

A Companion to the Augmented Technology Literacy Standards for Students

INTRODUCTION

The iKeepSafe Digital Citizenship C3 Matrix™ is designed to assist educators in integrating the concepts of cyber-safety, cyber-security, and cyber-ethics (C3) into existing technology and literacy standards and curricula. Based on the C3 Framework created by education and technology expert Davina Pruitt-Mentle, Ph.D., the C3 Matrix takes a holistic and comprehensive approach to preparing students for 21st century digital communication. Competency levels for C3 concepts are divided into three levels: basic, intermediate, and proficient.



Cyber-safety, Cyber-security, Cyber-ethics, (C3) Digital Literacy Skills

The vision guiding the iKeepSafe Digital Citizenship C3 Matrix springs from the vision of Eleanor Roosevelt and the ancient Greeks that the true purpose of education is to produce citizens. All students must have the awareness, knowledge, opportunity and resources to develop the C3 skills required for full participation as informed, responsible, ethical and productive citizens. The C3 Matrix provides educators with guidance regarding cyber-safety, security, and ethics principles that all students should know and be able to apply independently when using technology, technology systems, digital media and information technology, including the Internet.

Although C3 concepts are presented here as separate categories, they are not distinct and/or separable; they are, in fact, interrelated and should be considered as a whole. These principles should be embedded systemically throughout students' K-12 experience, not taught in isolation, and should be applied when meeting learning outcomes in the content areas. They can also be used as a companion and supplement to the various technology literacy standards for students created by ISTE, AASL, AECT, and others.

The three competency levels outlined in the C3 Matrix are not identified by

grade level; rather, they represent progressive levels of cognitive complexity at which youth should be expected to understand and practice. The levels were developed utilizing Bloom's *Taxonomy of Educational Objectives* (2001 revised edition), a hierarchy of six progressively complex cognitive processes that learners use to attain objectives or perform activities. Bloom's Taxonomy, the preferred system for articulating program objectives, categorizes cognitive skills by increasing order of complexity. From least to most complex these are: remembering, understanding, applying, analyzing, evaluating, implementing, and creating.

This taxonomy aids curriculum developers, policy makers and instructional designers in better defining the desired learning level of a target audience and then developing an appropriate design that will help the learner achieve desired learning goals. Additionally, this taxonomy aids in crafting behavioral assessment instruments.

What follows is a theoretical framework that can be used to inform a national, regional, or local agenda. It uses three dimensions, based on practical circumstances and experiences with educating students and teachers, with

input from multiple stakeholders including parents, students, educators, technology coordinators, media specialists, curriculum resource teachers, Internet safety experts, and industry security specialists. While C3 subject areas have common ground, they also have significant content that is distinct and important in discussing on an individual basis.

Cyber-safety

Cyber-safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviors protect personal information and reputation and include safe practices to minimize danger from behavioral-based, rather than hardware/software-based, problems.

Cyber-security

Whereas cyber-safety focuses on acting safely and responsibly, cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. Cyber-security is defined by HR 4246, Cyber Security Information Act (2000) as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist,

intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of the Internet, public or private telecommunications systems, or other similar conduct that violates federal, state, or international law, that harms interstate commerce of the US, or that threatens public health or safety." In contrast, most of the issues covered in cyber-safety are steps that one can take to avoid revealing information by "social" means.

Cyber-ethics

Cyber-ethics is the discipline of using appropriate and ethical behaviors and acknowledging moral duties and obligations pertaining to online environments and digital media.

Cyber-safety, security, and ethics cannot be stagnant, because technologies are dynamic and ever changing. For example, cyber-ethical issues are experiencing vast transformation as a result of factors driven by the multi-media aspects of cell phones and the immense reservoir of information on the Internet. It is essential that educators have tools for technology education that are also dynamic and evolving. The C3 Matrix provides these tools for teachers and administrators—and the students they teach.



CONTRIBUTORS

- Cable in the Classroom, Frank Gallagher
- Consortium for School Networking, Linda Sharp
- Educational Technology Policy, Research and Outreach (ETPRO), Dr Davina Pruitt-Mentle
- Florida Gulf Coast University, Dr Russell Sabella
- Harvard University, Center on Media and Child Health, Dr. David Bickham
- National Cyber Security Alliance
- Pennsylvania State University, Karl Sprenger
- Rochester's Institute of Technology, Dr. Samuel McQuade
- State Educational Technology Directors Association, Sarah Hall
- The iSchool at Drexel University College of Information Science and Technology, Dr. Belinda De Abreu
- Virginia State Board of Education, Dr. Tammy McGraw
- WoogiWorld, a Kid's Educational Virtual World, Scott Dow, CEO

© 2009 Internet Keep Safe Coalition. All rights reserved. This was developed copyrighted, and distributed for incidental, classroom and limited commercial sharing. Copies and reproductions of this content, in whole or in part, may be reproduced or transmitted for incidental, classroom use. Commercial copying is allowed provided that all copies/transmissions contain IKSC copyright language and distribution restrictions. Direct questions to: legal@iKeepSafe.org



HARVARD SCHOOL
OF PUBLIC HEALTH



C3 Framework Promoting Responsible Use

I. Cyber-Ethics

Students recognize and practice responsible and appropriate use while accessing, using, collaborating, and creating technology, technology systems, digital media and information technology. Students demonstrate an understanding of current ethical and legal standards, the rights and restrictions that govern technology, technology systems, digital media and information technology within the context of today's society. Students will:

- A. Understand and follow acceptable policies (school, home and community), and understand the personal and societal consequences of inappropriate use.
- B. Demonstrate and advocate for ethical and legal behaviors among peers, family, and community.
- C. Practice citing sources of text and digital information and make informed decisions about the most appropriate methods for avoiding plagiarism.
- D. Make ethical and legal decisions while using technology, technology systems, digital media and information technology when confronted with usage dilemmas.
- E. Exhibit responsibility and Netiquette when communicating digitally.
- F. Recognize the signs and emotional effects, the legal consequences and effective solutions for Cyberbullying.
- G. Recognize appropriate time and place to use digital tools, techniques and resources.
- H. Understand the importance of online identity management and monitoring. Advocate others to understand the importance of Online Reputation Management.

II. Cyber-Safety

Students practice safe strategies to protect themselves and promote positive physical and psychological well-being when using technology, technology systems, digital media and information technology including the Internet. Students will:

- A. Recognize online risks, to make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.
- B. Make informed decisions about appropriate protection methods and safe practices within a variety of situations.
- C. Demonstrate and advocate for safe behaviors among peers, family, and community.

III. Cyber-Security

Students practice secure strategies when using technology, technology systems, digital media and information technology that assure personal protection and help defend network security. Students will:

- A. Recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.
- B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.
- C. Demonstrate commitment to stay current on security issues, software and effective security practices.
- D. Advocate for secure practices and behaviors among peers, family, and community.

CYBER-SAFETY



Physical and Psychological Well-being:

Students practice safe strategies to protect themselves and promote positive physical and psychological well-being when using technology, technology systems, digital media and information technology, including the Internet.

BASIC	INTERMEDIATE	PROFICIENT
<p>A. Recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.</p> <ul style="list-style-type: none"> Recognize safety issues* related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). Use safe practices related to technology, technology systems, digital media and information technology including the Internet. Recognize and understand the purpose of protection measures (including filtering systems) for various types of technology, technology systems, digital media and information technology. 	<p>Safe and Responsible Practices</p> <ul style="list-style-type: none"> Recognize and discuss safety issues related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). Use safe practices and procedures related to technology, technology systems, digital media and information technology including the Internet. Explain the purpose of technology, technology systems, digital media and information technology protection measures. 	<p>Safe and Responsible Practices</p> <ul style="list-style-type: none"> Recognize and discuss safety issues related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). Use safe practices and procedures related to technology, technology systems, digital media and information technology including the Internet. Explain the purpose of technology, technology systems, digital media and information technology protection measures.
<p>B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.</p> <ul style="list-style-type: none"> Adhere to privacy and safety guidelines, policies, and procedures. Discuss the potential for addictive behaviors and the excessive use of technology and Internet. Describe procedures for exiting an inappropriate site. Describe procedures for reducing the chance of being a victim of cyber-bullying. Describe procedures for reporting cyber-bullying and other inappropriate behavior or content. 	<ul style="list-style-type: none"> Adhere to privacy and safety guidelines, policies, and procedures. Describe technology and Internet addictive behaviors. Describe procedures for exiting an inappropriate site. Describe procedures for reducing the chance of being a victim of cyber-bullying. Describe effective steps to manage and resolve a cyber-bullying situation. Model understanding about current safety needs. 	<ul style="list-style-type: none"> Adhere to privacy and safety guidelines, policies, and procedures. Describe and practice procedures for disciplining and productive Internet use (e.g., balance between time on and off the Internet). Describe and practice procedures for exiting an inappropriate site. Describe and practice procedures for reducing the chance of being a victim of cyber-bullying. Describe and practice effective steps to manage and resolve a cyber-bullying situation.
<p>C. Demonstrate and advocate for safe behaviors among peers, family, and community.</p>	<ul style="list-style-type: none"> Model personal safety within a variety of situations. 	<ul style="list-style-type: none"> Model personal safety within a variety of situations. Demonstrate commitment to stay current on safety issues and effective protection practices. Advocate for safe practices and behaviors among peers, family, and community.

* Safety issues could include but are not limited to: upload and download of objectionable content, cyber-bullying, reputation damage response to unwanted communications from businesses or predators, and Internet addiction

CYBER-SECURITY

Digital Security:

Practice secure strategies that assure personal protection and help defend network security.



BASIC	INTERMEDIATE	PROFICIENT
<p>A. Recognize security risks, make informed decisions, and take appropriate actions to protect themselves while using technology systems, digital media and information technology.</p> <p>Secure Practices</p> <ul style="list-style-type: none">Understand security risks and the potential harm of intrusive applications related to technology, technology systems, digital media, and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering).Understand effective basic security practices related to technology, technology systems, digital media and information technology including the Internet (e.g., strong passwords, protecting password and user ID, not disclosing important personal information, minimizing/evaluating pop up ads).Recognize and understand the purpose of technology, technology systems, digital media and information technology security protection measures.Discuss strategies for managing everyday hardware and software problems.	<p>B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.</p> <p>Secure Practices</p> <ul style="list-style-type: none">Understand and discuss security risks and the potential harm of intrusive applications related to technology, technology systems, digital media and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering).Describe and practice effective security practices, beyond the basic level, related to technology, technology systems, digital media and information technology including the Internet and critically evaluate digital resources.Recognize and understand the purpose of security protection measures for technology, technology systems, digital media and information technology.Model understanding about current security needs	<p>C. Demonstrate commitment to stay current on security issues, software and effective security practices.</p> <p>Secure Practices</p> <ul style="list-style-type: none">Understand and discuss security risks and the potential harm of intrusive applications related to technology, technology systems, digital media and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering).Practice effective security practices and analyze new options, beyond the intermediate level, related to technology, technology systems, digital media and information technology including the Internet and critically evaluate digital resources.Recognize and understand the purpose of security protection measures for technology, technology systems, digital media and information technology.Adhere to security guidelines, policies, and procedures.Use effective strategies for managing everyday hardware and software problems.Use effective strategies for securing wireless connections (e.g. connect to only legitimate wi-fi hot spots or turn off wi-fi, turn off file share mode, encrypt sensitive data/information, use and update anti-virus software, use a firewall, update operating system)Model secure practices within a variety of digital communities.
<p>D. Advocate for secure practices and behaviors among peers, family, and community.</p>		<ul style="list-style-type: none">Model secure practices within a variety of digital communities.Advocate for secure practices and behaviors among peers, family, and community.

CYBER-ETHICS



Legal and Ethical Issues:

Students recognize and practice responsible and appropriate use while accessing, using, collaborating, and creating technology, technology systems, digital media and information technology. Students demonstrate an understanding of current ethical and legal standards, rights and restrictions governing technology, technology systems, digital media and information technology within the context of today's society.

BASIC	INTERMEDIATE	PROFICIENT
<p>A. Understand and follow acceptable use policies (school, home and community), and understand the personal and societal consequences of inappropriate use.*</p> <p>B. Demonstrate and advocate for ethical and legal behaviors among peers, family, and community.</p>	<p>A. Understand and follow acceptable use policies (e.g., school, home, and community settings).</p> <p>Discuss basic issues related to responsible use of technology, technology systems, digital media and information technology, and describe personal consequences of inappropriate use*.</p> <p>B. Demonstrate and advocate for ethical and legal behaviors among peers, family, and community.</p>	<p>A. Understand and follow acceptable use policies (e.g., school, home, and community settings).</p> <p>Demonstrate responsible use of technology, technology systems, digital media and information technology in different settings (e.g., school, home, and community) and describe and analyze personal and societal consequences of inappropriate use*.</p> <p>B. Demonstrate and advocate for legal and ethical behaviors among peers, family, and community regarding responsible use of technology, technology systems, digital media and information technology dilemmas.</p>
<p>C. Practice citing sources of text and digital information and make informed decisions about the most appropriate methods for avoiding plagiarism.</p>	<p>C. Practice citing sources of text and digital information and make informed decisions about the most appropriate methods for avoiding plagiarism.</p>	<p>C. Understand and follow ethical standards of conduct (e.g., AUP, Student Handbooks, Student Code of Conduct, Honor Codes).</p> <p>Discuss definitions and basic concepts and issues related to plagiarism/electronic cheating and consequences of plagiarism.</p> <p>Demonstrate appropriate strategies for avoiding plagiarism (e.g., quoting, citing, acknowledging source and/or paraphrasing).</p> <p>Discuss the importance of respecting the rights of others regarding their work.</p>
		<p>A. Understand and follow ethical standards of conduct (e.g., school, home, and community settings).</p> <p>Demonstrate responsible use of technology, technology systems, digital media and information technology in different settings (e.g., school, home, and community) and describe and analyze personal and societal consequences of inappropriate use*.</p> <p>B. Demonstrate and advocate for legal and ethical behaviors among peers, family, and community regarding responsible use of technology, technology systems, digital media and information technology dilemmas.</p> <p>C. Understand and follow ethical standards of conduct (e.g., AUP, Student Handbooks, Student Code of Conduct, Honor Codes).</p> <p>Discuss definitions and basic concepts and issues related to plagiarism/electronic cheating and consequences of plagiarism.</p> <p>Practice citing sources of text and digital information.</p> <p>Determine and practice the use of appropriate strategies for avoiding plagiarism (e.g., quoting, citing, acknowledging source and/or paraphrasing).</p> <p>Demonstrate and advocate for ethical behaviors among peers, family, and community.</p>

* Inappropriate use could include, but is not limited to, viewing inappropriate content, using the school's network for non-educational purposes, or work networks for non-school/work related activities, posting incorrect/inaccurate information, hacking, participating in hate groups, harassing or sending/posting mean comments, sharing or downloading copyrighted materials/movies/music and/or making and sharing copies of copyrighted materials, etc.

CYBER-ETHICS

BASIC

- D. Make ethical and legal decisions when confronted with usage dilemmas while using technology, systems, digital media and information technology
- **Discuss definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use and file sharing.**
 - **Describe personal and societal consequences of respecting versus ignoring rights, laws and practices such as copyright, private/public domain, fair use, and file sharing.**
 - **Understand and follow school, home and community policies on access to information resources and adhere to local, state, and federal laws.**
 - **Demonstrate appropriate social and ethical behaviors when using technology and digital media including the recognition of intellectual property rights, fair use of copyrighted material, and legal file sharing or downloading of software, music and videos.**
 - **Make ethical and legal use of technology, technology systems, digital media and information technology when confronted with usage dilemmas**

INTERMEDIATE

- D. Make ethical and legal decisions when confronted with usage dilemmas while using technology, systems, digital media and information technology
- **Discuss definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use, and file sharing.**
 - **Describe personal and societal consequences of respecting versus ignoring rights, laws and practices such as copyright, private/public domain, fair use, and file sharing.**
 - **Understand and follow school, home and community policies on access to information resources and adhere to local, state, and federal laws.**
 - **Demonstrate appropriate social and ethical behaviors when using technology and digital media including the recognition of intellectual property rights, fair use of copyrighted material, and legal file sharing or downloading of software, music and videos.**
 - **Make ethical and legal use of technology, technology systems, digital media and information technology when confronted with usage dilemmas**

PROFICIENT

- D. Make ethical and legal decisions when confronted with usage dilemmas while using technology, systems, digital media and information technology
- **Discuss definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use, and file sharing.**
 - **Describe personal and societal consequences of respecting versus ignoring rights, laws and practices such as copyright, private/public domain, fair use, and file sharing.**
 - **Describe personal and societal consequences involving intellectual property rights, media copyright laws, private/public domain, fair use, and file sharing.**
 - **Understand and follow school, home and community policies on access to information resources and adhere to local, state, and federal laws.**
 - **Distinguish the legal implications between personal, educational, and commercial uses of protected works.**
 - **Demonstrate social and ethical behaviors when using technology and digital media regarding intellectual property recognition, fair use of copyrighted material, including file-sharing and pirating versus legal downloading of software, music and videos.**
 - **Make ethical and legal use of technology, technology systems, digital media and information technology when confronted with usage dilemmas.**
- E. Exhibit responsibility and netiquette (i.e. appropriate digital communication skills) when communicating digitally.
- **Recognize personal differences and practice etiquette within diverse situations.**
 - **Recognize positive and negative social and ethical behaviors when using technology and digital media and information technology.**
 - **Recognize positive and negative social and ethical behaviors when using technology and digital media and information technology.**
 - **Recognize personal differences and practice etiquette within diverse digital communities.**
 - **Recognize positive and negative social and ethical behaviors when using technology and digital media and information technology.**

CYBER-ETHICS

BASIC INTERMEDIATE PROFICIENT

<p>F. Recognize the signs, emotional effects, legal consequences of and effective solutions for cyber-bullying.</p> <ul style="list-style-type: none">Understand and discuss the signs and solutions for cyber-bullying.Recognize appropriate time and place to use digital tools, techniques, and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message).Apply proper communication skills when communicating digitally.	<p>G. Recognize appropriate time and place to use digital tools, techniques and resources.</p> <ul style="list-style-type: none">Demonstrate a thorough understanding of the signs, emotional effects, legal consequences of, and effective solutions for cyber-bullying.Recognize appropriate time and place to use digital tools, techniques, and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message)	<p>H. Understand the importance of online identity management (ORM). Advocate others to understand the Importance ORM.</p> <ul style="list-style-type: none">Demonstrate a thorough understanding of the signs, emotional effects, legal consequences of, and effective solutions for cyber-bullying.Make informed choices when confronted with cyber-bullying dilemmas.Recognize appropriate time and place to use digital tools, techniques and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message).Apply appropriate communication skills when communicating digitally.Practice digital etiquette to support collaborationAdvocate for proper netiquette behaviors among peers, family, and community.	<p>Understand the importance of online reputation management and monitoring (ORM).</p> <ul style="list-style-type: none">Understand that content posted to the web or sent through other digital means (e.g., cell phones, cameras) is accessible to a wide audience and can be permanently archived. <p>Understand the importance of online reputation management and monitoring (ORM).</p> <ul style="list-style-type: none">Understand that content posted to the web or sent through other digital means (e.g., cell phones, cameras) is accessible to a wide audience and can be permanently archived. <p>Understand the importance of online reputation management and monitoring (ORM).</p> <ul style="list-style-type: none">Understand the importance of online reputation management and monitoring (ORM).Recognize positive and negative uses of electronic postings as related to ORM.Demonstrate appropriate strategies for protecting, monitoring, and/or positively promoting personal identity (i.e. ORM).Analyze selected electronic media/postings and reflect, as an individual, on the appropriateness of each for effective ORM.
--	--	--	---

A U G M E N T E D

Technology Literacy Standards for Students

This graph is designed to help educators see how C3 concepts (cyber-safety, cyber-security, and cyber-ethics) can be integrated into existing standards. A teacher or technology coordinator may refer back to the C3 Matrix for ways to address safety, security, and ethics while teaching concepts from the national standards.

How content addresses:

- ISTE/NETS•S Standards
- AASL Standards for the 21st Century Learner
- AASL/AECT Information Literacy Standards for Student Learning
- iKeepSafe Digital Citizenship C3 Matrix
- 21st Century Framework.

Activity/Module:

* Completion of any activity does not certify competency in the identified area; however, it will contribute to development of the competency

ISTE/NETS•S Standard and Outcomes	Indicators	Addressed In this activity	EXAMPLE
1. Creativity & Innovation Students demonstrate creative thinking, construct knowledge, and develop innovative products & processes AASL 1.1.1, 1.2.1, 1.2.3., 2.1.1., 2.1.6., 2.2.4., 4.1.5., 4.1.8. AASL/AECT 1.3, 3.2, 3.3, 5.3, iKeepSafe C3 Matrix 21 st 1.1, 1.4, 2.4, 2.5, 3.1,	Students: <ul style="list-style-type: none"> a. apply existing knowledge to generate new ideas, products, or processes b. create original works as a means of personal or group expression c. use models and simulations to explore complex systems and issues d. identify trends and forecast possibilities. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2. Communication and Collaboration Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others. AASL 1.1.9, 1.3.2., 1.3.4., 2.1.4., 2.1.5., 2.2.4., 2.3.2, 3.1.1, 3.1.2., 3.1.4., 3.2.1., 3.2.3., 3.3.1., 3.3.2, 3.4.3, 4.2.1, 4.3.1, 4.4.4. AASL/AECT 3.4, 5.3, 9.1, 9.2, 9.3, 9.4, 7.1, C3 Conceptual Framework 21 st 1.2, 1.3, 3.1, 4.1, 4.2, 4.3, 8.1, 8.2, 10.1, 10.2, 10.3,	Students: <ul style="list-style-type: none"> a. Interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media. b. communicate information and ideas effectively to multiple audiences using a variety of media and formats. c. develop cultural understanding and global awareness by engaging with learners of other cultures. d. contribute to project teams to produce original works or solve problems. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3. Research and Information Fluency Students apply digital tools to gather, evaluate, and use information AASL 1.1.4, 1.1.5, 1.1.6., 1.1.7, 2.1.1., 2.1.2., 2.2.3., 2.2.4., 3.1.1, 3.1.4, 3.4.2., 4.1.6. AASL/AECT 1.2, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 3.1, 4.1, 4.2, 6.1, iKeepSafe C3 Matrix 21 st 2.4, 2.5, 5.1, 5.2, 6.3, 7.1, 7.2, 11.2, 12.3	Students: <ul style="list-style-type: none"> a. plan strategies to guide inquiry. b. locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media. c. evaluate and select information sources and digital tools based on the appropriateness to specific tasks. d. process data and report results. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<p>4. Critical Thinking, Problem Solving and Decision Making</p> <p>Students use critical thinking skills to plan & conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools & resources</p> <p>AASL 1.1.1, 1.1.3, 1.1.4., 1.2.2., 1.2.4, 1.3.2., 2.1.3, 3.1.4., 3.2.3., 3.3.4., 4.2.3. AASL/AECT 6.2, <i>iKeepSafe C3 Matrix</i> 21st 2.1, 2.2, 2.4, 2.5, 4.1, 4.2, 8.1, 8.2, 9.4, 9.5,</p>	<p>Students:</p> <ul style="list-style-type: none"> a. identify and define authentic problems and significant questions for investigation. b. plan and manage activities to develop a solution or complete a project. c. collect and analyze data to identify solutions and/or make informed decisions. d. use multiple processes and diverse perspectives to explore alternative solutions. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<p>5. Digital Citizenship</p> <p>Students understand human, cultural, and social issues related to technology & practice legal and ethical behavior</p> <p>AASL 1.3.1, 1.3.3., 1.3.5., 2.3.3., 3.1.6, 3.2.2, 3.3.7, 4.3.4., 4.4.3., 4.4.4., 4.4.5. AASL/AECT 8.1, 8.2, 8.3, 7.1, <i>C3 Conceptual Framework</i> 21st 4.1, 4.2, 4.3, 5.2, 6.2, 6.3, 7.2, 9.6, 10.1, 10.2, 10.3, 12.3</p>	<p>Students:</p> <ul style="list-style-type: none"> a. advocate and practice safe, legal, and responsible use of information and technology. b. exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity. c. demonstrate personal responsibility for lifelong learning. d. exhibit leadership for digital citizenship. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<p>6. Technology Operations & Concepts</p> <p>Students demonstrate a sound understanding of technology concepts, systems, and operations</p> <p>AASL 1.1.8., 2.1.4., 3.4.2. <i>C3 Conceptual Framework</i></p>	<p>Students:</p> <ul style="list-style-type: none"> a. understand and use technology systems. b. select and use applications effectively and productively. c. troubleshoot systems and applications. d. transfer current knowledge to learning of new technologies. 	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Correlation of the ISTE/NET•S & AASL/AECT, 21st Century Framework and C3 Matrix

AASL Addressed				AASL/AECT Addressed									ISTE/NET•S Standards	C3 Matrix			21 st Century Framework Addressed									
1	2	3	4	1	2	3	4	5	6	7	8	9		1	2	3	4	5	6	7	8	9	10	11	12	
X	X			X	X		X	X	X	X				Cyberethics												
X	X	X	X			X		X	X	X	X			Cybersafety												
X	X	X	X	X	X	X	X	X	X	X		Cybersecurity														
X	X	X												1. Creativity & Innovation	X		X	X	X							
X	X	X	X											2. Communication & Collaboration	X		X	X	X				X	X		
X	X	X	X	X	X	X	X	X	X	X				3. Research & Information Fluency	X		X	X	X	X	X	X	X	X		
X	X	X	X											4. Critical Thinking, Problem Solving and Decision Making	X		X	X					X	X		
X	X	X	X											5. Digital Citizenship	X			X	X	X	X	X	X	X		
														6. Technology Operations & Concepts	X											

© Internet Keep Safe Coalition 2009. All rights reserved. Educational Technology Policy, Research and Outreach. For information contact Davina Pruitt-Mentle, Ph.D. – (410) 531-3910 – dpruitt@umd.edu
 NETS-S –Educational Technology Standards and Performance Indicators for Students: http://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007.htm

AASL - <http://www.ala.org/ala/mgrps/divs/aasl/aaslprotools/learningstandards/standards.cfm>

AASL/AECT - http://www.ala.org/ala/mgrps/divs/aasl/aaslprotools/informationpower/informationliteracyStandards_final.pdf

Partnership for 21st Century Skills http://www.21stcenturyskills.org/index.php?itemld=120&id=254&option=com_content&task=view

Numerical ordering of skill/definitions are assigned for brevity within table format.

NETS for Students: National Educational Technology Standards for Students, Second Edition, © 2007, ISTE® (International Society for Technology in Education), www.iste.org. All rights reserved.