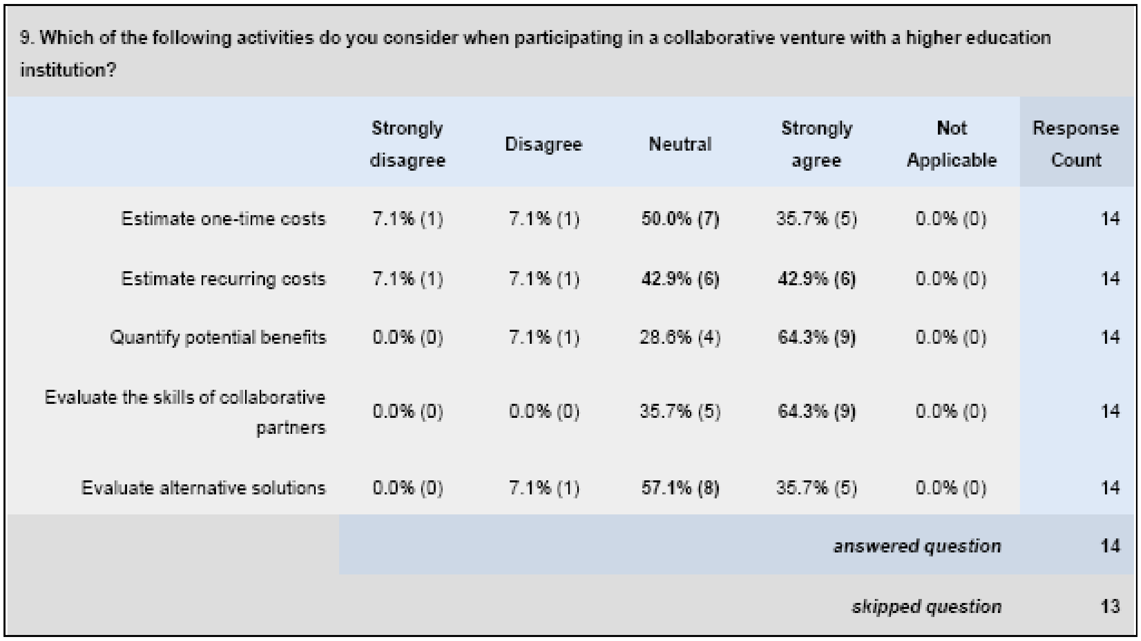
8. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
My school is most likely to pursue collaborations with higher education leaders with whom we have a long-standing professional relationship.	7.1% (1)	0.0% (0)	7.1% (1)	**85.7% (12)**	0.0% (0)	14
My school formally evaluates each potential collaboration partner.	7.1% (1)	14.3% (2)	**71.4% (10)**	7.1% (1)	0.0% (0)	14
All of our collaborative activities have well-defined goals.	0.0% (0)	**42.9% (6)**	35.7% (5)	21.4% (3)	0.0% (0)	14
We always weigh the benefits of our collaborative activity.	0.0% (0)	21.4% (3)	28.6% (4)	**50.0% (7)**	0.0% (0)	14
Our collaborations always include mechanisms to facilitate continuous improvement.	7.1% (1)	28.6% (4)	**50.0% (7)**	14.3% (2)	0.0% (0)	14
					answered question	14
					skipped question	13

Figure 17. Survey 2, Question 8.

Question 9: Which of the Following Activities Do You Consider When Participating in a Collaborative Venture With a Higher Education Institution?

Figure 18 encapsulates the respondent's level of agreement or disagreement with the applicable question as posed. There was strong agreement among participants that when entering into a collaborative venture with higher education, 64.3% stated that they would quantify potential benefits and similarly evaluate the skills of collaborative partners. Thirteen respondents did not answer this question.



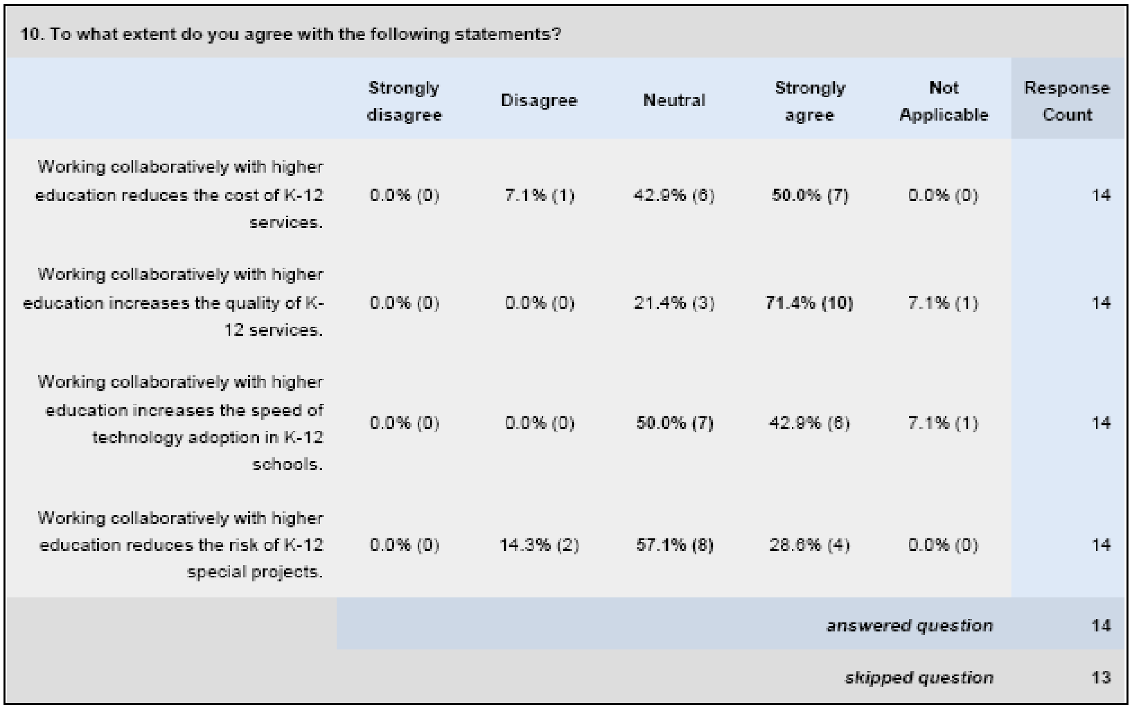
9. Which of the following activities do you consider when participating in a collaborative venture with a higher education institution?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
Estimate one-time costs	7.1% (1)	7.1% (1)	50.0% (7)	35.7% (5)	0.0% (0)	14
Estimate recurring costs	7.1% (1)	7.1% (1)	42.9% (6)	42.9% (6)	0.0% (0)	14
Quantify potential benefits	0.0% (0)	7.1% (1)	28.6% (4)	64.3% (9)	0.0% (0)	14
Evaluate the skills of collaborative partners	0.0% (0)	0.0% (0)	35.7% (5)	64.3% (9)	0.0% (0)	14
Evaluate alternative solutions	0.0% (0)	7.1% (1)	57.1% (8)	35.7% (5)	0.0% (0)	14
					answered question	14
					skipped question	13

Figure 18. Survey 2, Question 9.

Question 10: To What Extent Do You Agree With the Following Statements?

Figure 19 encapsulates the respondent’s level of agreement or disagreement with the applicable question as posed. Respondents indicated strong agreement about working collaboratively with higher education: 50% stated that it reduces the cost of K-12 services; 71.4% stated that it increases the quality of K-12 services. Thirteen respondents did not answer this question.



10. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
Working collaboratively with higher education reduces the cost of K-12 services.	0.0% (0)	7.1% (1)	42.9% (6)	**50.0% (7)**	0.0% (0)	14
Working collaboratively with higher education increases the quality of K-12 services.	0.0% (0)	0.0% (0)	21.4% (3)	**71.4% (10)**	7.1% (1)	14
Working collaboratively with higher education increases the speed of technology adoption in K-12 schools.	0.0% (0)	0.0% (0)	**50.0% (7)**	42.9% (6)	7.1% (1)	14
Working collaboratively with higher education reduces the risk of K-12 special projects.	0.0% (0)	14.3% (2)	**57.1% (8)**	28.6% (4)	0.0% (0)	14
					answered question	14
					skipped question	13

Figure 19. Survey 2, Question 10.

Stakeholder Questionnaire

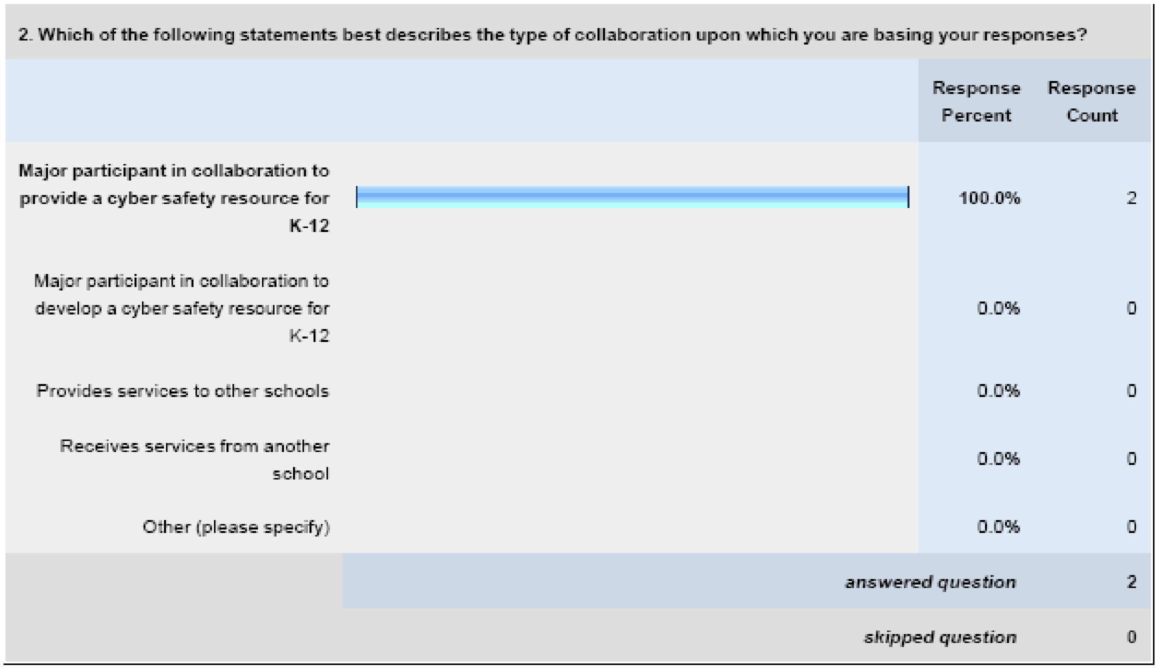
This stakeholder questionnaire was administered to the two major liaisons, one each representing Rockingham County and Harrisonburg City schools, with whom this researcher interacted throughout the case study. Based upon their level of authority and oversight for their school districts, the sample was not projected to be larger than these two participants. Responses were anonymous.

Question 1: Please Identify the K-12 Grade Level You Support

Both respondents supported all K-12 grades as ITRT professionals.

Question 2: Which of the Following Statements Best Describes the Type of Collaboration Upon Which You Are Basing Your Responses?

Figure 20 shows that both liaisons, one for each institution, participated in this "wrap-up" questionnaire.



2. Which of the following statements best describes the type of collaboration upon which you are basing your responses?

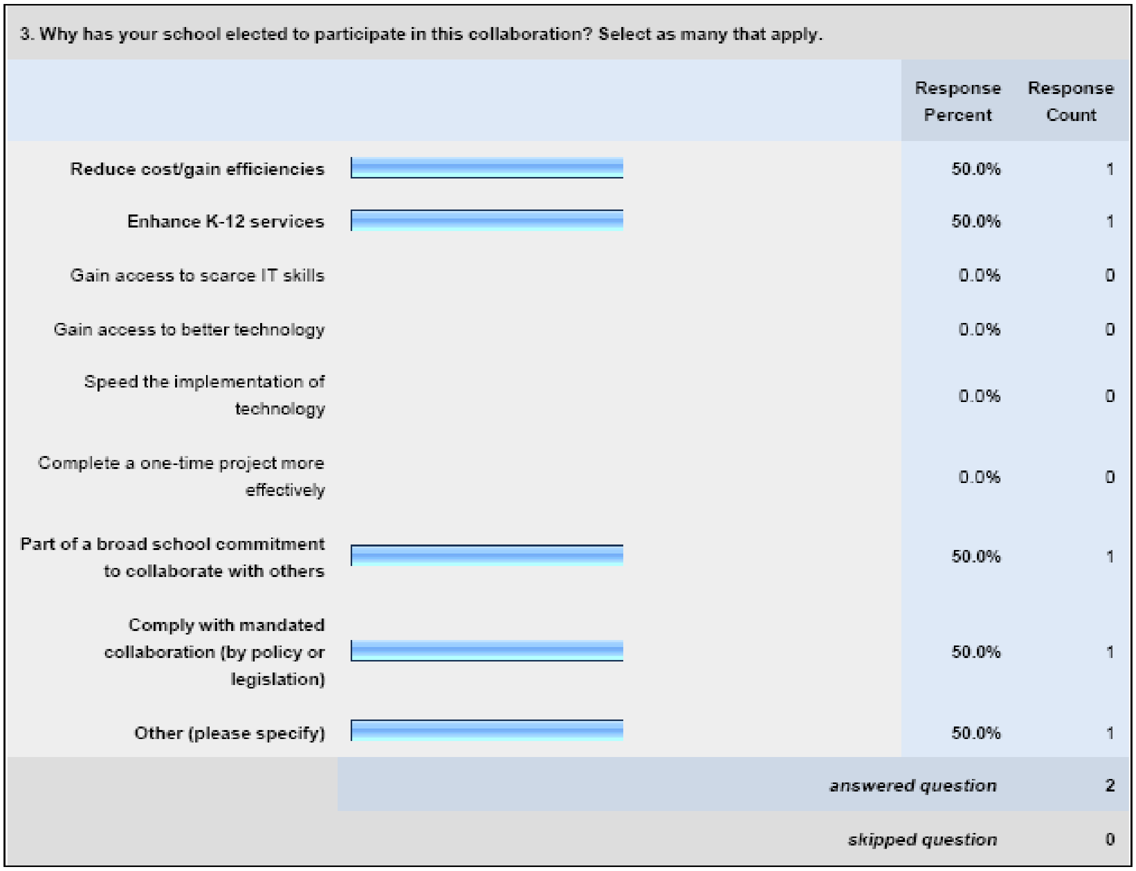
	Response Percent	Response Count
Major participant in collaboration to provide a cyber safety resource for K-12	100.0%	2
Major participant in collaboration to develop a cyber safety resource for K-12	0.0%	0
Provides services to other schools	0.0%	0
Receives services from another school	0.0%	0
Other (please specify)	0.0%	0
	answered question	2
	skipped question	0

Figure 20. Stakeholder Questionnaire Question 2.

Question 3: Why Has Your School Elected to Participate in This Collaboration? Select as Many as Apply.

As shown in Figure 21, both respondents selected the following once:

- Reduce cost/gain efficiencies
- Enhance K-12 services
- Part of a broad school commitment to collaborate with others
- Comply with mandated collaboration (by policy or legislation)
- Gain access to resources.



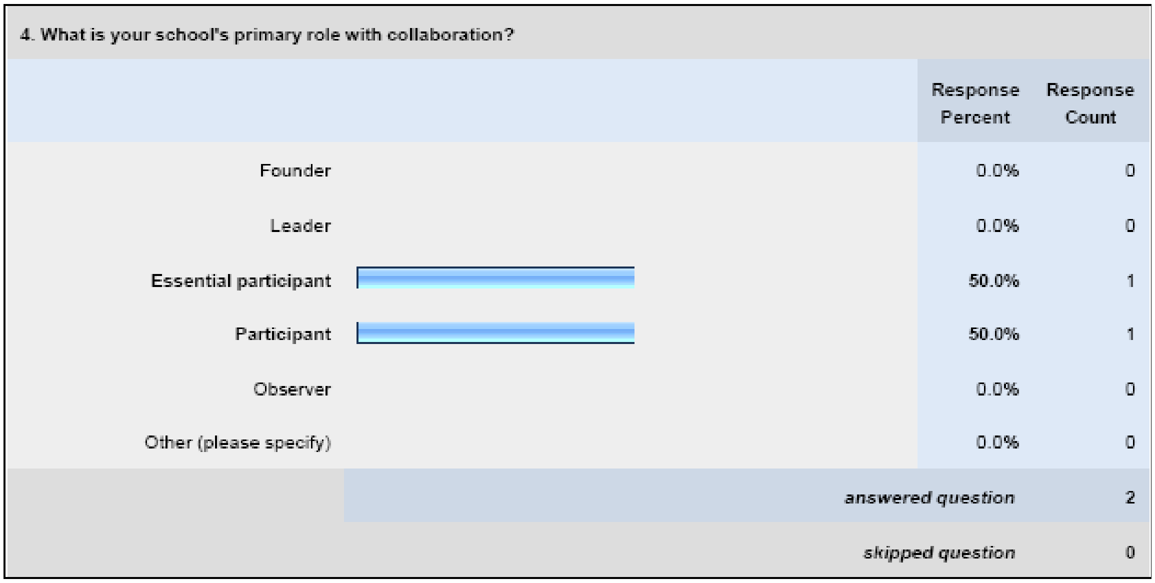
3. Why has your school elected to participate in this collaboration? Select as many that apply.

	Response Percent	Response Count
Reduce cost/gain efficiencies	50.0%	1
Enhance K-12 services	50.0%	1
Gain access to scarce IT skills	0.0%	0
Gain access to better technology	0.0%	0
Speed the implementation of technology	0.0%	0
Complete a one-time project more effectively	0.0%	0
Part of a broad school commitment to collaborate with others	50.0%	1
Comply with mandated collaboration (by policy or legislation)	50.0%	1
Other (please specify)	50.0%	1
	answered question	2
	skipped question	0

Figure 21. Stakeholder Questionnaire Question 3.

Question 4: What Is Your School’s Primary Role With Collaboration?

As Figure 22 shows, each participant selected either “participant” or “essential participant.”



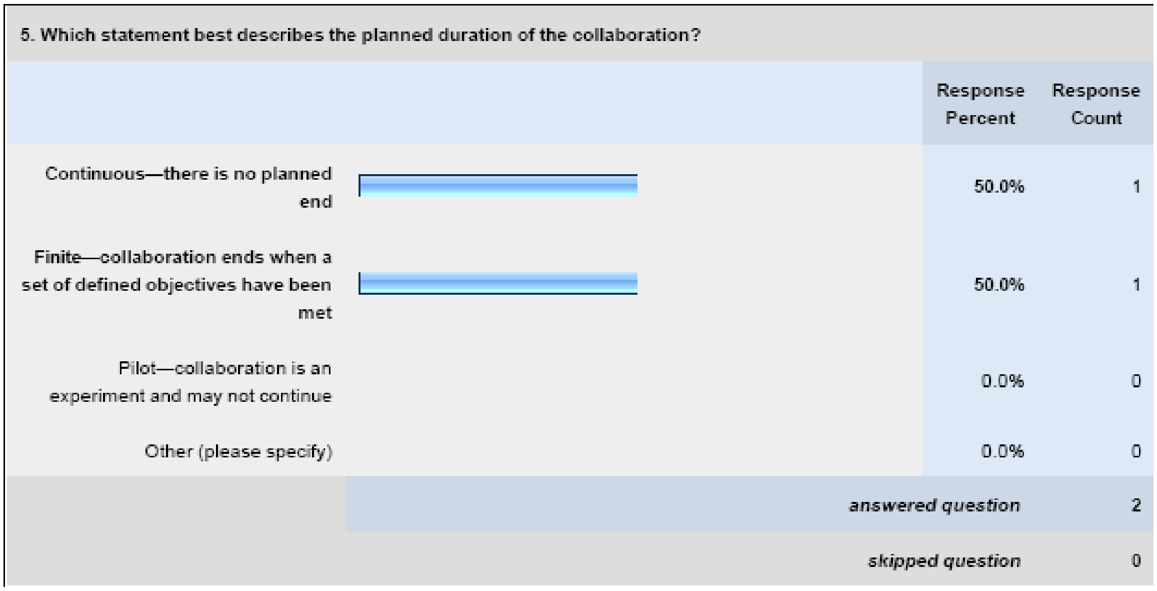
4. What is your school's primary role with collaboration?

	Response Percent	Response Count
Founder	0.0%	0
Leader	0.0%	0
Essential participant	50.0%	1
Participant	50.0%	1
Observer	0.0%	0
Other (please specify)	0.0%	0
	answered question	2
	skipped question	0

Figure 22. Stakeholder Questionnaire Question 4.

Question 5: Which Statement Best Describes the Planned Duration of the Collaboration?

Figure 23 reveals 1 participant indicated “continuous – there is no planned end”; the other participant indicated “finite – collaboration ends when a set of defined objectives has been met.”



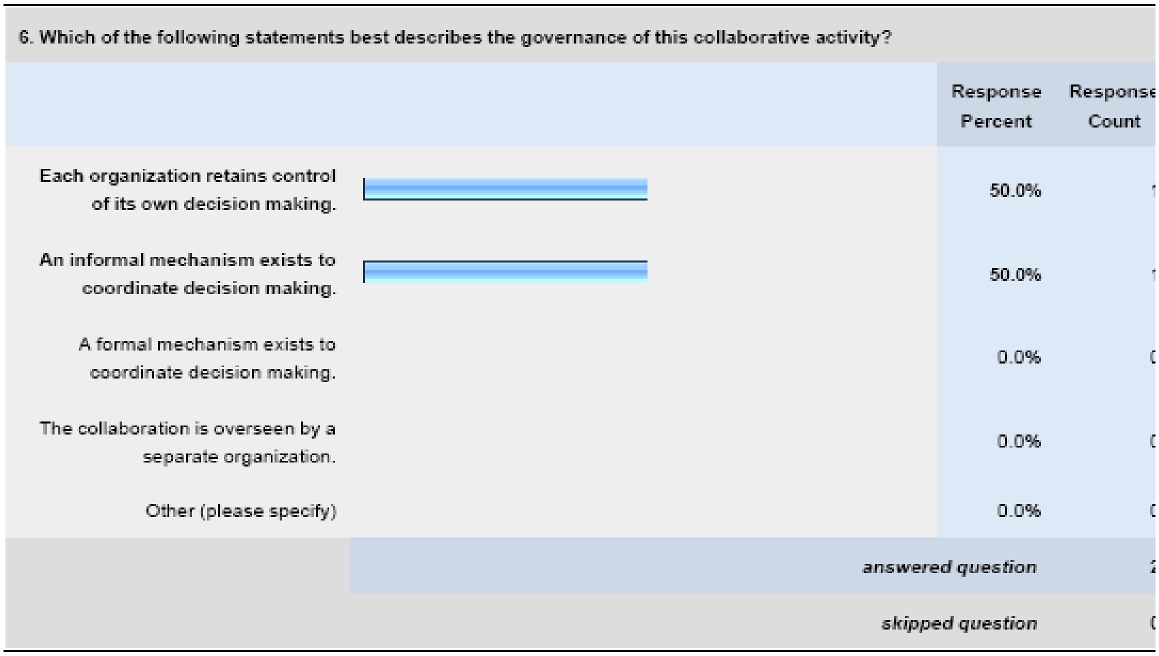
5. Which statement best describes the planned duration of the collaboration?

	Response Percent	Response Count
Continuous—there is no planned end	50.0%	1
Finite—collaboration ends when a set of defined objectives have been met	50.0%	1
Pilot—collaboration is an experiment and may not continue	0.0%	0
Other (please specify)	0.0%	0
answered question		2
skipped question		0

Figure 23. Stakeholder Questionnaire Question 5.

Question 6: Which of the Following Best Describes the Governance of This Collaborative Activity?

As noted in Figure 24, 1 respondent indicated that “each organization retains control of its decision making,” and the other chose “an informal mechanism exists to coordinate decision making.”



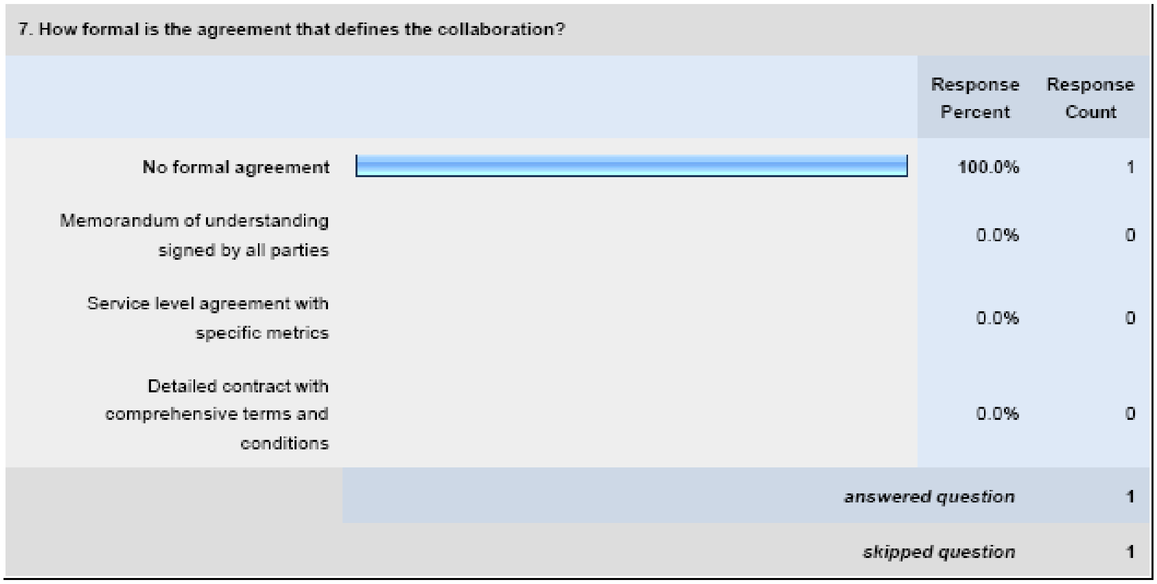
6. Which of the following statements best describes the governance of this collaborative activity?

	Response Percent	Response Count
Each organization retains control of its own decision making.	50.0%	1
An informal mechanism exists to coordinate decision making.	50.0%	1
A formal mechanism exists to coordinate decision making.	0.0%	0
The collaboration is overseen by a separate organization.	0.0%	0
Other (please specify)	0.0%	0
answered question		2
skipped question		0

Figure 24. Stakeholder Questionnaire Question 6.

Question 7: How Formal Is the Agreement That Defines the Collaboration?

As shown in Figure 25, one respondent indicated that there was “no formal agreement”; the other respondent did not answer this question.



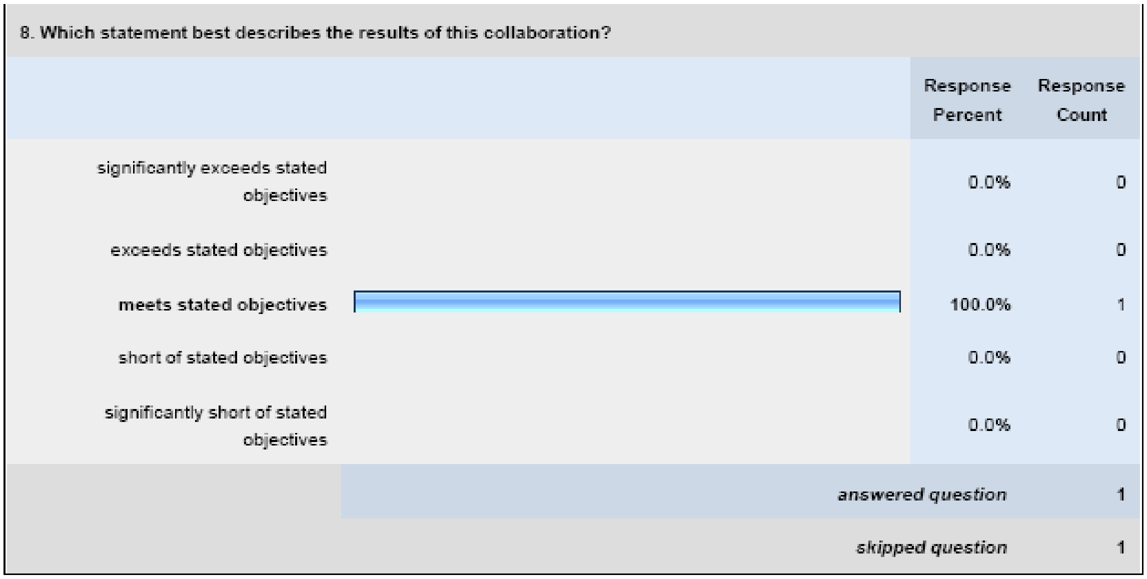
7. How formal is the agreement that defines the collaboration?

	Response Percent	Response Count
No formal agreement	100.0%	1
Memorandum of understanding signed by all parties	0.0%	0
Service level agreement with specific metrics	0.0%	0
Detailed contract with comprehensive terms and conditions	0.0%	0
	answered question	1
	skipped question	1

Figure 25. Stakeholder Questionnaire Question 7.

Question 8: Which Statement Best Describes the Results of This Collaboration?

Figure 26 details that only one response was provided, indicating that “it met the stated objectives.”



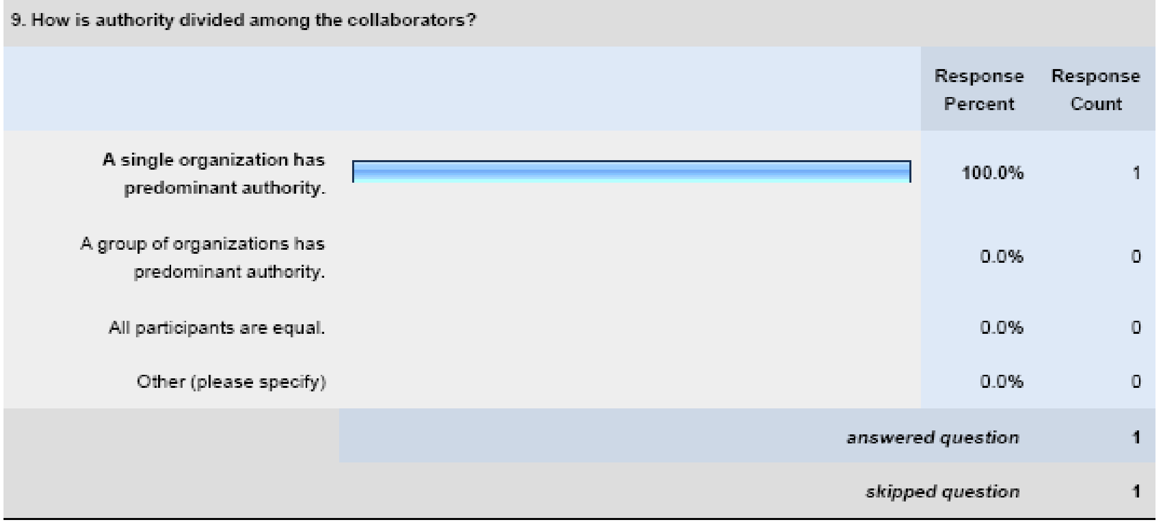
8. Which statement best describes the results of this collaboration?

	Response Percent	Response Count
significantly exceeds stated objectives	0.0%	0
exceeds stated objectives	0.0%	0
meets stated objectives	100.0%	1
short of stated objectives	0.0%	0
significantly short of stated objectives	0.0%	0
answered question		1
skipped question		1

Figure 26. Stakeholder Questionnaire Question 8.

Question 9: How Is Authority Divided Among Collaborators?

As shown in Figure 27,only one response was provided, in which the respondent stated “a single organization has predominant authority.”



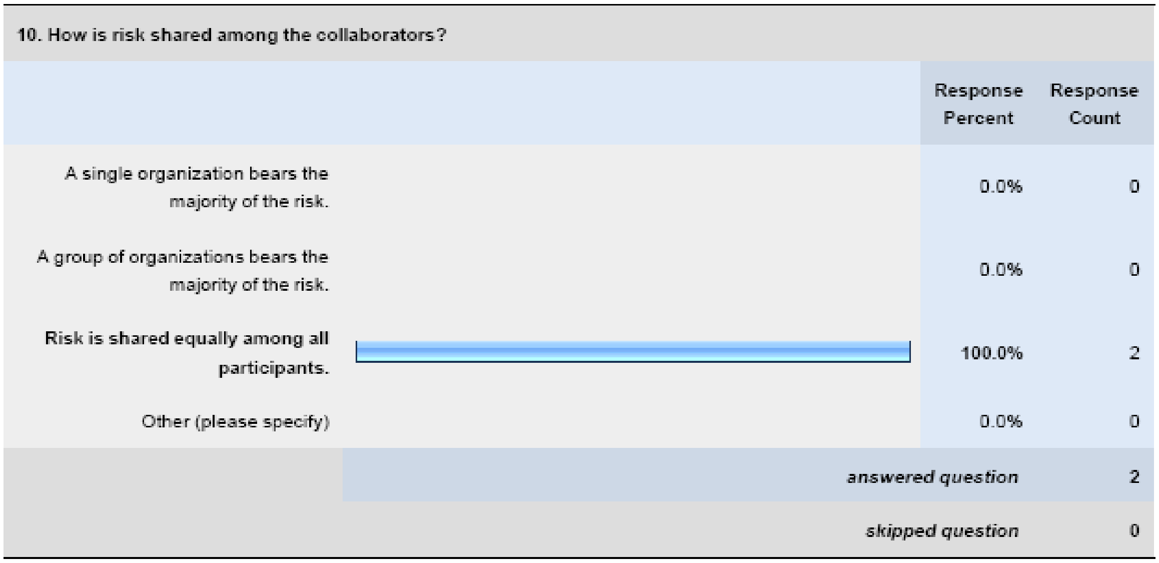
9. How is authority divided among the collaborators?

	Response Percent	Response Count
A single organization has predominant authority.	100.0%	1
A group of organizations has predominant authority.	0.0%	0
All participants are equal.	0.0%	0
Other (please specify)	0.0%	0
answered question		1
skipped question		1

Figure 27. Stakeholder Questionnaire Question 9.

Question 10: How Is Risk Shared Among the Collaborators?

As depicted in Figure 28, both responses indicated that the risk was "shared equally among all participants."



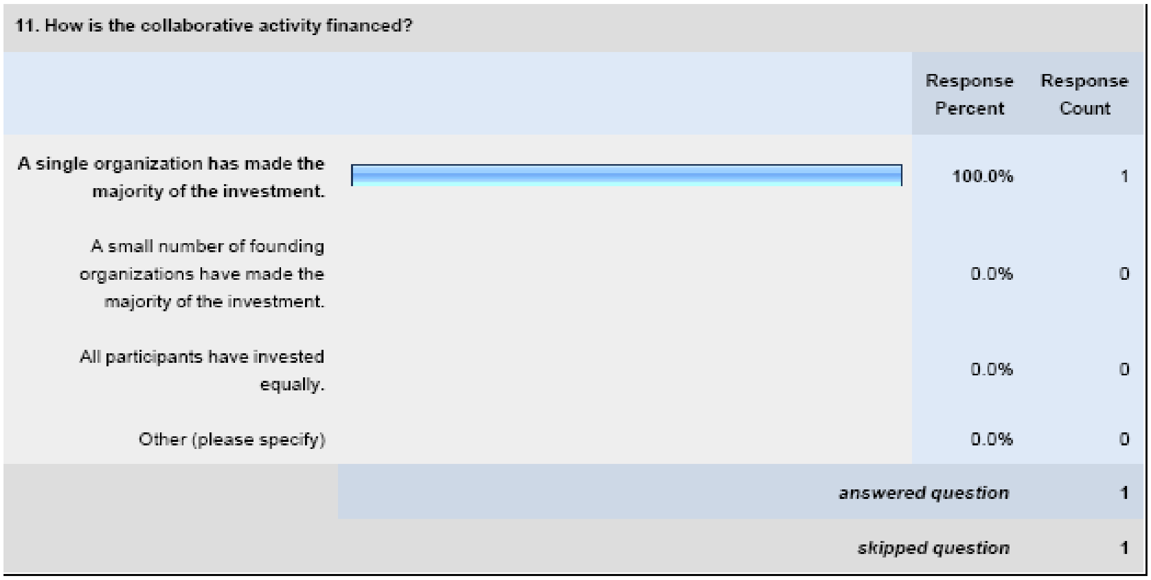
10. How is risk shared among the collaborators?

	Response Percent	Response Count
A single organization bears the majority of the risk.	0.0%	0
A group of organizations bears the majority of the risk.	0.0%	0
Risk is shared equally among all participants.	100.0%	2
Other (please specify)	0.0%	0
answered question		2
skipped question		0

Figure 28. Stakeholder Questionnaire Question 10.

Question 11: How Is the Collaborative Activity Financed?

Figure 29 shows that only one response was provided, in which the respondent stated “a single organization has made the majority of the investment.”



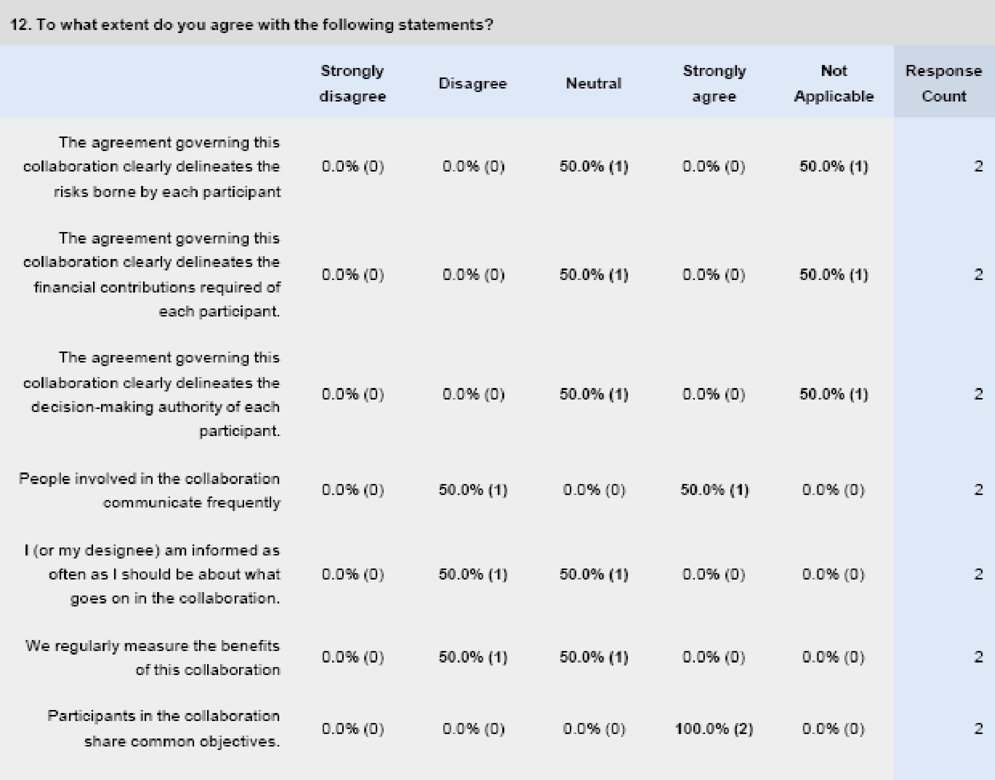
11. How is the collaborative activity financed?

	Response Percent	Response Count
A single organization has made the majority of the investment.	100.0%	1
A small number of founding organizations have made the majority of the investment.	0.0%	0
All participants have invested equally.	0.0%	0
Other (please specify)	0.0%	0
	answered question	1
	skipped question	1

Figure 29. Stakeholder Questionnaire Question 11.

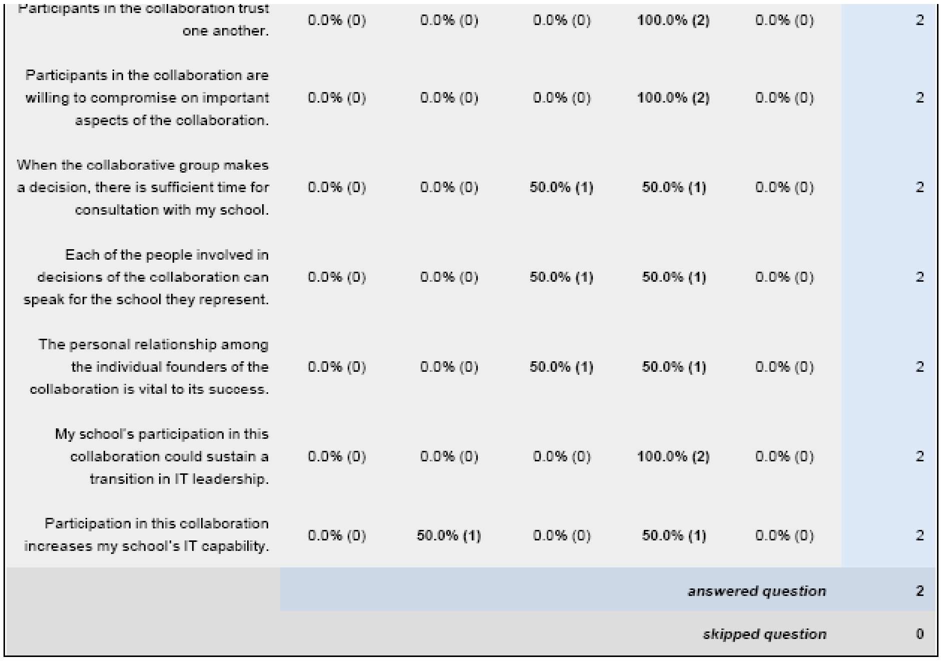
Question 12: To What Extent Do You Agree or Not With the Following Statements?

Figure 30 encapsulates both respondents' agreement or disagreement with each statement.



12. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
The agreement governing this collaboration clearly delineates the risks borne by each participant	0.0% (0)	0.0% (0)	50.0% (1)	0.0% (0)	50.0% (1)	2
The agreement governing this collaboration clearly delineates the financial contributions required of each participant.	0.0% (0)	0.0% (0)	50.0% (1)	0.0% (0)	50.0% (1)	2
The agreement governing this collaboration clearly delineates the decision-making authority of each participant.	0.0% (0)	0.0% (0)	50.0% (1)	0.0% (0)	50.0% (1)	2
People involved in the collaboration communicate frequently	0.0% (0)	50.0% (1)	0.0% (0)	50.0% (1)	0.0% (0)	2
I (or my designee) am informed as often as I should be about what goes on in the collaboration.	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	0.0% (0)	2
We regularly measure the benefits of this collaboration	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	0.0% (0)	2
Participants in the collaboration share common objectives.	0.0% (0)	0.0% (0)	0.0% (0)	100.0% (2)	0.0% (0)	2

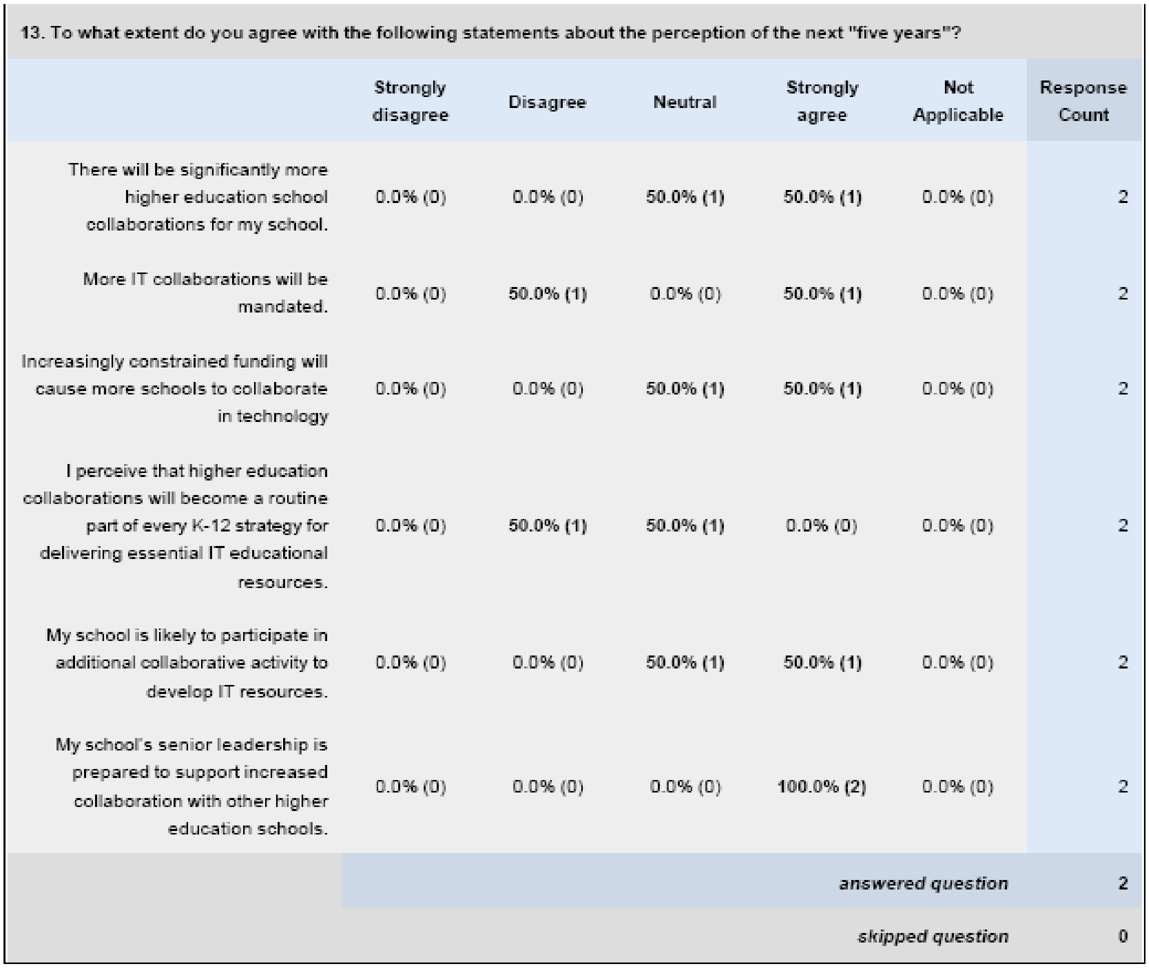


Participants in the collaboration trust one another.	0.0% (0)	0.0% (0)	0.0% (0)	**100.0% (2)**	0.0% (0)	2
Participants in the collaboration are willing to compromise on important aspects of the collaboration.	0.0% (0)	0.0% (0)	0.0% (0)	**100.0% (2)**	0.0% (0)	2
When the collaborative group makes a decision, there is sufficient time for consultation with my school.	0.0% (0)	0.0% (0)	**50.0% (1)**	**50.0% (1)**	0.0% (0)	2
Each of the people involved in decisions of the collaboration can speak for the school they represent.	0.0% (0)	0.0% (0)	**50.0% (1)**	**50.0% (1)**	0.0% (0)	2
The personal relationship among the individual founders of the collaboration is vital to its success.	0.0% (0)	0.0% (0)	**50.0% (1)**	**50.0% (1)**	0.0% (0)	2
My school's participation in this collaboration could sustain a transition in IT leadership.	0.0% (0)	0.0% (0)	0.0% (0)	**100.0% (2)**	0.0% (0)	2
Participation in this collaboration increases my school's IT capability.	0.0% (0)	**50.0% (1)**	0.0% (0)	**50.0% (1)**	0.0% (0)	2
					answered question	**2**
					skipped question	**0**

Figure 30. Stakeholder Questionnaire Question 12.

Question 13: To What Extent Do You Agree or Not With the Following Statements About the Perception of the Next Five Years Regarding Collaboration?

Figure 31 captures the responses. Respondents indicated they felt their school leadership is prepared to support increased collaboration with other higher education schools.



13. To what extent do you agree with the following statements about the perception of the next "five years"?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable	Response Count
There will be significantly more higher education school collaborations for my school.	0.0% (0)	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	2
More IT collaborations will be mandated.	0.0% (0)	50.0% (1)	0.0% (0)	50.0% (1)	0.0% (0)	2
Increasingly constrained funding will cause more schools to collaborate in technology	0.0% (0)	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	2
I perceive that higher education collaborations will become a routine part of every K-12 strategy for delivering essential IT educational resources.	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	0.0% (0)	2
My school is likely to participate in additional collaborative activity to develop IT resources.	0.0% (0)	0.0% (0)	50.0% (1)	50.0% (1)	0.0% (0)	2
My school's senior leadership is prepared to support increased collaboration with other higher education schools.	0.0% (0)	0.0% (0)	0.0% (0)	100.0% (2)	0.0% (0)	2
					answered question	2
					skipped question	0

Figure 31. Stakeholder Questionnaire Question 13.

Stakeholder Interviews—Online

The Survey Monkey tool was used to capture online interview responses from the three participants in Rockingham County and Harrisonburg City schools who felt more comfortable participating electronically than in person or via telephone. To ensure confidentiality and anonymity, all interview subjects were assigned pseudonyms, and their respective schools' names were omitted.

Question 1: Do You Feel Collaboration Between Higher Education and K-12 Is a Good Thing? Why Collaborate?

Betty:

There are situations where collaboration can be helpful. For example, sometimes higher ed has more funding and equipment, and that can benefit K-12 if we collaborate. Also, sometimes higher ed has students who need to interact with k-12 for their practicum's, and this is a good benefit for K-12. Why collaborate? K-12 receives time, equipment and expertise benefits.

Wilma:

Yes, collaboration is a good thing. There is much to be gained by bringing together a variety of perspectives, talents, and resources to meet a common goal. There are many ways that higher ed can support K-12 through the development of resources, such as the Internet safety guide, and the sharing of ideas.

Fred:

Sure, academia and higher ed, are creative grounds for new ideas and high level pedagogy. Higher Ed. needs to see the actual teaching process in public schools and gain skill sets that teachers "on the firing line" are developing. In many cases, higher education teachers that have never been in the public classroom, or spent sufficient time to develop superior teaching techniques, are challenged to really understand the processes and techniques needed to teach the new k-12 learner.

Question 2: What Is Helpful and Not So Helpful About Collaboration? What Suggestions Do You Have for Improving Collaborative Efforts Between K-12 and Higher Education?

Betty:

In the Cyber Safety collaboration, there was a minimum of interaction between the higher ed participants and k-12 participants. Improved collaboration would have taken place with more involvement by additional staff, and perhaps student involvement, too.

Wilma:

Collaboration is helpful when the collaborators are working together on a common goal. It is less helpful when the collaboration is one entity providing what they perceive the other needs without close contact to ensure that they understanding the situation. It seems a closer relationship between the institutions would foster greater collaboration. Each needs to understand the needs of the other as well as what each has to offer. One suggestion would be to meet more frequently to discuss ideas.

Fred's response was that "Administrators at both ends need to try to find time to communicate. [T]ough problem."

Question 3: What Other Ways Could K-12 Benefit From Collaboration With Higher Education?

Wilma's response: "K-12 could benefit from collaboration by taking advantage of the talent base that the university has to offer to work with students on specific projects that the school division does not have the resources or knowledge to provide."

Fred responded that "internships and collegiate student time spent in public schools connecting with kids" could be helpful.

Question 4: What Reasons or Ways Do You and Your Organization Benefit From Collaboration, in General and as it Relates to Internet Safety Awareness and Education?

Betty:

In past collaborative efforts, we have borrowed equipment, had students come help us with projects, and had guest speakers, for some examples. We have received software as part of grants, in some collaborations. Lessons have been developed and shared in some. In the Internet safety collaboration, we hope to benefit by having an interactive web site set up which our students can use.

Wilma:

Collaboration has provided students and teachers with experiences beyond what may have been available. Some students worked with a JMU student to create video; teachers worked with JMU students on web pages. The Internet safety guide will be a useful resource for both students and teachers.

Fred's response was: "In my case, [the JMU representative] and I have worked on producing a project that can be used for schools including teacher/student guides, posters, web pages, etc."

Question 5: Please Tell Me About Your Collaboration Efforts in the Past. What Were Your Experiences (Positive and/or Negative) and What Worked and Did Not Work So Well?

Betty:

> We have had students come as class assistants, and to share a lesson in art—works well. We have participated in classes in which we received hardware and software as part of our continued use and extension of class learning—good things. In addition to things mentioned above, we have had students visit college campuses for lectures, lab visits and tours. This is a positive!

Wilma:

> The collaborative efforts between [the two K-12 schools] has been very beneficial to us probably mostly due to a shared vision. Collaborative efforts that have been negative have been those times when one party was simply doing what they thought we needed without awareness of our real needs. For example, JMU students created the websites for the teachers using software and skills that the teachers were not able to maintain. For true collaboration to occur, I think it is necessary for the relationship to develop. For example, we weren't involved in the creation of the guide initially and really felt there wasn't any collaboration going on until we met with [the JMU representative] and suggested the use of a website

instead of a print format. If this meeting had occurred earlier in the process, it would have been beneficial to both parties.

Fred’s response was that “The Cyber Citizen project with JMU is of value and is just getting started.”

Question 6: Do You Have Any Suggestions for How This Collaborative Effort Between Higher Education (JMU) and Rockingham County and Harrisonburg City Schools Relating to Internet Safety Awareness and Education Could Be Replicated in Other Parts of the Commonwealth of Virginia?

Betty:

The web site will be a wonderful resource; having interactive assessment related to NET*S standards were a wonderful idea proposed by [the JMU representative]. Once developed, this would be a resource that any school in the state could use. A continued effort to keep the website updated and available for online grading of the proposed NET*S assessments would be terrific.

Wilma:

The guide certainly can be shared to school divisions throughout the state. Collaboration could occur as modules and topics are added based on the needs of the divisions. Again, there needs to be contact and relationships developed for this to occur.

Fred:

The ITRT are the “go to” people on Internet safety in public schools. They are the first line of initiation of programs. This conduit is the most successful method yet

> to date. That said, higher education needs to have an ongoing relationship with the ITRT and computer specialists in the school divisions. Taking [the JMU representative] (and her outstanding efforts through the IIIA department) out of the equation, there has been no collaboration whatsoever from any department at JMU including the education department. The education department and the cyber security department are obvious departments that "should" have an interest in this topic. [The two K-12 schools] have an ongoing working relationship teaching Internet safety through the ITRT connections."

Stakeholder Interviews—Telephone

Telephone interviews were conducted with the two other stakeholders, one from Marketing and External Relations, Institute for Infrastructure and Information Assurance, JMU, the other from Educational Technology, Virginia Department of Education. To ensure confidentiality and anonymity, all interview subjects were assigned pseudonyms, and their respective schools' names were omitted. These interviews were conducted on February 21, 2008.

Question 1: Regarding Collaboration – (1) What Do You See From Other Ventures That Worked Well, and Those That Were Not as Positive? (2) How Does That Contrast With This Venture Between Rockingham County, Harrisonburg City Schools and JMU?

Jane:

> Collaboration offers an ease on burden of resources and communication. Schools wished to participate because of the need to provide an avenue for a solution to

the Internet Safety Guidelines. Collaboration usually works best when agreements are not formalized; and offer flexibility and ease of use. I would be interested in what people participating thought they were getting out of the partnership versus what they actually received. There is value in understanding the particular role of higher education in Internet safety and it is probably best communicated through the school board and parent teacher organizations (PTO) for the most value, access, visibility and impact to a district or program.

Mary:

Although I cannot give you specific details, I have heard a general sentiment within the community that JMU creates great products and then presents them to the community with a "here's something good for you" attitude. There has been some feelings of resentment and patronization. The University is sometimes seen as the 500 pound gorilla instead of a collaborative partner. In the past there could have been better cooperation in development of projects and materials to gain more community buy-in.

The CyberCitz project, however, was developed from the start with community involvement, specifically with middle school teacher collaborations. Joe Showker, especially, was involved with preconceptions, content preparation and editing. As the project was nearing completion, we met with other middle school teachers to get feedback on the guide. It was at this point that the teachers told us, “please don’t give us any more print materials. Give it to us electronically, and if you could add ‘stupid flash games,’ it would be great!” This interaction caused us to alter the course for the project. Instead of having only a youth-focused booklet of information, the project now includes a printed educators' guide, a youth-edition website, classroom posters on technology and ethics, and e-lessons templates available through a free learning management system.

The project started out as a simple printed booklet and grew—because of the collaboration—to much more. As a result of our willingness to truly collaborate, I feel we have a product that already has buy-in from its audience and a long practical life ahead.

Question 2: Is This Higher Education K-12 Collaborative Effort Something That Can Be Used Throughout the Commonwealth, in Your Opinion?

Jane:

Feedback that more schools want collaboration with higher education is extremely positive and recommendations to make resources and solutions that higher education can share with K-12 are of real value…. Products should be portable or accessible via the internet and should provide ease of use for incorporating the resource into the program of study…. I was referred to a Pokemon Learning resource that the company was working with VA DOE…. Absolutely this can be accomplished and it is not quite as hard for technology rich environments like [Bedrock] County or Northern Virginia schools.

Mary:

It is my sense that often higher eds set out to do good things for their communities; albeit, with a "holier than thou" attitude. We have the information, the knowledge and the know-how that somehow transcends what practitioners experience. If the efforts are truly collaborative, I believe higher ed has sometime spectacular to offer. If that information, knowledge and know-how can be translated into programs that facilitate practitioners' efforts, then this project can be a model for the Commonwealth for other issues. But the collaboration requires careful listening with frequent feedback and teamwork.

Summary

This chapter detailed all the data collected by the instruments. The next chapter, Chapter V, presents the recommendations and conclusions based upon this data.

V. RECOMMENDATIONS AND CONCLUSION

Introduction

This study builds upon the recommendation made by EDUCAUSE (2005), on behalf of the higher education, to the U.S. Congress that colleges and universities have long been interested in supporting the efforts of elementary and secondary schools to improve the awareness of students on issues such as cyber ethics and security. Hence, this study has significance to the development of higher education, presents a solution for the vision of technology use in education for the future, provides effective lessons learned, and fosters a better understanding of the collaborative resolve of higher education in furthering its advisory and leadership role within communities.

This study provides potential solutions for the following intended audiences:

- **Virginia Educational Leaders:** A solid foundation of information resulted that can be used to understand the themes of Internet safety and how higher education can facilitate educational leadership movements with its academic strengths within its communities.
- **Teachers** can build on this framework and create lessons built around Internet safety within their classrooms.

- **Technology Leaders** can use this *Kids Guide*, in both hard copy and electronic form, as a resource to educate and implement an Internet safety awareness program within their schools.
- **Administrators** can use this *Kids Guide* to examine necessary school rules and regulations and how Internet safety can help lead to solutions for current or future problems regarding technology use in the middle school community.

Higher Education Officials can use the lessons learned from this higher education partnership as a model to collaborate with K-12 education.

Research Questions

The study's goal was to evaluate one higher education institution's (JMU's) effectiveness in assisting the middle school education community through its community partnership with the VA DOE, Rockingham County, and Harrisonburg City middle school educators in meeting Virginia's Internet safety awareness and education requirements for middle school children in 2007. Meeting these requirements was achieved through JMU's development and delivery of its *Cyber Citizenship for Kids Guide* (IIIA, 2007) in both hard copy and electronic version. These tools were to serve as an Internet safety handbook for Virginia middle school children. Once this *Kids Guide* was distributed in the Fall of 2007, this study pursued the following research questions to achieve this study's goal:

Research Question 1: Was JMU's grassroots approach, as subject matter expert in information security education, and through its community-based partnership with VA DOE and middle school teachers in Virginia, *perceived as being effective* in helping

Virginia educators meet the requirements set forth by the VA DOE's *Guidelines and Resources for Internet Safety in Schools* (2006b) with its *Cyber Citizenship for Kids Guide* for Internet safety awareness and best practices?

Research Response 1: Yes. This research suggests that JMU's grassroots approach, as subject matter expert in information security education, and through its community-based partnership with VA DOE and middle school teachers in Virginia, was perceived as being effective in helping Virginia educators meet the requirements set forth by the VA DOE's *Guidelines and Resources for Internet Safety in Schools* (2006b) with its *Cyber Citizenship for Kids Guide* for Internet safety awareness and best practices on a number of levels.

This JMU *Kids Guide* project started out as a simple printed booklet and grew—because of the collaboration—to much more. As a result of JMU's and the K-12 schools' willingness to truly collaborate, this resource provided educators with another resource to meet the requirements set forth by the Commonwealth for Internet safety in schools.

Research Question 2: Was this community partnership on cyber safety between higher education and K-12 institutions perceived by educational stakeholders as feasible and effective?

Research Response 2: Yes. Throughout the survey instruments (e.g., Figure 17, Survey 2, Question 7-8) the responses collected indicated that 85.7% strongly agreed that these schools were likely to pursue future collaboration activities with higher education leaders with whom they have a long-standing professional relationship, like JMU in Rockingham County (Figure 8, Question 7). The effectiveness of this community partnership was further demonstrated throughout stakeholder interviews that not only were Rockingham County schools eager to participate and collaborate with JMU, but such collaboration occurred frequently to ensure this JMU *Kids Guide* met the educator requirements. Common themes of providing a high-value educational resource on Internet safety via a higher education collaborative approach were echoed throughout the surveys and interviews conducted.

Research Question 3: Finally, what aspects of a county-wide community partnership effort to enhance K-12 cyber safety awareness can serve as a credible delivery model for Virginia Commonwealth and federal efforts in this area?

Research Response 3: The greatest strength that this case study in Rockingham County, Virginia, has is that it can serve as a model for delivering Internet safety education best practices throughout the Commonwealth by taking on one community at a time—that is, encompassing a grassroots approach versus a top-down approach wherein Internet safety resources are developed by higher education and provided to K-12 as a possible solution. This research study demonstrates that this type of top-down approach was not welcomed within Rockingham County schools; rather, these schools respected and appreciated the level of involvement once JMU became more hands-on with the liaisons and collaborated on a common vision for an Internet safety resource that could meet the Commonwealth-wide guidelines for middle school Internet safety education and awareness. This personal approach to education and collaboration is what separates this higher education and K-12 collaboration environment from other top-down models for delivery of similar Internet safety education and awareness programs and materials. This sentiment was actively demonstrated throughout the interviews and stakeholder questionnaire. For example, Wilma stated “the collaboration efforts between the two K-12 schools has been very beneficial to us mostly due to a shared vision.” In this study, relationships developed which allowed trust and a shared vision to flourish in developing an Internet safety resource in the *Kids Guide*.

This grassroots approach is further supported in response to a follow-up question with the Virginia Department of Education, Office of Educational Technology staff: Which counties or areas in Virginia appear to have the greatest need for Internet safety education and/or resources, in your opinion? An official in their office shared the following response:

> All school divisions have equal access to the information and resources’ links posted on the Office of Educational Technology’s web pages for the *Guidelines and Resources for Internet Safety* at http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml.
>
> Most of the materials listed in the resources section of the *Guidelines* are Web-based, or free upon request. Printed and CD materials have been issued to school divisions by the State Attorney General’s office.
>
> School divisions have been working for the past two years on the development of their division’s Internet safety policy and program to implement the policy. The program of implementation will include professional development. By September 1, 2008, all school division are required by state code to submit to the Office of Educational Technology a final copy of the division’s

> Internet safety policy, as a part of their Acceptable Use Policy, and an overview of the division’s program to implement the Internet safety policy.
>
> If you wish to provide free assistance through higher education institutions to local school divisions in the form of professional development, we suggest that you contact school divisions in your area to see what their specific needs are. The following are divisions that may be interested in your free assistance and professional development sessions:
>
> - Greene County
> - Nelson County
> - Clarke County
> - Madison County
> - Page County
> - Rappahannock County
> - Shenandoah County
> - Warren County
>
> We appreciate your willingness to offer free assistance through higher education institutions to local school divisions. (personal communication, February 8, 2008)

Strengths and Weaknesses

This case study’s major strength was that it represented a community-based effort in Rockingham County, Virginia. The institutions of JMU, Rockingham County Schools, and Harrisonburg City Schools participated because they were actively seeking a solution to provide Internet safety education awareness and resources to the K-12 students within the Rockingham County community. Participants were provided an overview of the collaborative project via their school liaison, and participation was completely voluntary. Survey and interview instruments were provided via a third-party web software platform (Survey Monkey) and, therefore, responses to the surveys were completely anonymous. Participants who wanted to contribute via an interview format were provided the option of either interacting online via Survey Monkey, face-to-face, or via a telephone interview. The strength in providing a flexible format for sharing and collecting data was that it encouraged open, relaxed, and honest communication. Another of this study's greatest strengths was that it was small and afforded a community-focused approach, thereby allowing a greater breath of questioning in both the interview sessions and surveys.

Ironically, this case study's primary weakness was the same as its greatest strength, in that it only focused on Rockingham County and Harrisonburg City schools. It did not take into account other counties throughout the Commonwealth. In addition, it did not focus on the quality of the Internet safety content provided by JMU, nor address the students' points of view. It was limited to various levels of instructors and administrators and their perspectives on how successful—or not—community collaboration was between JMU, Rockingham County, and Harrisonburg City schools.

Recommendations

Since this was a community-led program, recommendations are proposed for each of the participants in this study: higher education (with JMU as the model program), K-12, and VA Department of Education, Office of Educational Technology.

Recommendations for Higher Education

Create Mentorship Opportunities With Local K-12 Schools

Create opportunities to mentor the K-12 schools in your areas of expertise. In doing so, foster relationships through the K-12 Parent Teachers Organizations (PTO) for greater visibility of the collaboration opportunities and resources you can make available to the K-12 community. In particular, (a) provide Internet safety educational resources to students, parents, guardians, ITRT staff, and other academic resources; (b) publicize professional/teacher development activities; (c) capture the requirements for K-12's needed educational resources from your community schools.

Allow the K-12 school the flexibility to participate in developing curriculum enhancing resources (e.g. *Cyber Citizenship Kids Guide*), and ensure your resources are electronic and web-based for ease of use in the classrooms. Almost 54% of the respondents (as indicated in Figure 7) were uncertain of benefits in collaboration with higher education. Figure 5 shows that 50% of the respondents indicated they had not engaged with higher education in a partnership to provide an education resource due to a perceived lack of higher education outreach. Thus, higher education working through the schools' PTA/PTO organizations can provide great visibility to their level of expertise in areas like Internet safety. Further, working with and through the ITRTs rather than directly with the teachers can better ensure that resources are "integrated" with lesson plans to meet the Commonwealth SOL standards.

Foster a Community-Based Working Group

Foster a community-based working group encompassing higher education, local K-12 leadership including ITRT and teacher support, middle school students' parents and guardians, and community stakeholders including law enforcement. This coalition can share community-wide responsibility for providing funding-strapped K-12 programs with Internet safety resources to be used in the classrooms and at home. Figure 9 identifies that the respondents had mixed reviews on whether their school was highly skilled in forming collaborations with higher education, industry, or government organizations. This Figure 9 also draws strong attention to the fact that the respondents believed their educational leadership believes strongly that collaboration increases learning resources for their classrooms. Figure 17 reveals 85.7% of the respondents strongly agreed that their school is likely to pursue collaboration with higher education leaders with whom they have a longstanding relationship. Fostering community-based working groups to meet Internet safety requirements for the K-12 community—to include K-12, higher education, industry, law enforcement, and leadership from the Virginia Department of Education, Office of Educational Technology—can provide a strong funnel for Internet safety resources for K-12.

Recommendations for Rockingham County and Harrisonburg K-12 School Leadership

Empower School Leadership to Seek External Support

Empower school leadership to seek external professional development activities relating to Internet safety so they have every opportunity to become Internet safety, security, and ethically aware. Figure 3 identifies that 82.6% of the respondents had participated in Internet safety awareness or education programs nationally or locally in the 18 months prior to the survey. Although both Rockingham and Harrisonburg County school staff identified themselves as proficient regarding Internet safety, it is a constantly changing environment, creating a constant need for all of us to remain proficient and up-to-date with the latest views and learning methods regarding Internet safety. Leverage the PTA/PTO to provide a platform for higher education to aid in educating parents, guardians, and the community on Internet safety, security, and ethics principles.

Empower ITRT Staff to Seek External Support

Empower all ITRT staff to develop stakeholder relationships with higher education to allow for more open access to state-supported educational resources and areas of expertise with subject matter experts. In addition, ITRTs should form a committee which regularly assesses the completeness and effectiveness of their own Internet safety awareness educator program. Figure 9 identifies "difficulty structuring collaborative agreements" as the primary barrier to pursuing collaboration more extensively within the schools. While Figure 17 identified that 82.6% of the respondents stated that they had participated in Internet safety education or awareness programs in the 18 months prior to the survey, 78.6% of these same respondents had not participated in collaboration with higher education on any level in the last five years. ITRT staff acting as the technology arm of the school programs for all K-12 levels should be brokering opportunities with higher education as one avenue for future solution providers regarding Internet safety.

Become a Model Program and Mentor

Become a model program for Internet safety and mentor other K-12 county schools that are potentially less knowledgeable regarding Internet safety and less sure of how to meet the guidelines for Internet safety education in the Commonwealth. While the respondents showed (Figure 9) that they did not regularly look to other peer schools as sources of innovation, Figure 17 reveals that over 86% of the respondents agreed that it was beneficial for their respective schools to share their higher education collaboration resources with peer schools.

Recommendation to Virginia Department of Education, Office of Educational Technology

Establish State-Wide Working Groups

Establish several community-based working groups throughout the Commonwealth with key stakeholders from each K-12 district and the associated higher education institutions, forming a "one-team" relationship that can be leveraged to direct Internet safety, security, and ethics resources to K-12 educators, ITRTs, and parents. This posturing helps provide a net for all K-12 programs to meet the requirements of the VA Department of Education's *Guidelines and Resources for Internet Safety in Schools* (2006b).

Collaboration Roadmap Implementation Strategies

For this case study to have purpose throughout the Commonwealth and its lessons learned to serve as model steps for connecting higher education and K-12 with guidance from the Commonwealth, this study recommends a “Roadmap” (Table 7) for future implementation strategies.

Table 7

Recommended Higher Education Collaboration Roadmap

Responsible Body	Recommended Action
Virginia Department of Education, Office of Educational Technology	**1. Establish several community-based working groups throughout the Commonwealth with key stakeholders from each K-12 district, the associated higher education institutions, and form a “one-team” relationship that can be leveraged to direct Internet safety, security and ethics resources to K-12 educators, ITRTs, and parents.** *This posturing helps provide a net for all K-12 programs to meet the requirements of the Virginia Department of Education Internet Safety Guidelines.*
Commonwealth K-12 Schools	**1. Empower school leadership to seek external professional development activities relating to Internet safety so they have every opportunity to become Internet safety, security and ethically aware.** **2. Individual schools should have the flexibility to identify the manner in which Internet safety education is completed and/or integrated into their lesson plans to meet SOL standards.** **3. Increase awareness for professional development activities for ALL staff—not just ITRTs—when seeking to teach Internet safety curriculum.** **4. Internet safety education programs and materials should be made available through the PTA/PTO organizations to all parents, guardians, and community members.** **5. School districts should develop an evaluation arm via the ITRTs.**
Higher Education	**1. Create opportunities to mentor the K-12 schools within your community in your areas of expertise.** *In doing so, foster relationships through the K-12 Parent Teachers Organizations (PTO) for greater visibility of the collaboration opportunities and resources you can make available to your K-12 community. In particular: (a) provide Internet safety educational resources to students, parents, guardians, ITRT staff, and other academic resources; (b) publicize professional/teacher development activities; (c) capture the requirements for K-12’s needed educational resources from your community schools.* **2. Foster a community-based working group.** *Have the group encompass higher education, local K-12 leadership including ITRT and teacher support, and community stakeholders including law enforcement. This coalition can share community-wide responsibility for providing funding-strapped K-12 programs with Internet safety resources to be used in the classrooms and at home.*

Implications for Further Research

This research did not survey K-12 students to learn about issues affecting their understanding and/or level of individual competency regarding Internet safety awareness or education. Future studies in this areas would be helpful to potentially provide K-12 authorities an opportunity to better understand how Internet safety awareness and education is being comprehended by their students. This research also did not focus on the competency of JMU's Internet safety educational resource entitled *Cyber Citizenship Kids Guide*, but instead specifically focused on the collaborative environment that was created around the ad hoc partnerships formed between K-12 middle schools in Rockingham County, Harrisonburg City, JMU, and the Virginia Department of Education, Office of Educational Technology in working collaboratively to meet the mandated cyber safety educational requirements for Rockingham County and Harrisonburg City middle schools.

As noted in the Literature Review (Chapter II), standardization and focus needs to be followed through National Education Technology Standards for Teachers (NETS-T) (International Society for Technology in Education, 2002b), which required teachers to be technologically literate about issues concerning technology use, and National Education Technology Standards for Students (NETS-S) (International Society for Technology in Education, 2002a), which provides standards for students to master computer technology concepts. The National Cyber Security Alliance's (NCSA) planning forward follows a similar suit, noting "NETS for teachers, administrators, and students as a framework to guide educational leaders in recognizing and addressing the essential conditions for effective use of technology support in education" (NCSA 2007). Further research in understanding teachers' levels of Internet safety preparedness and competency would serve well in understanding both teachers' and students' comprehension levels for Internet safety and awareness education resources.

Conclusion

Since this research was initiated in 2006, several national-level actions occurred. The NCSA, in its letter to the Attorney General for the United States dated July 24, 2007, calls for *A Need for Comprehensive Cyber Ethics, Safety and Security Education within the United States* (NCSA, 2006). The Virginia Department of Education states that "The new Children's Internet Privacy Act (CIPA) requires all schools to implement various technologies that are designed to shield children from harmful content" (VA Department of Education, 2006). Therefore, higher education in Virginia should be poised to carry the torch and assist K-12 in meeting its Commonwealth-mandated effort for Internet safety awareness in K-12 schools.

Additionally, a step which supports this researcher's scholarly work within this collaboration study has been incorporated in theory. The NCSA (2007), within its plan entitled *A Need for Comprehensive Cyber Ethics, Safety and Security Education within the United States* recommended that all "cyber awareness prevention programs must incorporate cyber ethics, safety, and security (C3)™ principles" (NCSA, 2007b). NCSA created a similar roadmap which it identifies under "A Framework for Implementing State Wide Cyber Safety, Security, and Ethics Lessons and Programs within Schools, Libraries and After School Programs" (NCSA, 2007b). NCSA's proposed outline works from these (C3) principles and gathering the right stakeholders with levels of expertise within a topic area to deliver effective curricula. In addition, for 2007, the NCSA developed a toolkit for educators providing a solution for presenting cyber security awareness messages and tips to students in middle schools (NCSA, n.d., see http://www.staysafeonline.org/basics/assemblyinabox.html).

On a Rockingham County local level, the Virginia Department of Education reports that “the Bedford County (VA) Sheriff’s Office, has provided access to Virginia school divisions to allow NetSmartz materials from the National Center for Missing and Exploited Children as a tool to assist in implementing a division’s program for Internet safety” (VA Department of Education, 2006b).

NCSA recently conducted focus groups with adults ranging from 18 to 65, and found that the majority of adults assumed schools are already teaching cyber security, safety, and ethics classes. According to an NCSA report (2007b), “most adults felt that if schools were not currently teaching such classes as part of their curricula, they should be.” According to the focus group participants for the NCSA, “parents feel overwhelmed with teaching their children the technical aspects of how to protect their identities and information online, and look to educators as the best suited to instill such training and good habits” (NCSA, 2007b). Based on NCSA’s recent research, there is a “clear expectation among adults, parents and constituents that school districts and their education system are already or should already be integrating cyber security, safety and ethics lessons within the curriculum” (NCSA, 2007b). This most recent NCSA research (2007) pointed to a 2007 University of Michigan National Poll on Children’s Health

Issues wherein adults ranked “Internet safety” as the 7th most important issue affecting children.

Currently, according to the NCSA, “Virginia is the only state with a law in place requiring schools to teach Internet safety and security lessons on an annual basis” (2007b) In addition, the NCSA states that “other states such as California and New York have legislation pending to require schools to teach safety, while looking for ways to include such lessons in their statewide ‘technology in the classroom’ mandates” (2007b).

The Virginia Department of Education’s *Guidelines and Resources for Internet Safety in Schools* (2006b) provide local schools a flexible framework to provide local school districts with the means to integrate cyber awareness programs and curricula into already existing prevention programs and lessons. While the Virginia example is the best model that currently exists in the country that provides students with cyber awareness lessons and programs, it still can benefit from community stakeholder support to fulfill its mandated (yet unfunded) requirement for Internet safety education commonwealth-wide.

Implementation Status

As of this writing, a follow-up with the VA Department of Education, Office of Educational Technology, revealed that the key lessons learned from this collaboration study are already being implemented in spirit throughout the Commonwealth outreach programs. JMU also noted that through their membership and participation in the NCSA, NCSA was working to integrate the spirit of this study’s recommendations on a nationwide level (C. Elliott, personal communication, February 10, 2008).

The recommendations outlined in this chapter provide a suggested “roadmap” with key steps to ensure this case study can be modeled throughout the Commonwealth and successfully ensure all K-12 schools meet the requirements for Internet safety education—not only in 2008, but in future years.

In a Superintendent’s memo dated March 14, 2008, the Commonwealth of Virginia Department of Education Superintendent for Instruction announced the availability of technical assistance for school years 2008-2009 and appropriated $5 million Commonwealth-wide for federal funds under the No Child Left Behind Act of 2001 (VA DOE, 2008a). Under this Tech Ed program, the goal is to improve student academic achievement through using technology in schools. The VA Department of Education states that “It is also designed to assist every child crossing the digital divide by ensuring that every student is technology literate by the end of the eighth grade, and encourage effective integration of technology with teacher training and curriculum development” (VA DOE, 2008b). This memo spurred the Virginia Department of Education, Office of Educational Technology to award eight regional consortium grants. The approximately $5 million will be distributed each year for a five-year period in the form of competitive sub-grants for professional development—i.e, learning how to use technology that helps to transform the teaching and learning environment. Virginia’s eight consortia presented a showcase of their activities at the Educational Technology Leadership Conference in March 2008.

This exciting development means the lanes in the road that have been developed since this case study was kicked off in 2006—indeed, the concepts in the roadmap created by this study—are beginning to be realized today, 2008. Communication and information sharing are now more important elements in the Virginia Ed Tech program. The system is also one of the methods it uses to provide technical assistance and professional development to consortia members and individual formula grant participants. The Virginia Department of Education, Office of Educational Technology reports, “Each consortium has a system for its members to email, work collaboratively, and have virtual planning sessions. Some of the systems being used by individual consortia for this are Angel, Blackboard, and Tapped In 2” (2008).

The map of the Commonwealth in Figure 32 identifies the eight consortia across the state. As of this writing, the school divisions have identified their individual needs, goals, and objectives to the regional consortium level. Consortium technology programs and professional development activities will be implemented in coming years to address these needs.

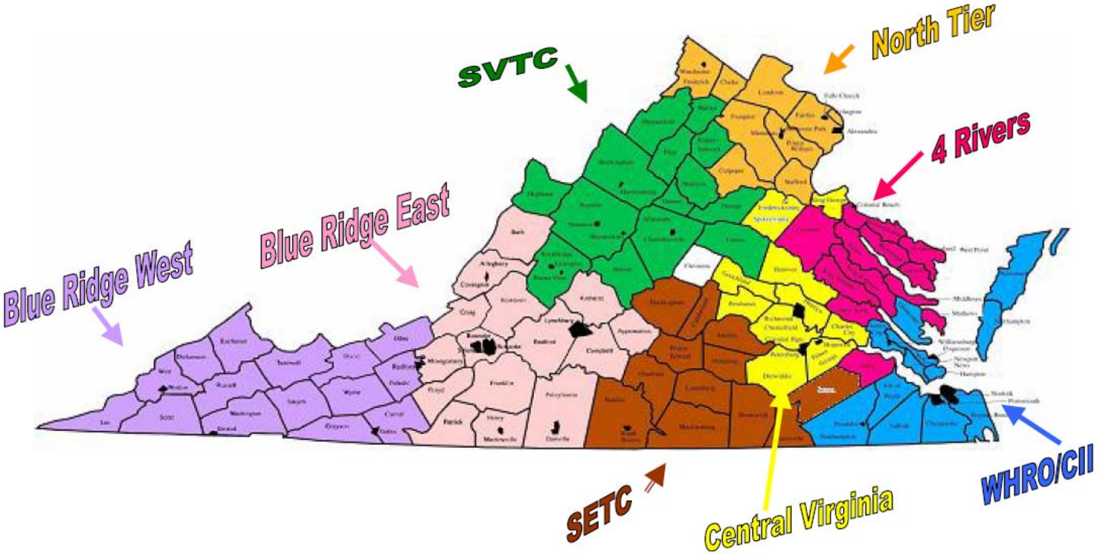


Figure 32. Virginia’s eight Ed Tech consortia. From Virginia Department of Education (2008).

The Shenandoah Valley Consortia indicates in their *Enhancing Education Through Technology (Ed Tech) Competitive Grant Report* (VA DOE, 2008a) that they plan to use potential funding for two overarching goals: “Provide sustained, high quality professional development activities on integrating technology within new or existing curricula”; and “Implement and encourage ongoing integration methods for effective technology into classroom instruction” (VA DOE, 2008a).

The Shenandoah Valley Consortia—which includes both the Harrisonburg City and Rockingham County district schools examined in this case study—includes a total of 20 school divisions and 3 private schools. There are 170 schools in total, 8,000 teachers, and 83,000 students (VA DOE, 2008a). This Shenandoah Consortia includes the following districts: Albemarle, Augusta, Buena Vista, Charlottesville, Greene, Harrisonburg, Highland, Lexington, Madison, Nelson,, Orange and Page. Shenandoah Consortia partners include: Blue Ridge Community College, Explore Learning, Intel Corporation, International Society for Technology in Education, James Madison University, Shenandoah Public Education Network, United Learning, University of Virginia, and the Virginia Educational Technology Alliance (VA DOE, 2008b).

Through these collaborative “lanes in the road” being implemented via these eight Commonwealth consortiums operating under the Virginia Office of Educational Technology leadership, this research’s seven overall recommendations have been effectively achieved. These lanes, developed under the No Child Left Behind and Enhancing Education Through Technology (EdTech) Competitive Grant process, could fully encompass Internet safety criteria. The Virginia Department of Education states that “each K-12 school division must still submit to the Office of Educational Technology a copy of their schools’ Internet safety component and a statement that the Internet safety program has been reviewed” (VA DOE, 2006b). During September 2008, the Office of Educational Technology will review each school division’s submission to ensure they meet the *Guidelines and Resources for Internet Safety in Schools* (2006b) as originally outlined.

Since this case study was initiated and its follow-on surveys and interviews were completed, the Virginia Department of Education, Office of Educational Technology has also issued guidance and relevant materials to enhance the success of Internet safety education and awareness to meet its goals throughout the Commonwealth, bringing the educational community together for a common goal, under the eight consortiums, for the No Child Left Behind effort phased with the Commonwealth's Enhancing Education Through Technology (Ed Tech) Program. The department recently published *A Handbook for Virginia's School Divisions* (March 2008) and *Ideas for Integrating Internet Safety Into the Curriculum* (June 2007). Similar to the JMU *Kids Guide* (IIIA, 2007), these two guides are expected to provide ideas for addressing Internet safety within the context of the Virginia SOLs.

This study witnessed a collective community rise between higher education, the Virginia Department of Education's Office of Educational Technology, and Rockingham County and Harrisonburg City schools to assume leadership roles with a "one-team" spirit to deliver Internet safety solutions for the middle schools students in these school districts. Implementing this study's recommendations should only further strengthen the existing Commonwealth programs' framework and provide another collaborative and agile solution aimed at protecting children in cyberspace.

APPENDIX A. DEFINITION OF TERMS

Abuse: Improper or excessive use or treatment (Merriam-Webster, 2004).

Acceptable Use Policy (AUP):

Policy set up by the network administrator or other school leaders in conjunction with their technology needs and safety concerns. This policy restricts the manner in which a network may be used, and helps provide guidelines for teachers using technology in the classroom. (4teachers.org, 2004)

Access: Ability to get what you need. Data access is being able to get to (and, usually, having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider such as America Online (WhatIs, 2004).

Bandwidth: Amount of information that one can send through a connection, measured in bits-per-second (Bps). A standard page of English text contains about 16,000 bits (4teachers.org, 2004).

Blog (from We**Blog**)**:** Web page that contains links to Web sites that cover a particular subject or that are based on some other criterion, such as interesting or entertaining sites. The blog typically provides a short summary of the referenced sites and may also contain commentary and humor. Blogs have become a form of artistic expression, enabling anyone to personally publish a directory about a subject that interests them (TechWeb, 2004).

Bluetooth: An industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency (Wikipedia).

Browser: Software application that allows people to view Internet pages (4teachers.org, 2004).

Cellular Telephone (or Mobile Phone): Type of short-wave analog or cyber telecommunication in which a subscriber has wireless connection from a mobile telephone to a relatively nearby transmitter. The transmitter's span of coverage is called a cell (WhatIs, 2004).

Chat Room:

Interactive discussion (by keyboard) about a specific topic that is hosted on the Internet or on a Bulletin Board Service (BBS). On the Internet, chat rooms are available from major services such as AOL, individual Web sites and the Internet Relay Chat (IRC) system, the Net's traditional computer conferencing. Chat rooms are set up to handle group discussions, and everyone sees what everyone else types in, although two people can decide to break off and have their own keyboard chat. "Instant messaging" (IM), a similar concept, works in an opposite manner. With instant messaging, two people normally interact back and forth and must specifically invite others to join in. (TechWeb, 2004)

Citizen(ship): Person who works against injustice not for individual recognition or personal advantage but for the benefit of all people. In realizing this task-shattering privilege, ensuring information and competence, acting in favor of all—each person becomes a citizen (Johnson & Nissenbaum, 1995).

Communication:

1: Act or instance of transmitting **2a:** information communicated **b:** a verbal or written message **3a:** process by which information is exchanged between individuals through a common system of symbols, signs, or behavior also**:** exchange of information **b:** personal rapport **4a:** system (as of telephones) for communicating **b:** system of routes for moving troops, supplies, and vehicles **c:** personnel engaged in communicating **5a:** a technique for expressing ideas effectively (as in speech) **b:** the technology of the transmission of information (as by print or telecommunication). (Merriam-Webster, 2004)

Computer Ethics: Analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology (Johnson & Nissenbaum, 1995).

Computer Literacy: Level of expertise and familiarity someone has with computers. Computer literacy generally refers to the ability to use applications rather than to program. Individuals who are very computer literate are sometimes called power users (PC Webopedia, 2004).

Cyberspace:

Metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. The term was coined by author William Gibson in his sci-fi novel *Neuromancer* (1984). (PC Webopedia, 2004)

Cyber:

System based on discontinuous data or events. Computers are cyber machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on. There is no simple way to represent all the values in between, such as 0.25. All data that a computer processes must be encoded cyberly, as a series of zeroes and ones. Internally, computers are cyber because they consist of discrete units called bits that are either on or off. But by combining many bits in complex ways, computers simulate analog events. In one sense, this is what computer science is all about. (PC Webopedia, 2004)

Cyber Access: Full electronic participation in society regardless of gender, race, age, ethnicity, and physical or mental challenges (Ribble & Bailey, 2004b).

Internet Safety: Norms of behavior with regard to technology use (Ribble & Bailey, 2004b).

Cyber Commerce: Electronic buying and selling of goods (Ribble & Bailey, 2004b).

Cyber Communication: Electronic exchange of information (Ribble & Bailey, 2004b).

Cyber Divide:

Discrepancy between people who have access to and the resources to use new information and communication tools, such as the Internet, and people who do not have the resources and access to the technology. The term also describes the discrepancy between those who have the skills, knowledge and abilities to use the technologies and those who do not. The cyber divide can exist between those living in rural areas and those living in urban areas, between the educated and uneducated, between economic classes, and on a global scale between more and less industrially developed nations. (PC Webopedia, 2004)

Cyber Education: Process of teaching and learning about technology and the use of technology (Ribble & Bailey, 2004b).

Cyber Etiquette: Electronic standards of conduct or protocol (Ribble & Bailey, 2004a).

Cyber Responsibility: Electronic responsibility for actions and deeds which is either ethical or unethical (Ribble & Bailey, 2004b).

Cyber Rights: Those freedoms extended to every student, administrator, teacher, parent or community member (Ribble & Bailey, 2004b).

Cyber Safety: Free from cyber danger and guaranteed cyber physical wellbeing (Ribble & Bailey, 2004b).

Internet Safety (Self-Protection): Taking necessary precautions to guarantee electronic cyber safety (Ribble & Bailey, 2004b).

Distance Learning:

Type of education, typically college-level, where students work on their own at home or at the office and communicate with faculty and other students via e-mail, electronic forums, videoconferencing, chat rooms, bulletin boards, instant messaging and other forms of computer-based communication. Most distance learning programs include a computer-based training (CBT) system and communications tools to produce a virtual classroom. Because the Internet and World Wide Web are accessible from virtually all computer platforms, they serve as the foundation for many distance learning systems. (PC Webopedia, 2004)

E-Commerce – Electronic-Commerce: Buying and selling of goods and services on the Internet, especially the World Wide Web (WhatIs, 2004).

Education:

1a: Action or process of educating or of being educated; also**:** a stage of such a process; the knowledge and development resulting from an educational process; the field of study that deals mainly with methods of teaching and learning in schools. (Merriam-Webster, 2004)

Educational:

Technology is used by some to mean hardware—the devices that deliver information and serve as tools to accomplish a task—but those working in the field use technology to refer to a systematic process of solving problems by scientific means. Hence, educational technology properly refers to a particular approach to achieving the ends of education. Instructional technology refers to the use of such technological processes specifically for teaching and learning. (Ely, 1996)

E-mail - Electronic-mail:

Transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, minicomputers, and computer networks have an e-mail system. Some electronic-mail systems are confined to a single computer system or network, but others have gateways to other computer systems, enabling users to send electronic mail anywhere in the world. Companies that are fully computerized make extensive use of e-mail because it is fast, flexible, and reliable. (PC Webopedia, 2004)

Etiquette: Conduct or procedure required by good breeding or prescribed by authority to be observed in social or official life (Merriam-Webster, 2004).

Firewall: Hardware and/or software that separates a Local Area Network (LAN) into two or more parts for security purposes (4teachers.org, 2004).

File Transfer Protocol (FTP):

Set of rules that allows two computers to "talk" to one another while transferring files from one to another. This is the protocol used when you transfer a file from one computer to another across the Internet. Many Internet sites have publicly accessible repositories of information that can be obtained using FTP, by logging in using the account name "anonymous." These sites are called "anonymous ftp servers." (4teachers.org, 2004)

Homepage: Page on the Internet which most often gives users access to the rest of the Web site. A site is a collection of pages (4teachers.org, 2004).

Inappropriate: Not appropriate, unsuitable (Merriam-Webster, 2004).

Information Literacy: Ability to locate, evaluate, and use information to become independent lifelong learners (Southern Association of Colleges and Schools, 1996).

Instant Messaging (IM):

Exchanging messages in real-time between two or more people. Unlike a dial-up system such as the telephone, instant messaging (IM) requires that both parties be logged onto their IM service at the same time. Also known as "chatting," IM has become very popular for both business and personal use. In business, IM provides a way to contact coworkers at any time of the day, providing that they are at their computers. Because you are signaled when other IM users have logged on, you know they are back at their desks, at least for the moment. Thus, IM is often used as a way to avoid telephone tag, whether the communication continues as text messages or winds up as a traditional phone call. (TechWeb, 2004)

Instructional Technology:

Hardware, such as personal computers, CD-ROMs and multimedia, handheld learning devices and software that are the instructional programs run on personal computers. It also includes distance learning modalities such as the Internet, videos, television, satellite, radio, cable, fiber optics, short wave, microwave and related technologies. (U.S. Department of Education, 2004)

Internet: Global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions (PC Webopedia, 2004).

Internet Protocol (IP) Number:

Unique number consisting of four parts separated by dots, for example 129.237.247.243. This is the number assigned to a host machine which is retrieved by a DNS when a request for an Internet site is made. These numbers usually correspond to unique domain names, which are easier for people to remember. (4teachers.org, 2004)

Local Area Network (LAN): Computer network limited to the immediate area, usually the same building (4teachers.org, 2004).

Leader: Person responsible for achieving objectives through the work of others and for building and maintaining the team of which he or she is a member (Tozer, 1997)

Misuse: “**1:** Use incorrectly **2:** Abuse, Mistreat” (Merriam-Webster, 2004).

Mobile Phone see Cellular Telephone

MP3: File extension for MPEG, audio layer 3. Layer 3 is one of three coding schemes (layer 1, layer 2 and layer 3) for the compression of audio signals. Because MP3 files are small, they can easily be transferred across the Internet. (PC Webopedia, 2004).

Napster:

Application that gives individuals access to one another's MP3 files by creating a unique file-sharing system via the Internet. Napster lets users view and download the contents of MP3 directories from other Napster users' hard drives. Napster has been under fire from the Recording Industry Association of America (RIAA), who interprets Napster as copyright-infringement software. But, because the MP3 files do not reside on Napster's servers, nor does Napster charge a fee for the service, critics felt the RIAA had a weak legal leg to stand on. (PC Webopedia, 2004).

Netiquette (from Inter**net etiquette**)**:**

Etiquette guidelines for posting messages to online services, and particularly Internet newsgroups. Netiquette covers not only rules to maintain civility nature of forum messages (PC Webopedia, 2004).

Network: Connected computers that allow people to share information and equipment. Many schools have a Local Area Network and are also connected to a Wide Area Network, such as the World Wide Web (4teachers.org, 2004).

Palmtop: Small computer that literally fits in your palm. Compared to full-size computers, palmtops are severely limited, but they are practical for certain functions such as phone books and calendars. (PC Webopedia, 2004).

PDA - Personal Desktop Assistant: Handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. (PC Webopedia, 2004).

Plagiarize: “To steal and pass off (the ideas or words of another) as one’s own**:** use (another’s production) without crediting the source**:** to commit literary theft**:** present as new and original an idea or product derived from an existing source” (Merriam-Webster, 2004).

Responsibility: “**1:** Quality or state of being responsible: as a : moral, legal, or mental accountability b: Reliability, Trustworthiness **2**: something for which one is responsible: a Burden” (Merriam-Webster, 2004).

Rights:

Qualities (as adherence to duty or obedience to lawful authority) that together constitute the ideal of moral propriety or merit moral approval **2:** something to which one has a just claim**:** the power or privilege to which one is justly entitled (2) plural**:** the property interest possessed under law or custom and agreement in an intangible thing especially of a literary and artistic nature **3:** something that one may properly claim as due **4:** the cause of truth or justice. (Merriam-Webster, 2004)

Safety: Condition of being safe from undergoing or causing hurt, injury, or loss (Merriam-Webster, 2004).

School:

Division of the school system consisting of students in one or more grades or other identifiable groups and organized to give instruction of a defined type. One school may share a building with another school or one school may be housed in several buildings. (U.S. Dept. of Education, 2004)

Search Engine: Any of a number of giant databases on the Internet which store data on Web sites and their corresponding URLs. Some popular search engines are Metacrawler, Alta Vista, and Excite (4teachers.org, 2004).

Security:

1: Quality or state of being secure : as **a:** freedom from danger **b:** freedom from fear or anxiety **2a:** something that secures **b**(1)**:** measures taken to guard against espionage or sabotage, crime, attack, or escape (2)**:** an organization or department whose task is security. (Merriam-Webster, 2004)

Software: Programs used to operate computers and related devices (Whatis, 2002).

Staff Development: Professional training to advance the knowledge, skills, and effectiveness of teachers (Joyce & Showers, 1988).

TCP/IP - Transmission Control Protocol/Internet Protocol: Programming protocols invented by individuals in the U.S. Department of Defense to carry messages around the Internet (4teachers.org, 2004).

Technology:

Application of scientific discoveries to the development and improvement of goods and services that ideally improve the life of humans and their environment. Such goods and services include materials, machinery, and processes that improve production or solve problems. (4teachers.org, 2004).

Technology Integration: Planned, systematic introduction and institutionalization of technology into schools and organizations (Pownell, 2002)

Technology Leader: One who leads the school or district in its effort to improve or restructure, using emerging technologies as core resources for educational change (Bailey, Lumley, & Dunbar, 1995).

Text Messaging:

Sending short text messages to a device such as a cellular phone, PDA or pager. Text messaging is used for messages that are no longer than a few hundred characters. The term is usually applied to messaging that takes place between two or more mobile devices. (PC Webopedia, 2004)

Uniform Resource Locator (URL): Address of any given site on the Internet (4teachers.org, 2004).

Virtual:

Not real. The term virtual is popular among computer scientists and is used in a wide variety of situations. In general, it distinguishes something that is merely conceptual from something that has physical reality. For example, virtual memory refers to an imaginary set of locations, or addresses, where you can store data. It is imaginary in the sense that the memory area is not the same as the real physical memory composed of transistors. (PC Webopedia, 2004).

Wide Area Network (WAN):

This network connects several computers so they can share files and sometimes equipment, as well as exchange e-mail. A wide area network connects computers across a large geographic area, such as a city, state, or country. The World Wide Web is a WAN. (4teachers.org, 2004)

Web Browser: “Computer programs, such as Netscape Navigator, Microsoft Internet Explorer, and Mosaic, that help you navigate the Web and access text, graphics, hyperlinks, audio video, and other multimedia” (Classzone, 2006).

Wireless: Telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path (Whatis, 2001).

APPENDIX B. SURVEY QUESTIONNAIRE 1

JMU Higher Education & K-12 Community Partnership Initiative
Cyber Safety Awareness
Rockingham County and Harrisonburg City Middle Schools
2007 Survey Questionnaire

Thank you for your willingness to answer this survey which focuses on your experiences with and perceptions about how higher education institutions collaborate and develop and deliver K-12 related cyber safety awareness and educational resources within their community. This case study is being conducted by James Madison University, Institute for Infrastructure and Information Assurance (IIIA) and James Lantzy, Doctoral Student, George Mason University. It will employ a single case study including a survey process, and follow up interviews with key stakeholders from higher education, academia and state educational authorities.

This survey will help us better understand your current perception of the "existing" collaborative environment in Rockingham County and Harrisonburg City between higher education and the K-12 community. In addition, the current acceptability and role of national cyber safety and other higher education programs and collaboration efforts in the middle school landscape.

1. ROLE:______________________________
(e.g., Classroom teacher, library, ITRTs, Administrative, or other)

Please circle the appropriate answer (Y / N)

2. Have you now or in the past 18 months been a participant in a partnership with at least one other institution to assess a cyber safety, cyber security or cyber ethics awareness or educational program – either nationally or locally? (Y / N)

3. Do you currently use any nationally known programs (i.e., isafe, netkidz, other) in your classroom? Is so, why? If not, why?

4. To what extent do you agree with the following statements?

		Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
4.1.	My organization places high value on external collaboration					
4.2.	My organization places high value on innovation in its operations					
4.3.	My institution collaborates frequently with other institutions in areas related to information technology?					
4.4	My institution collaborates frequently with other institutions in areas related to Internet safety?					
4.5	You have been made aware of the VA Internet Safety Guidelines and educator responsibilities for 2007?					
4.6.	You have been provided a copy of the VA Internet Safety Guidelines?					
4.7	You have your students access the Internet daily for lessons or suggest use at home?					
4.8	My institution regularly looks to peer institutions as sources of innovation?					
4.9	My institution regularly looks to higher education environments for innovative learning opportunities					
4.10	My institution regularly looks to other industries or government for innovative learning opportunities					

5. What are the primary reasons your institution has not engaged with higher education in a partnership to provide an educational resource to your institution? Please select as many that are applicable.

i. ___Failed prior attempts
ii. ___Lack of funding
iii. ___Lack of institutions outreach
iv. ___Lack of understanding in how to manage collaborations

v. ___More confident in own institutions capabilities

vi. ___Risk

vii. ___Other: Please explain
____.

6. In what technology areas has your institution participated in collaboration for a resource in the past?

AREA	NO	YES
Enterprise information systems (email, web development, management)		
Learning management systems		
Instructional Technology		
Internet safety		

6.1.1 What is the major reason your institution has elected to collaborate with higher education to provide an Internet/cyber safety related resource?

6.2.1 What have been the most significant barriers you have had to overcome to become a major participant in collaborations to provide essential IT resources? Select as many that apply.
___Lack of start-up funding
___Lack of institutional support
___Uncertain benefits
___Legal obstacles
___Lack of suitable institutions to collaborate with
___Establishing a common vision for the collaboration with other participating institutions

7. In the past 18 months, has your institution been in a partnership with at least one other institution to DEVELOP an essential IT resource (e.g., cyber safety tools) that involved sharing risk, resources and/or management control?
___No
___Yes

7.1 If yes, please elaborate____.

8. To what extent do you agree with the following statements?

		Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
8.1.	Receiving educational resources from higher education to meet future resource tool demands I perceive as a necessity					
8.2.	In the future, my institution will likely look for more ways to collaborate with higher education to meet future resource needs.					
8.3.	I expect to share my higher education resource needs with other peer institutions					
8.4.	My institution is highly skilled at forming collaborations with higher education					
8.5.	My institution is highly skilled at forming collaborations with other organizations (schools, government, industry)					
8.6.	My institution does not regularly look to collaborate with higher education					
8.7	My institution does not regularly look to collaborate with other sources					

8.8	Institution leaders regularly assess the risks of our collaboration efforts					
8.9	Single accountability for managing my institutions collaboration efforts exists					
8.10	The leadership of my institution understands the extent of collaboration activity at my institution.					
8.11	My institutions senior leadership believes higher education collaboration promotes positive educational leadership					
8.12	My institutions senior leadership believes that higher education collaboration increases learning resources					
8.13	I believe higher education collaboration has increased learning resources					

APPENDIX C. SURVEY QUESTIONNAIRE 2

JMU Higher Education & K-12 Community Partnership Initiative
Cyber Safety Awareness
Rockingham County and Harrisonburg City Middle Schools
2007 Survey Questionnaire (2)

Thank you for your willingness to answer this survey which focuses on your experiences with and perceptions about how higher education institutions collaborate and develop and deliver K-12 related cyber safety awareness and educational resources within their community. This case study is being conducted by James Madison University, Institute for Infrastructure and Information Assurance (IIIA) and James Lantzy, Doctoral Student, George Mason University. It will employ a single case study including a survey process, and follow up interviews with key stakeholders from higher education, academia and state educational authorities.

This survey will help us better understand your perception of the community partnership between higher education and K-12 institutions perceived effectiveness and overall feasibility meeting the cyber safety requirements for selected middle schools in Rockingham County and Harrisonburg City middle schools. Additionally, what aspects of this county-wide partnership effort to enhance cyber safety awareness can serve as a credible model for Virginia statewide and/or federal efforts in cyber safety?

ROLE:______________________________
(e.g., Classroom teacher, library, ITRTs, Administrative, or other)

1. Which of the following statements best captures your view of the maturity of higher education's multi-institutional collaborative efforts to deliver or develop essential cyber safety learning resources to K-12?
___ Experiments that still need to demonstrate results
___ Pilot programs that should be expanded
___ Proven methods for delivering some IT resources
___ Essential strategies for the future that should be widely implemented

2. What are the most important factors to you in selecting an institution to collaborate with? Select as many that apply.
___Common institutional missions
___Geographic proximity
___Collaborator's technology capability

___Collaborator’s IT staff skills
___Relationship with IT leaders
___Relationship with institutional leaders
___Common objectives for the collaboration
___Collaborator’s willingness to share risk
___Other

3. To what extent do you agree with the following statements?

		Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
1.	My institution is most likely to pursue collaborations with leaders at other institutions with whom we have a long-standing professional relationship.					
	My institution formally vets each potential collaboration partner.					
	All of our collaborative activities have well-defined goals.					
	We always measure the benefits of our collaborative activity.					
	Our collaborations always include mechanisms to facilitate continuous improvement.					

4. Which of the following activities do you perform when considering participating in a collaborative venture?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
Estimate one-time costs					
Estimate recurring costs					
Quantify potential benefits					
Evaluate the skills of collaborative partners					
Evaluate alternative solutions					

5. What are the primary barriers to pursuing collaboration more extensively at your institution? Select as many that apply.

___Lack of adequate funding
___Insufficient benefits
___Higher priorities
___Technology issues
___Lack of institutional leadership's support
___Lack of staff expertise
___Lack of alignment with the institutional priorities
___Lack of suitable institutions to work with
___Difficulty structuring collaborative agreements
___Other

6. My institution has participated in a collaborative project with higher education in the past five years that failed to meet its stated objectives.

___No
___Yes

If you answered yes – then which of the following best describes the nature of the failed collaboration?

___Effort to develop a software solution
___Effort to provide shared IT infrastructure
___Effort to provide a shared IT service
___Effort to work jointly to implement a new technology

7. In what way did the collaboration fail?

___Actual costs exceeded initial estimates.
___Actual benefits were less than expected.
___Collaboration dissolved before a solution could be created.

8. What were the primary reasons the collaboration failed? Select as many that apply.
___Different objectives among collaborators
___Ineffective governance
___Effort to manage too great
___Insufficient resources
___Technical reasons
___Insufficient leadership
___Insufficient communications
___Inability to make efficient decisions
___Unequal investment among collaborators
___Unequal contributions among collaborators

9. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
Working collaboratively with higher education institutions reduces the cost of K-12 services.					
Working collaboratively with higher education institutions increases the quality of K-12 services.					
Working collaboratively with higher education institutions increases the speed of technology adoption in K-12 institutions.					
Working collaboratively with higher education institutions reduces the risk of K-12 special projects.					

APPENDIX D. INTERVIEW QUESTIONNAIRE OF KEY STAKEHOLDERS

JMU Higher Education & K-12 Community Partnership Initiative
Cyber Safety Awareness
Rockingham County and Harrisonburg City Middle Schools
2007 Interview Questionnaire of Key Stakeholders(1)

The following detailed questions relate to the governance, management, accomplishment of objectives, communications, and outcomes of this community collaborative partnership between higher education and K-12 in Rockingham County and Harrisonburg City K-12 institutions.

ROLE:______________________________
(e.g., Classroom teacher, library, ITRTs, Administrative, or other)

1. Which of the following statements best describes the type of collaboration upon which you are basing your responses?

___Major participant in collaboration to provide a cyber safety resource for K-12
___Major participant in collaboration to develop a cyber safety resource for K-12
___Provide IT services to other institutions
___Get IT services from another institution
___Other

2. Why has your institution elected to participate in this collaboration? Select as many that apply.

___Reduce cost/gain efficiencies
___Enhance K-12 services
___Gain access to scarce IT skills
___Gain access to better technology
___Speed the implementation of technology
___Complete a one-time project more effectively
___Part of a broad institutional commitment to collaborate with others
___Comply with mandated collaboration (by policy or legislation)

3. What is your institution's primary role in the collaboration?

___Founder
___Leader
___Essential participant
___Participant
___Observer

4. Which statement best describes the planned duration of the collaboration?
___Continuous—there is no planned end
___Finite—collaboration ends when a set of defined objectives have been met
___Pilot—collaboration is an experiment and may not continue

5. Which of the following statements best describes the governance of this collaborative activity?
___Each organization retains control of its own decision making.
___An informal mechanism exists to coordinate decision making.
___A formal mechanism exists to coordinate decision making.
___The collaboration is overseen by a separately incorporated organization.
___Other

6. How formal is the agreement that defines the collaboration?
___No formal agreement
___Memorandum of understanding signed by both parties
___Service level agreement with specific metrics
___Detailed contract with comprehensive terms and conditions

7. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
The agreement governing this collaboration clearly delineates the risks borne by each institution					
The agreement governing this collaboration clearly delineates the financial contributions required of each participant.					
The agreement governing this collaboration clearly delineates the decision-making authority of each participant.					

8. How is authority divided among the collaborators?
___A single institution has predominant authority.
___A group of institutions have predominant authority.
___All participants are equal.

9. How is risk shared among the collaborators?

___A single institution bears the majority of the risk.
___A group of institutions bears the majority of the risk.
___Risk is shared equally among all participants.

10. How is the collaborative activity financed?

___A single institution has made the majority of the investment.
___A small number of founding institutions have made the majority of the investment.
___All participants have invested equally.

11. To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
People involved in the collaboration communicate frequently					
I (or my designee) am informed as often as I should be about what goes on in the collaboration.					
We regularly measure the benefits of this collaboration					
Participants in the collaboration share common objectives.					
Participants in the collaboration trust one another.					
Participants in the collaboration are willing to compromise on important aspects of the collaboration.					
When the collaborative group makes a decision, there is sufficient time for consultation with my institution.					

Each of the people involved in decisions of the collaboration can speak for the institution they represent.					
The personal relationship among the individual founders of the collaboration is vital to its success.					
My institution’s participation in this collaboration could sustain a transition in IT leadership.					
Participation in this collaboration increases my institution’s IT capability.					

12. Which statement best describes the results of this collaboration?

___significantly exceeds stated objectives
___exceeds stated objectives
___meets stated objectives
___short of stated objectives
___significantly short of stated objectives

13 To what extent do you agree with the following statements about the next five years?

	Strongly disagree	Disagree	Neutral	Strongly agree	Not Applicable
There will be significantly more higher education institutional collaborations for my institution.					
More IT collaborations will be mandated.					

Increasingly constrained funding will cause more institutions to collaborate in technology					
I perceive that higher education collaborations will become a routine part of every K-12 strategy for delivering essential IT educational resources.					
My institution is likely to participate in additional collaborative activity to develop IT resources.					
My institution's senior leadership is prepared to support increased collaboration with other higher education institutions.					

REFERENCES

REFERENCES

4teachers.org. (2004). Dictionary Main Page. Retrieved February 22, 2006, from http://www.4teachers.org

Adelman, H. (2004). Teaching online safety. *Voices From the Middle, 11*, 17-23.

American Library Association. (2006). *Children's Internet Protection Act of 2002*. Retrieved March 12, 2006 from http://www.ala.org/ala/washoff/WOissues/civilliberties/cipaweb/cipa.htm

Aftab, P. (2000). *The parent's guide to protecting your children in cyberspace*. New York: McGraw-Hill.

Bailey, G. D., Lumley, D., & Dunbar, D. (1995). *Leadership and technology: What school board members need to know*. Alexandria, VA: National School Board Association.

Beach, R., & Bruce, B. C. (2002). Using digital tools to foster critical inquiry. In Alvermann, D. (Ed.) *Adolescents and literacies in a digital world* (pp. 147-163). New York: Peter Lang Publishing, Inc.

Bennett, L. (2005). Guidelines for using technology in the social studies classroom. *The Social Studies, 96*(1), 38-40.

Berson, I. R., Berson, M. J., & Ferron, J. (2002). Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States. *Journal of School Violence, 1*(2), 51-72.

Berson, M. J. (2000). The computer can't see you blush. *Kappa Delta Pi Record, 36,* 158-162.

Berson, M. J., Berson, I. R., & Ralston, M. E. (1999). Threshing out the myths and facts of Internet safety. *Social Education, 63,* 160-162.

Berrier, T. (2007). *Sixth-, seventh-, and eighth-grade students' experiences with the Internet and their Internet safety knowledge*. Unpublished doctoral dissertation, East Tennessee State University. Retrieved November 20, 2008 from http://etd-submit.etsu.edu/etd/theses/available/etd-1023107-155209/unrestricted/BerrierT103107f.pdf

Boyte, H. C. (2002). *Information-Age populism: Higher education as a civic learning organization* [Monograph]. Washington, DC: Council on Public Policy Education.

Burbules, N., & Callister, T. (1996). Knowledge at the crossroads: Some alternative futures of hypertext learning environments. *Educational Theory* , *46*(1), 23-50.

CERIAS K-12 Outreach Program. (2003) *K-12 program description*. Retrieved March 19, 2004, from http://www.cerias.purdue.edu/education/k-2/ k12_program_packet.pdf

Cho, C., & Cheon, J. (2005). Children's exposure to negative Internet content: Effects of Family context. *Journal of Broadcasting and Electronic Media*, *49*, 488-510.

Classzone. (2006). Dictionary Main Page. Retrieved February 16, 2006, from http://www.classzone.com

Computer Security Institute. (2002). *2002 CSI/FBI Computer Crime and Security Survey*. Retrieved July 11, 2006, from http://www.gocsi.com/press/20020407.html

Consortium for School Networking (COSN). (2004). *CyberSecurity for the digital district*. Retrieved June 26, 2006, from http://securedistrict.cosn.org/

Coutu, D. L. (2003, September). Technology and human vulnerability: A conversation with MIT's Sherry Turkle. *Harvard Business Review, 81*(9), 44.

CyberSmart Education Company. (2005a). *CyberSmart curriculum/standards*. Retrieved April 1, 2005, from http://www.cybersmartcurriculum.org/act_sheets/ tech_standards_alignment.pdf

CyberSmart Education Company. (2005b). *CyberSmart K-12 professional development and overview presentation*. Retrieved March 12, 2006, from http://www.cybersmart.org/info/overview_pres.asp

De Geus, A. (1997). *The living company*. Boston: Harvard Business School Press.

eCorridors. (1999). *Virginia Tech's eCorridors Program*. Retrieved April 10, 2006, from http://www.ecorridors.vt.edu/pilots/danville

eCorridors. (2002). *Virginia Tech Broadband Map Program*. Retrieved April 9, 2008, from http://www.ecorridors.vt.edu/research/papers/pdf/ eCorridors_broadband_03-20-08.pdf

Educational Technology, Policy Research, and Outreach – National Cyber Security Alliance (ETPRO-NCSA). (2008a). *2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study*. Retrieved November 20, 2008, from http://staysafeonline.mediaroom.com/file.php/98/NationalC3BaselineSurvey_11_14_08_Final_w_forward+%283%29.pdf

Educational Technology, Policy Research, and Outreach – National Cyber Security Alliance (ETPRO-NCSA). (2008b). *National 2008 Cyberethics, Cybersafety, Cybesecurity Baseline Study Key Findings*. Retrieved November 20, 2008, from http://staysafeonline.mediaroom.com/file.php/97/Baseline+Study+Fact+Sheet.pdf

EDUCAUSE (2005). *Cybersecurity.* Retrieved April 13, 2006, from http://www.educause.edu/Browse/645?PARENT_ID=702

EDUCAUSE Center for Applied Research (ECAR). (2004). *Key findings – Information technology leadership in higher education: The condition of the community.* Retrieved March 12, 2005, from http://www.educause.edu/node/16835

Ely, D. P. (1996). The field of educational technology: A dozen frequently asked questions. (Update of ED 232616). Retrieved March 20, 2006, from ERIC Clearinghouse on Information and Technology, http://www.ericfacility.net/ericdigests/ed366330.html

Ethics. (2001). *American Heritage Dictionary*. Wilmington, MA: Houghton Miflin.

Ethics. (2001). *Webster's Dictionary*. Springfield, MA: Merriam Webster.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online victimization: A report on the nation's youth.* Retrieved November 20, 2008 from http://www.missingkids.com/en_US/publications/NC62.pdf

Gall, M., Borg, W., & Gall, J. (1996). *Educational research: An introduction*. White Plains, NY: Longman.

Gibney, M. (1999) *Globalizing rights: The Oxford Amnesty Lectures*. New York, NY. Oxford University Press.

Gurak, L. J. (2001). *Cyberliteracy: Navigating the Internet with awareness*. New Haven, CT: Yale University Press.

Hirshhorn, L. (2002, July). Campaigning for change. *Harvard Business Review, 80*(7), 98-104.

Institute for Infrastructure and Information Assurance at James Madison University (IIIA). (2007). *Cyber Citizenship for Kids Guide*. Harrisonburg, VA: Author.

International Society for Technology in Education. (2002a). *National education technology standards for students (NETS-S)*. Retrieved April 1, 2005, from http://cnets.iste.org/students/s_profile-68.html

International Society for Technology in Education. (2002b). *National education technology standards for teachers (NETS-T)*. Retrieved April 1, 2005, from http://cnets.iste.org/teachers/t_profile-first.html

Internet2. (2000). *The evolution of multicast: from the MBone to interdomain multicast to Internet2 deployment*. Network IEEE. Retrieved February 4, 2005, from http://ieeexplore.ieee.org

Internet Safety Industry Alliance. (2006). *CSIA policy papers*. Retrieved March 25, 2006, from http://www.csialliance.org/publications/csia_whitepapers/

International Reading Association. (2001). *Integrating literacy and technology in the curriculum: A position statement.* Retrieved December 12, 2004, from http://www.reading.org/positions/technology.html

James Madison University Office of Media Relations. (n.d.). *The newsroom*. Retrieved August 1, 2008, from http://www.jmu.edu/news/TheNewsroom/

Jarvis P., Holford, J., & Griffin, C. (2003). *The theory and practice of learning* (2nd ed.). London: Kogan Page Limited.

Johnson, D. G., & Nissenbaum, H. (1995). *Computers, ethics and social values*. Upper Saddle River, NJ: Prentice Hall.

Joyce, B., & Showers, B. (1988). Training research and pre-service teacher education: A reconsideration. *Journal of Teacher Education, 39*(5), 32-36

Kajder, S., & Bull, G. (2003). Scaffolding for struggling students: Reading and writing with blogs. *Learning and Leading with Technology*, *31*, 32-35.

Karmel, T., & Maclean, R. (Eds.). (2007). *Technical and vocational education and training in an ageing society: Experts meeting proceedings*. National Centre for Vocational Education Research. Retrieved November 20, 2008, from http://www.ncver.edu.au/research/core/cp06110pt1.pdf

Lassner, D. (2006). New directions for higher education. *Partnering with K-12: A statewide approach, 2000*, 111, 35-44.

Lewandowski, J. (2002). Using moral development theory to teach K-12 cyber ethics. *Proceedings of Society for Information Technology and Teacher Education International Conference 2002* (pp. 864-866). Chesapeake, VA: AACE.

McCann, J. (2008, April 3). Focusing on cyber safety. *Education Week's Digital Directions*, *1*. Retrieved Nov. 20, 2008, from http://www.edweek.org/dd/articles/2008/04/03/04teixeira_web2.h01.html

McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and Social Psychology Review*, *4*(1), 57–75.

Merriam-Webster. (2004). *Merriam-Webster unabridged*. Retrieved December 12, 2004, from http://unabridged.merriam-webster.com/

Moore, A. H. (2004). Technology, learning and change: Community development revisited. *EDUCAUSE Quarterly*, 27(2). Retrieved September 17, 2008, from http://www.educause.edu/ir/library/pdf/EQM0426.pdf

National Center for Education (NCES). (n.d.) *Safeguarding your technology*. NCES publ. no. 98-297. Retrieved February 14, 2006, from http://nces.ed.gov/pubs98/safetech

National Council of Teachers of Mathematics. (2003). *The use of technology in the learning and teaching of mathematics*. Retrieved April 1, 2005, from http://www.nctm.org/about/position_statements/position_statement_13.htm

National Council for the Social Studies. (2008). *National Council for the Social Studies*. Retrieved March 1, 2005, from http://www.ncss.org

National Cyber Security Alliance (NCSA). (n.d.). *National Cyber Security Alliance's Cyber Security Assembly Toolbox*. Retrieved June 15, 2008, from http://www.staysafeonline.org/basics/assemblyinabox.html.

National Cyber Security Alliance (NCSA). (2006). *New cyber security study shows consumers are overconfident about identifying online scams*. Retrieved July 12, 2006, from http://www.staysafeonline.org/news/ncsabofafraudstudy.html

National Cyber Security Alliance (NCSA). (2007a). *National Cyber Security Alliance calls on states and school districts to teach Internet safety and security in schools*. Retrieved August 10, 2008, from http://staysafeonline.org/news/ teachinternetsafetyinschools.html

National Cyber Security Alliance (NCSA). (2007b). *A need for comprehensive cyber ethics, safety and security education within the United States*. Retrieved August 10, 2008, fromhttp://staysafeonline.org/whitepapers/ CSAC3WhitePaper-Final081507.pdf

National Internet Safety Alliance. (March 14, 2006). *Roundtable Series: Cyber Security, Safety, and Ethics Education*. Washington, DC: Author.

National Science Teachers Association. (1999). The use of computers in science education. Retrieved April 1, 2005, from http://www.nsta.org/159&psid=4

National Science Teachers Association. (2003). *Inquiring safely: A guide for middle school teachers*. Arlington, VA: Author.

O'Connell, R. (2001). Be somebody else but be yourself at all times: Degrees of identity deception in chatrooms. Retrieved March 15, 2006 from http://www.theonceproject.net/print/deception_print.htm

Payne S. (1999). *Strategic alliances: Building strong ones and making them last.* Retrieved March 1, 2005, from http://www.educause.edu/ir/library/html/cnc9818.html

PC Webopedia. (2004). Dictionary Main Page. Retrieved February 26, 2004, from http://www.pcwebopedia.com

Peterson, R. (2004). *EDUCAUSE: Computer and network security in higher education.* New York: Jossey-Bass.

Pownell, D. (2002). Implementing handheld computers in schools: The research, development and validation of a technology leader's resource guide (Doctoral dissertation, Kansas State University, 2002). *Dissertation Abstracts International, 63*, 2515.

President's Critical Infrastructure Protection Board. (2002). *The national strategy to secure cyberspace*. Retrieved on March 12, 2006, from http://www.whitehouse.gov/pcipb/

Regional Network for the Exchange of Information and Experience in Science and Technology, The (ASINFO). (1999). Learning to be a citizen of cyberspace. *ASINFO Newsletter*. Retrieved July 1, 2005, from http://static.stii.dost.gov.ph/

Ribble, M., & Bailey, G. (2004a).Monitoring Technology Misuse and Abuse. *The Journal Online, Technology Horizons in Education*. Retrieved September 17, 2008 from http://www.educ.ksu.edu/digitalcitizenship/

Ribble, M., & Bailey, G. (2004b). Internet safety: Survival skills for the 21st century. *Learning & Leading with Technology*. Retrieved September 17, 2008 from http://www.educ.ksu.edu/digitalcitizenship/

Ribble, M., Bailey, G., & Ross, T. (2004). Internet safety and ISTE's National Educational Technology Standards: Identifying appropriate technology behavior. *Learning & Leading with Technology*. Retrieved September 17, 2008 from http://www.educ.ksu.edu/digitalcitizenship/Articles.htm.

Rodin, J. (2004). *Engagement through university–community partnerships*. Retrieved May 16, 2006, from http://www.pew-partnership.org/pdf/new_directions/2_partnerships.pdf

Senge, Peter M. (1994). *The fifth discipline: The art and practice of the learning organization*. New York: Currency Doubleday.

Shenandoah Valley Consortium. (2008). *Enhancing Education Through Technology Ed Tech Program consortia grant projects*. Retrieved from http://www.doe.virginia.gov/VDOE/Technology/EdTech/ConsortiaInfo-Goals.pdf

Southern Association of Colleges and Schools. (1996). Criteria for Accreditation. *Commission on Colleges*, 59.

Swain, C., & Gilmore, E. (2001). Repackaging for the 21st century: Teaching copyright and computer ethics in teacher education courses. *Contemporary Issues in Technology and Teacher Education* [Online serial], *1*(4). Retrieved July 1, 2006, from http://www.citejournal.org/vol1/iss4/currentpractice/article1.htm

TechWeb. (2006). Dictionary Main Page. Retrieved March 5, 2006, from http://www.techweb.com

Toffler, A. (1985). *The adaptive corporation*. New York: McGraw-Hill.

Tozer, J. (1997). *Leading initiatives: Leadership, teamwork and the bottom line*. Melbourne, Australia: Butterworth-Heinemann.

U.S. Department of Education. (2004). *Research and Statistics*. Retrieved February 25, 2004, from http://www.ed.gov

Virginia Board of Education. (2005). *Commonwealth of Virginia computer technology standards of learning for Virginia's public schools*. Retrieved February 22, 2006 from http://www.pen.k12.va.us/VDOE/Superintendent/Sols/compteck12.pdf

Virginia Department of Education. (2008a). *Enhancing Education Through Technology competitive grant.* Retrieved June 11, 2008, from http://www.doe.virginia.gov/VDOE/Technology/EdTech/consortia-map.pdf

Virginia Department of Education. (2008b). *Enhancing Education Through Technology Ed Tech Program.* Retrieved June 11, 2008 from http://www.doe.virginia.gov/VDOE/Technology/EdTech/consortiainfo.shtml

Virginia Department of Education, Office of Educational Technology. (2006a). *2003-2009 Educational Technology Plan for Virginia*. Author.

Virginia Department of Education, Office of Educational Technology. (2006b). *Guidelines and resources for Internet safety in schools*. Retrieved from http://www.doe.virginia.gov/VDOE/Technology

Virginia Department of Education, Office of Educational Technology. (2007). *Ideas for integrating Internet safety into the curriculum*. Retrieved June 11, 2008, from http://www.doe.virginia.gov/VDOE/Technology/ITRThandbook.pdf

Virginia Department of Education, Office of Educational Technology. (2008). *A handbook for Virginia's school divisions*. Retrieved June30, 2008 from http://www.doe.virginia.gov/VDOE/Technology/AUP/home.shtml

Virginia Department of Education, Superintendent's Memos. (2008). *Superintendent's memo on Virginia law and impact on schools and libraries*. Retrieved June 11, 2008, from http://www.doe.virginia.gov/info_centers/superintendents_memos/ 2008/03_mar/inf057.html

Virginia's Internet Safety Law. (2006). *Tech Law Journal*. Retrieved from http://www.techlawjournal.com/cong109/bills/house/ hr5319/hr5319ih.asp

Web Wise Kids. (n.d.). "Missing" game. Retrieved August 2, 2008, from http://www.webwisekids.org/our_software.asp

WhatIs. (2004). Dictionary Main Page. Retrieved March 5, 2004, from http://www.whatis.com

Wheatley, M. J., & Kellner-Rogers, M. (1998). Bringing life to organizational change. *Journal of Strategic Performance Management*.

Wikipedia. (n.d.). *The free encyclopedia*. Retrieved June 16, 2006, from http://www.wikipedia.org/

Willard, N. E. (2002). *Computer ethics, etiquette and safety: For the 21st-century student* (1st ed.). Eugene, OR: International Society for Technology in Education.

Wilson, D. (2005). Auburn University. *Black belt booklet.* Retrieved July 17, 2008, from http://www.auburn.edu/outreach/events/publications/bridgingthedivide.pdf

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2002). Close online relationships in a national sample of adolescents. *Journal of Adolescence*, *37*, 441-456.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003). Escaping or connecting? Characteristics of youth who form close online relationships. *Journal of Adolescence*, *26*, 105-119.

Young, K. S. (1998). *Caught in the net: How to recognize the signs of Internet addiction and a winning strategy for recovery*. New York: John Wiley & Sons, Inc.

CURRICULUM VITAE

James E. Lantzy was born in Barnesboro, Pennsylvania. He graduated from Bishop Carroll High School. He attended Saint Francis College in Loretto, Pennsylvania for both his Bachelor of Science degree and Master of Arts. He has been employed by the federal government since 1989 in varying elements of leadership.