Using the STEPP Framework for C3 Education: Addressing the Social, Legal and Ethical Issues through a Systemic Holistic Approach

Davina Pruitt-Mentle, Ph.D.

STEPP: *Schools, Technology, Environment, and Plans and Policies*

ABETS: *Administrators, Behavioral Specialists, Educators, Technology Professionals, Stakeholders*

C3®: *Cyberethics, Cybersafety and Cybersecurity*

INTRODUCTION

Information technology has moved beyond a luxury solely for the business world, to become an integral part of the modern world; it is ubiquitous outside the formal classroom setting and is becoming a universal part of the K-12 environment. Technology clearly has brought a large number of positive effects to the educational community, including improved access to information, improved simulation capabilities, enhanced productivity, and a means to provide technology-based assistive support. In spite of these advances, technology has also brought challenges.

The power and possibilities that technology affords students comes with drawbacks when inappropriately used, whether such use is intentional or unintentional. Improving staff and student knowledge and awareness of Social, Legal and Ethical Issues—including Cyberethics, Cybersafety, and Cybersecurity (C3®)[1] concepts help provide them with the means to protect themselves, and enhance the safety and security of our national infrastructure. Nurturing a social, legal and ethical sensibility is every bit as important to our future as technology training. We need an integrated approach to develop a technologically-savvy workforce that understands the context and usage of digital communication as well as the nuts and bolts behind coding and functionality.

Past efforts in teacher education (both in-service and pre-service) have focused on teachers becoming knowledgeable about specific instructional technologies. Teacher technology training has been geared toward skills development, integration techniques and providing students with hands-on opportunities to use technology. However, this training has not been complemented by a similar national initiative on Social, Legal and Ethical content. Teaching someone to drive is dangerous, unless you also teach them the rules of the road.

[1] Cyberethics, Cybersafety and Cybersecurity, referred to as *C3®* is a Cyberawareness framework developed by Pruitt-Mentle, 2000. More about the development of the framework can be found in Appendix A. Other Terms and Acronyms can be found in Appendix B.

The call for a national focus impacting student and educator awareness and knowledge about these efforts has surged recently. State legislation has started to surface regarding Cybersafety awareness curricula (aka Internet safety) and cyberbullying. Schools are expanding their Acceptable Use Policies (AUP), PTA groups are hosting safety assemblies, and a plethora of Internet safety providers and industry stakeholders are engaged in awareness campaigns.

Substantial and sustainable impacts require an educational thrust using multiple means. Current efforts serve only as a bandaid, as most strategies are limited to policy statements in an AUP, signing a student code of conduct packet, or attending one or a handful of one-day assemblies. While better than nothing, decades of research show single-contact coverage, whether in the classroom or at one-time workshops for teachers, has little impact. Ongoing instruction is needed throughout the K-12 experience, starting early and continuing through high school. Middle school seems to be the end of many assembly programs on these topics. However, changes in technology, new methods to plagiarize, and new safety and security concerns require ongoing and ever-evolving education, for students, educators, and parents.

In order to address these issues, a comprehensive approach requires insight from multiple stakeholders. Similar to a School Improvement Team (SIT) or as part of the SIT, a C3 (cyber ethics, security and safety) team can function to support and enable a school environment committed to enhanced achievement for all students. A primary tenet of the C3 team or a sub-group of the School Improvement Team is a focus on school-based decision-making and participatory management where decisions are made at the local site by those performing the functions.

Despite the creation of school or school district Internet Safety Task Forces in some proactive communities, problems still arise. Cyberbullying through some survey accounts continues to be on the rise, stories of students logging in to teachers' accounts to change grades continue, concerns are voiced by parents of increasing accounts of Internet or online gaming addictions, and teachers continue to see plagiarism. Often an assigned "Internet Safety Teacher" or "Internet Safety Task Force Team" , pick and choose which C3 topics to focus on, and too often only talk about Cyberethics (e.g. plagiarism or cyberbullying). As shown through the National C3 Baseline[2] Study and the 2010 Follow-up Survey[3], Cybersafety and Cybersecurity topics are virtually ignored in the educational setting, with the exception of a narrow focus on predators. Additionally, often school policies and instruction are uncoordinated and do not include all C3 topics because state and local education agency standards use broad-stroke statements to guide curriculum and

[2] Pruitt-Mentle, D. (2008). The national cyberethics, cybersafety and cybersecurity baseline study. Educational Technology Policy, Research and Outreach. National Cyber Security Alliance.

[3] Pruitt-Mentle, D. and Pusey, P. (2010). *2010 State of K-12 cyberethics, cybersafety and cybersecurity curriculum in the U.S. survey.* Educational Technology Policy, Research and Outreach. National Cyber Security Alliance.

competency. Interpretations of these standards or guidelines have in some cases missed the mark related to C3 issues and how they correlate with human behavior. Ethics is intended to represent personal choice. Using the analogy of riding a bicycle, ethically we choose not to ride on our neighbors grass. Safety refers to safe practices, i.e. ride on the right side of the road, and obey traffic laws. Security refers to additional items we have to do, for example adjust gears and brakes. The first is a moral choice, the second is the way we behave, and the third requires further action, and each operates at a different cognitive level and therefore needs to be broached differently. Clearly there is overlap between each, however, the subject matter and instructional approaches needed are different and are important to address.

Teaching to a C3 framework, where Cyberethics, Cybersafety, and Cybersecurity content, to include topics regarding social, legal and ethical issues are taught as a whole, yet spotlighting each component's importance, provides the opportunity for more complete coverage. For example, one might need to learn security procedures to avoid having a computer vulnerable to an attack, as well as the ethical reasons not to hack into a computer to change grades. A separate focus gives rise to better appreciation of the appropriate uses of technology and does not lump the issues under a vague heading of Internet safety.

Additionally, programs often are not designed to support the "whole school". Content is narrowly focused on one to two specific topics of hot concern, arrived at in many cases by the assigned personnel's interest. Canned presentations or assembly in a box are often the mode of delivery. Yet, educators and parents still are unclear as to what the school is doing, what the school's goals and objectives are, how these goals are measured and what impact has been made. The thought comes to mind, "*How successful is our school in increasing educator and student knowledge and awareness about social, legal and ethical issues to ensure students become responsible electronic and Internet users and digital goodwill ambassadors, learning and implementing the character traits that encourage them to be good influences in their homes, schools, and communities*"?

The description of content education heard can be questioned when there are generic descriptions such as, "Oh, yes our school teaches "internet safety"… Cyberbullying is covered at the same time as Bullying Prevention… Everything students need to know is in the Districts Acceptable Use Policy… We go over the AUP at the beginning of the year". How can meaningful understanding and appropriate behavioral responses result from such simplistic approaches to these complicated subjects. Knowledge gained from years advocating for Cyberethics, Cybersafety and Cybersecurity Awareness, consultation with national Internet Safety curriculum providers, membership on local, state and national education panels, and serving on a variety of Technology Advisory Groups, has indicated a need to satisfy the common requests to make recommendations about what materials or curriculum would be "best" for their school to use or share with students/parents, or what topic would be best for presentation. This, of course is difficult to answer without additional exploration. You need to explore the school, the technology available, the environment of the school, and the plans and policies that are in place. From those thoughts, the idea of a system of strategies, the STEPP Framework emerged, to help schools identify their individualized needs.

BACKGROUND

The STEPP Framework is a tool that helps a school gather and organize information that can be used to guide collaborative decisions about strategies, programs and activities that foster students becoming responsible electronic and Internet users and digital goodwill ambassadors, learning and implementing the character traits that encourage them to be good influences in their homes, schools, and communities.

The STEPP framework was originally conceived in 2001, as part of a course activity requirement for educators enrolled in EDUC 473/698T, *Cyberethics, Cybersafety and Cybersecurity (C3) for Educators: Social, Legal and Ethical Implications for Classroom Technology*. The framework activity exercise was derived from a similar exercise that was used in another University of Maryland course; EDUC 477/698O, *Assistive Technology/Universal Design for the General Classroom Setting*. The STEPP Framework is based on Joy Zabala's well known and successful SETT framework, which was developed to support assistive technology selection and use in educational settings. SETT, an acronym for Student, Environments, Tasks and Tools, "is based on the premise that in order to develop an appropriate system of Tools (supports – devices, services, strategies, accommodations, modifications, etc.) teams must first develop a shared understanding of the student, the customary environments in which the student spends time, and the tasks that are required for the student to be able to do or learn to do to be an active participant in the teaching/learning processes that lead to educational success. When the needs, abilities, and interests of the Student, the details of the Environments, and the specific Tasks required of students in those environments are fully explored, teams are able to consider what needs to be included in a system of tools that is Student-centered, Environmentally useful, and Tasks focused" (Zabala, 2005)[4].

Similarly, the STEPP Framework helps multiple stakeholders gather and organize information to create a shared understanding of the school and its needs, and choose instructional methods and content that addresses the needs. In addition, the group provides support to the school's C3 plan as an effort within the larger School Improvement Plan.

How does STEPP fit within my School Improvement Plan?

Prevention is the key to the social, legal, safe, secure and ethical implications of technology in K12 schools. Research indicates that educators consider the technological issues related to ethics, safety and security the responsibility of the IT department and misplace confidence in the power of the technical interventions of filters and district firewalls (2008, National C3 Baseline Study, 2010 C3 Follow-Up Survey) However, cyberawareness strategies that include the ethical, safety and security implications for technology within and outside the school walls can positively affect district well-being and bottom line by preventing catastrophic incidents from occurring with the technology and students. Furthermore, by creating a cyberaware population, administrators contribute to the overall safety for our nation's infrastructure while creating employable students with the cyberskills that

[4] Zabala, J. S. (2005). Ready, SETT, go! Getting started with the SETT framework. Closing the Gap, 23(6)

are in high demand from employers. A caveat should be included for administrators with special needs populations including the disabled and low socioeconomic status. Some of these students have few opportunities to have cyberawareness modeled for them and it is incumbent on their educators to instill these 21st century skills to make them desirable for future employers.

What is the STEPP Framework?

The STEPP Framework serves as the lens to focus examination of the needs and to choose outcomes in C3 design. It consists of looking at the **S**chools, **T**echnology, and **E**nvironment, to assess needs, and then choosing the **P**lans and **P**olicies which meet the identified needs. The questions below form the start of the discussion, and can lead to other investigations and new questions within each construct.

The School

- What school level (elementary, middle, high, K-8)?
- Public or private
- Demographics
- Current concerns (district mandates, federal mandates, rise in cases of cyberbullying, community/parent concerns)
- Special needs (large population of low income students—lack of internet access, high percentage of ESL)

The Technology

- Support (available to both the student and the staff)
    - In School
    - Central school system support
    - System Admin and Instructional Technology Support
- Materials and Equipment (commonly used by others in the environments)
    - MAC/PC
    - Local Area Network/Wide Area Network
    - 1:1 Laptop Initiatives
    - Net books
    - Web 2.0 tools
- Access Issues (technological, physical, instructional)
    - Firewall
    - Filters
- Grades kept online/offline
- Who is responsible for security/passwords
- Responsibility for student access

The Environments

- Attitudes and Expectations (staff, family, other)
    - Technology integrated in classroom or separate topic
- Technology Savvy
    - Students
    - Teachers
    - Parents
- Arrangement (instructional, physical)
    - In Classroom
    - In Media Center
    - Home Use
- C3 topics already covered (ex. cyberbullying in bullying curriculum)

- C3 topic coverage-gap analysis
- Involved PTA
- Parent/Home/Student Access and support
- Support from Business
- For or against technology use
- Grants/funding Opportunities
- Content/Curriculum Available
- Parent/Business Connections/Opportunities

While the individual processes that a team uses to investigate these first pieces of the STEPP framework may vary by team, there are some critical elements and outcomes which must be included. Specifically:

- *Shared Fact Gathering and Knowledge:* Valid outcomes are chosen by a complete and shared knowledge of the factors which are used to guide decisions. Validity is based not on solitary knowledge, but knowledge based on information agreed to and shared across the STEPP team.
- *Teamwork:* Successful plans and policies are rarely designed by one person working alone. Instead, the support and collaboration of stakeholders results not only in more complete and robust solutions since they take on the knowledge of the whole, but they also result in better implemented solutions as collaboration results in the buy-in essential for effective implementation.
- *Communication:* Respectful communication results in the opinions of all being shared and integrated into the final results. Multiple stakeholders must be given the opportunity and the venue to share and collaborate with the entire team.
- *Multiple Perspectives:* A difficult but critical concept is to bring multiple perspectives to the solution. This can be challenging as different ideas can be difficult to meld together to create a solution. Professional viewpoints are not necessarily more important than the layman's views as it is the students' and educators' needs that must be satisfied, not the technology professional. Understanding the multiple perspectives of student, parents, educator and administrator can make the difference between success and failure.

The analysis portion of the STEPP Framework leads to the plans and policies required to deliver the chosen C3 outcomes to the individualized school. These include (but are not limited to):

The Plans

- Delivery
    - Assemblies
    - Units within specific subjects
    - Separate Curriculum
        - School/system design
        - Non-profit/commercial curriculum
- Professional Development to team/staff
- Network/security arrangements
    - Stand-alone
    - Network
- Topic gap analysis
- Plagiarism detectors
- Conferences/Seminars
    - for teachers

    - for Students
    - for Parents (PTA)
- Support for special needs/low socio-economic
- Strategies/processes (ex. AUP will be covered in class several times during the school year and at PTA meeting with parents; fun special events to highlight AUP policy items-school TV news, school newspaper, parent newsletter, part of Cybersecurity awareness month competitions)

The Policies

- Acceptable Use Policies (AUP) and Student Codes of Conduct (includes specific consequences for your school- also includes educator "next steps" for instances)
- Coverage of school/district AUP (similar to plans section above but policy crafted to confirm coverage)
- Honesty / Honor Code/Academic Integrity Agreements
- Filtering/firewall design (while some policies are standard within school districts, each school usually modifies depending on instructional needs)
- Password changing
- Responsible educators for C3 delivery
- C3 Committee or C3 SIT sub-committee
- Physical set up of computers to minimize opportunities to cheat/distractions/filter workarounds
- Instructional needs for specific student populations (AT needs considered for IEP process, extended time/lunch/after school access for assignments for students without technology access

Who should Complete the STEPP Framework?

The STEPP Framework forms a basis for which SIT Teams or other school or local school system groups to examine the needs of the school(s) under their purview. This can be a separate group, or a subcommittee to the SIT team. Most importantly, the makeup of the team must include multiple stakeholders to provide the multiple perspectives described above. As a guideline, remember ABETS: Administrators, Behavioral Specialists, Educators, Technology Professionals, and other Stakeholders.

- *Administrators:* As leaders of the schools and school systems, administrators are key to making sure policies are followed and plans are implemented. They also have insight into the available funding and an overall understanding of the environment and connection to school districts expectations. They include:
    - Principals
    - Assistant Principals
- *Behavioral Specialists:* Provide insight into student goals and behaviors and ensure plans and policies match methods of access and modes of thought of youth
    - Psychologists
    - Guidance Counselors
    - Special Educators
    - Nurses
    - School Security Officers
- *Educators:* Know the time constraints to integrate, availability within the curriculum and technology acumen and problems arising with students
    - Classroom Teachers
    - Media Specialists
    - Technology Specialists

- *Technology Professionals:* Provide the technical expertise regarding what can and what can't be done, best practices, and implementation support.
    - Network Engineers
    - IT Support
    - Business Professionals
    - Government Guidance
- *Other Stakeholders:* Key contributors to expectations, needs, and buy-in. It critical these persons understand why certain solutions are chosen, realize their input was considered and integrated into the solutions, and used for funding and technical support.
    - Students
    - Parents
    - Businesses who understand desired outcomes and new technology
    - Government

How is the STEPP Information used to Think About a Systemic Holistic Approach to Cyberawareness ?

The STEPP Framework strategies take the form of training, curriculum, policies, technology implementations, and tools that address the complete holistic picture within which students reside. It takes into account the views of stakeholders at various levels and thereby results in plans and policies that take into account multiple opinions. Implementation should be supported by all, as buy in is created from being part of the process. If done correctly, technology in the classroom should remain useful and productive, and C3 implementation should be effective and not intrusive. It is important that the leadership and decision makers take into account the input and advice of the STEPP team and do not build consensus through the process, and then destroy it via what is perceived as unilateral decision making. During implementation, some questions the team should monitor include

- Does technology continue to serve as an educational facilitator or has its use become too hampered by plans and policies to be effective?
- Are the plans and policies implementable?
- Do students end up with an understanding of C3 ideas and how it fits into school, home, work, and society? How about parents?
- Is this a school solution only that doesn't imply outside of school?
- How can I collect data on implementation and effectiveness?

STEPP Framework as a Process

The STEPP Framework is a process model intended to aid in School Improvement Planning to promote collaborative decision-making towards a Systemic Holistic Approach to Cyberawareness from awareness/prevention, detection, intervention to evaluation of effectiveness. The framework is not itself an outcome. It directs the thought processes and data gathering exercises to be completed while heading toward the completed plans and policies. Additionally, it is important that the STEPP Framework should not be viewed as a linear process that ends. Schools, Environments and Technology continuously change, and Plans and Policies must be modified to keep pace. A process such as this is not magic; it is only as good (or bad) as the people and information that drives it.

Processes are aided by a series of templates which serve as examples of the set of questions that need to be asked along the way, and outcomes that others have used successfully. The danger of using others plans and policies is that they may end up "wagging the dog." In other words, the data is constructed to match the plans, and not the

data is identified and then the plans are chosen. Thus, the user must be careful to follow the process and let the outcomes match the data. Available templates include:

- Standard VI Self-Rating Tool
- C3 Team STEPP Data Scaffold
- C3 Topic Gap Analysis