C3 Framework
Cyberethics, Cybersafety and Cybersecurity

Promoting Responsible Use

Davina Pruitt-Mentle, Ph.D.

Educational Technology Policy,
Research and Outreach

Email: dpruitt@umd.edu

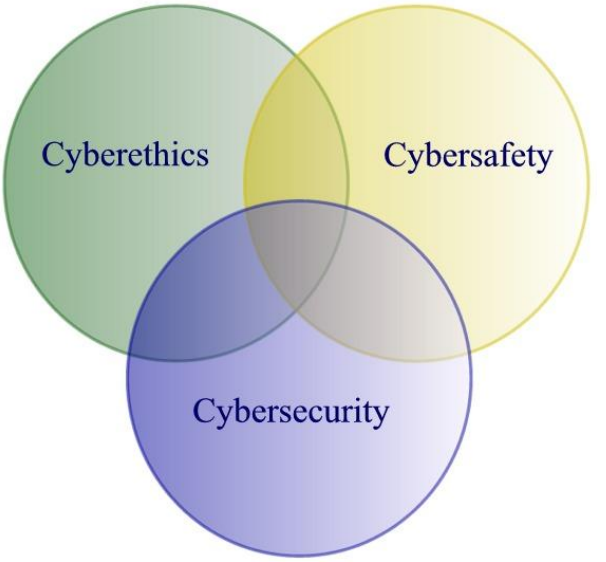
C3 Framework
Promoting Responsible Use

Promoting responsible use of technology is not a new phenomenon in education. It has been branded by a variety of stakeholders as *digital citizenship, cyberawareness,* and *cybercitizenship*. Existing strategies of instruction include detailing student, teacher, and administration standards and restrictions in Acceptable Use Policies and student handbooks. Additionally, IT departments have installed Internet filtering and blocking software within state and local education agencies to ensure students' safe and secure technology use. However, some argue that having rules in handbooks and blocking/filtering content is not equivalent to safe behavior instruction. Students need to understand the "why" behind the rules, and be able to institute best practices within their normal activities. Once students leave the school and are using unblocked open systems, they are left unprotected and are not able to make the distinction between safe and dangerous activities. Additionally, often school policies and instruction are uncoordinated and do not include all Cyberethics, Cybersafety, and Cybersecurity (C3) topics because state and local education agency standards use broad-stroke statements to guide curriculum and 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.

The Need for Developing a National Focus on C3

Many educational entities tend to pick and choose which C3 topics to teach, and often only talk about Cyberethics (e.g. plagiarism or cyberbullying). As revealed through survey findings[i], Cybersafety and Cybersecurity have been ignored in the past in the educational setting, with the possible exception of a narrow focus on predators and cyberbullying. Teaching to a C3 framework, where Cyberethics, Cybersafety, and Cybersecurity are taught as a whole, yet each having a unique focus, spotlighting the importance of each component, provides the opportunity for more complete coverage. Although clearly there is subject overlap (for example, one might need to learn security procedures to avoid having a computer vulnerable to an attack, and 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 negate the issues into one

C3 Framework:
Learning Areas For Policy Development



cloud labeled “Internet safety.” Analogously, automobile education is not one amorphous topic, but includes topics such as road rage (ethics), keeping tires inflated and following laws (safety), and alarms (security). By detailing particular elements under each domain, organizations can better design and address critical content. Teaching them as one, through branding such as digital citizenship or Internet safety curriculum makes it far too easy to check off the topic as “covered,” while only scratching the surface of individual domains.

The presence of a holistic policy framework can strengthen the already positive directions made by Internet safety providers, education entities and state attorney general offices. Adopting a policy framework adds the potential to broaden the impact on students, teachers, and parents in addressing ALL areas determined by government, business and industry, health agencies, and education to be of increasing importance. This C3 model was originally conceived in 2000, and has been embraced and adopted by the National Cyber Security Alliance, and several Internet safety providers and state educational agencies to guide the design of their policies, recommendations, and content.

The C3 theoretical framework can be used to inform a national, regional, or local agenda. Its three dimensions are 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 providers, and industry security specialists and serve as a basis for behavioral change. The logo with its overlapping rings of Cyberethics, Cybersafety, and Cybersecurity indicates the subject areas have common ground, but also have significant differences that must be discussed separately, including both subject matter and psychological differences. A brief synopsis of each area and associated topics are presented below.

Cyberethics is the discipline exploring appropriate and ethical behaviors, and the moral duties and obligations pertaining to online environments and digital media. It refers to choices about what is right and wrong in spite of the ability to do something. It includes plagiarism, bullying, and hacking to name a few.

Cybersafety describes the way you operate on-line. For example, only supplying personal information to known, on-line stores and staying away from sites that are not using https for transactions. Cybersafety includes keeping your personal information safe and limited on sites such as Facebook. Choosing varied and strong passwords to secure your information is also a good practice.

Cybersecurity refers to additional items you need to do on your computer to keep it secure from malicious people. This includes: installing virus software and firewalls, and updating them to keep up to date on new threats, and updating patches for your operating system and software on a regular basis to keep them secure.

Whereas Cyberethics focuses on the ability to act ethically and legally, Cybersafety addresses the ability to act in a safe and responsible manner on the Internet and in online environments. These behaviors can protect personal information and one’s reputation, and include safe practices to minimize danger— from behavioral-based rather than hardware/software-based problems.

Cybersecurity 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." Cybersecurity is defined to cover physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. In contrast, most of the issues covered in Cybersafety are steps that one can take to avoid revealing information by "social" means.

C3 Framework

1. **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.
2. **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.
3. **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.

About ETPRO

Educational Technology Policy, Research and Outreach, a research and development organization headquartered in Maryland, connects educational technology policy and research to instructional practice. ETPRO efforts draw from over two decades of experience in the educational community including more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and eleven years conducting educational technology policy analysis. ETPRO's understanding and insight into the fundamental gap between technology use and understanding of proper practices brought it to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3) initiatives.

---

i

---

[1] Pruitt-Mentle, D. (2000). The C3 Framework: Cyberethics, cybersafety and cybersecurity implications for the educational setting. C3 is a trademark registered with ETPRO. Materials can be used for educational and non-profit use. For other uses, contact Davina Pruitt-Mentle, dpruitt@umd.edu.

[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.