iKeepSafe℠ C3 MATRIX™ DIGITAL CITIZENSHIP

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

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). A taxonomy for learning, teaching and assessing: A revision of Bloom's Taxonomy of educational objectives: Complete edition, New York : Longman.

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.

cable in the classroom Kids. Cable. Learning.

cmch center on media and child health

PENNSTATE 1855

HARVARD SCHOOL OF PUBLIC HEALTH

Educational Technology Policy Research and Outreach Linking Research to Practice

VIRGINIA DEPARTMENT OF EDUCATION

CoSN ADVANCING K-12 TECHNOLOGY LEADERSHIP

STAYSAFEONLINE.org National Cyber Security Alliance

ROCHESTER INSTITUTE OF TECHNOLOGY R·I·T 1829

FLORIDA GULF COAST UNIVERSITY

The iSchool at Drexel

SETDA

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 polices (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.

C3 CYBER-SAFETY

iKeepSafe C3MATRIX DIGITAL CITIZENSHIP

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
A. Recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.	**Safe and Responsible Practices** • **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.	**Safe and Responsible Practices** • **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.	**Safe and Responsible Practices** • **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 and analyze the use of different protection measures for technology, technology systems, digital media and information technology.
B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.	• **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.	• **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.	• **Adhere** to privacy and safety guidelines, policies, and procedures. • **Describe** and **practice** procedures for disciplined 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.
C. Demonstrate and advocate for safe behaviors among peers, family, and community.		• **Model** personal safety within a variety of situations.	• **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.

C3 CYBER-SECURITY

iKeepSafe C3MATRIX DIGITAL CITIZENSHIP

Digital Security:

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

	BASIC	INTERMEDIATE	PROFICIENT
A. Recognize security risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.	**Secure Practices** • **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.	**Secure Practices** • **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. • **Recognize** and **understand** the purpose of security protection measures for technology, technology systems, digital media and information technology. • **Model** understanding about current security needs.	**Secure Practices** • **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.
B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.		• **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., connecy 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).	• **Adhere** to security guidelines, policies, and procedures. • **Describe** and **practice** strategies for managing everyday hardware and software problems. • **Describe** and **practice** 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.
C. Demonstrate commitment to stay current on security issues, software and effective security practices.		• **Model** secure practices within a variety of digital communities.	• **Model** secure practices within a variety of digital communities.
D. Advocate for secure practices and behaviors among peers, family, and community.			• **Advocate** for secure practices and behaviors among peers, family, and community.

C3 CYBER-ETHICS

iKeepSafe C3MATRIX DIGITAL CITIZENSHIP

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

* 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, bullying, participating in hate groups, harassing or sending/posting mean comments, hacking, illegally downloading copyrighted materials/movies/music and/or making and sharing copies of copyrighted materials, etc..

C3 CYBER-ETHICS

	BASIC	INTERMEDIATE	PROFICIENT
D. Make ethical and legal decisions when confronted with usage dilemmas while using technology, 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 verses 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.	• **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 verses 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.	• **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 verses 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. • **Demonstrate** and **advocate** for legal and ethical behaviors in this domain among peers, family, and community.
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** 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.	• **Recognize** personal differences and practice etiquette within diverse digital communities. • **Recognize** and **analyze** positive and negative social and ethical behaviors when using technology and digital media and information technology.

C3 CYBER-ETHICS

	BASIC	INTERMEDIATE	PROFICIENT
F. Recognize the signs, emotional effects, legal consequences of and effective solutions for cyber-bullying.	• **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.	• **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).	• **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 collaboration • **Advocate** for proper netiquette behaviors among peers, family, and community.
G. Recognize appropriate time and place to use digital tools, techniques and resources.	• **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.	• **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.	• **Understand** that content posted to the web or sent through other digital means (e.g., cell phones, cameras) are accessible to a wide audience and can be permanently archived.
H. Understand the importance of online identity management and monitoring (ORM). Advocate others to understand the importance ORM.	• **Understand** the importance of online reputation management and monitoring (ORM). • **Recognize** positive and negative uses of electronic postings as related to ORM	• **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- Online Reputation Management and monitoring (ORM).	• **Understand** the importance of online reputation management and monitoring (ORM). • **Recognize** positive and negative uses of electronic media/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 **21st 1.1, 1.4, 2.4, 2.5, 3.1,**	**Students:** **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.	☐ **Yes** ☐ **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 **21st 1.2, 1.3, 3.1, 4.1, 4.2, 4.3,8.1, 8.2,10.1, 10.2, 10.3,**	**Students**: 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.	☐ **Yes** ☐ **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 **21st 2.4, 2.5, 5.1, 5.2, 6.3, 7.1, 7.2, 11.2, 12.3**	**Students:** **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.	☐ **Yes** ☐ **No**	

4. Critical Thinking, Problem Solving and Decision Making Students use critical thinking skills to plan & conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools & resources **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,** iKeepSafe C3 Matrix **21st 2.1, 2.2,2.4, 2.5,4.1, 4.2,8.1, 8.2, 9.4, 9.5,**	**Students:** 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.	☐ **Yes** ☐ **No**	
5. Digital Citizenship Students understand human, cultural, and social issues related to technology & practice legal and ethical behavior **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,** C3 Conceptual Framework **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**	**Students:** **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.	☐ **Yes** ☐ **No**	
6. Technology Operations & Concepts Students demonstrate a sound understanding of technology concepts, systems, and operations **AASL 1.1.8., 2.1.4., 3.4.2.** C3 Conceptual Framework	**Students:** **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.	☐ **Yes** ☐ **No**	

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

AASL Addressed				AASL/AECT Addressed										C3 Matrix	21st Century Framework Addressed										
1	2	3	4	1	2	3	4	5	6	7	8	9	ISTE/NETS*S Standards	Cyberethics Cybersafety Cybersecurity	1	2	3	4	5	6	7	8	9	10	11	12
X	X		X	X		X		X	X	X			1. Creativity & Innovation	X	X	X	X										
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				3. Research & Information Fluency	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							X	X		5. Digital Citizenship	X				X	X	X	X		X	X			X
		X											6. Technology Operations & Concepts	X													

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/aaslproftools/learningstandards/standards.cfm
AASL/AECT - http://www.ala.org/ala/mgrps/divs/aasl/aaslproftools/informationpower/InformationLiteracyStandards_final.pdf
Partnership for 21st Century Skills http://www.21stcenturyskills.org/index.php?Itemid=120&id=254&option=com_content&task=view
Numerical ordering of skill/definitions are assigned for brevity within table format.