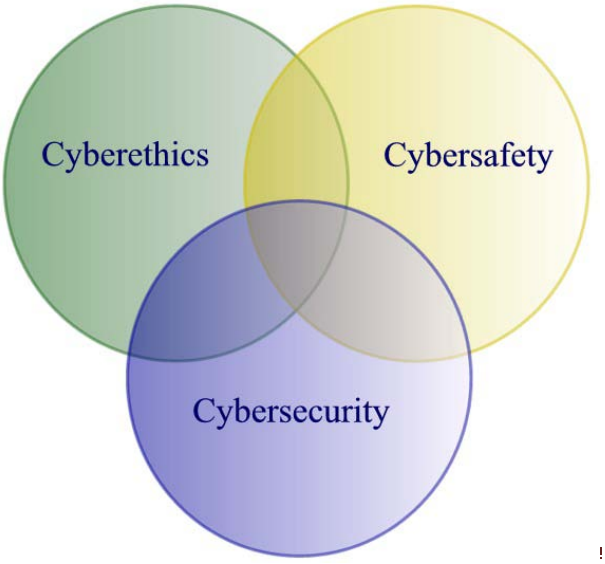
C3 Framework
Promoting Responsible Use

Promoting socially and ethically 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, Cybersafety and Cybersecurity are virtually ignored in the educational setting, with the possible exception of a narrow focus on predators. 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.

C3 Framework:
Learning Areas For Policy Development



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 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.