# Cyberethics, Safety and Security (C3®) Literacy Skills

## A Companion to the Augmented Technology Literacy Standards for Students

The vision guiding this document is that all students must have the awareness, knowledge, opportunities and resources to develop the C3® skills they need to pursue life's goals and to participate fully as informed responsible, ethical and productive members of society. This C3® framework is intended to provide guidance regarding Cyberethics, safety and security principles all students should know and be able to apply responsibility and independently when using technology, technology systems, digital media and information technology including the internet.

Although this document presents these principles within separated categories, we want to emphasize that they are not distinct and separable; they are, in fact, interrelated and should be considered as a whole. These principles are not meant to be taught in isolation but should be embedded systemically throughout the students' K-12 experience, and applied when meeting learning outcomes in the content areas. They can also be used as a companion and supplement to the various National Technology Literacy Standards for Students created by ISTE, AASL, AECT and others.

The various levels (basic, intermediate and proficient) are not identified by grade level. Instead, they represent progressive levels of cognitive complexity at which youth should be expected to understand and practice. The levels are developed utilizing Bloom's revised Taxonomy of Educational Objectives (2001), a hierarchy of six progressively complex cognitive processes 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, and creating.

This taxonomy aids educators, 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 providers, and industry security specialists. C3® subject areas have common ground, but have significant content that is distinct and important in discussing on an individual basis.

**Cyberethics** is the discipline dealing with what are appropriate and ethical behaviors, and with moral duties and obligations pertaining to online environments and digital media.

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.

The topics listed above cannot be stagnant. Technologies are dynamic and ever changing. For example, cyberethical issues are experiencing vast transformation as a result of factors driven by the multi-media aspects of cell phones and the vast reservoir of information on the Internet.

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.

# **C3**® Framework
# Promoting Responsible Use

## I. CyberEthics

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.

## II. CyberSafety

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.

## II. CyberSecurity

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.