Chapter 6
Intentionally Secure:
Teaching Students to Become Responsible and Ethical Users

Judith L. Lewandowski
Purdue University, USA

ABSTRACT

This chapter focuses upon the need to intentionally incorporate the principles of digital citizenship as an integrated curriculum element. Specifically, the infusion of information security and cyberethics principles should occur at the same time and rate as the use of technology within the educational setting. Through the development of a universal curriculum set, the author provides a content list and sample strategies for making these issues a natural part of the curricular goals of these courses.

INTRODUCTION

In the past, the term "technical literacy" referred to basic computer skills and functionality that enabled an individual to work with an application or specific software package. As the use of technology in our society has evolved, it's important that schools follow a similar pattern of adaptation. Educational environments need to become increasingly flexible, adaptable, and willing to anticipate the needs of students who will be using technology that is not yet in existence (Festa, 2007). Likewise, instructors and teachers need to also expand their skill set to reflect the changing nature of technology. In addition to the basic curricular skills that an educator must teach, they now must also be enabled to prepare their students to successfully navigate the digital world in ways that go far beyond clicking a mouse or creating a presentation. It's a daunting task to consider, but it is critical to address.

DOI: 10.4018/978-1-5225-5933-7.ch006

According to *21st Century Skills: Literacy in the Digital Age*, students need to become literate in a variety of areas. Specifically, "Digital Age Literacy" is broken down into a variety of types of skills including: Technological Literacy, Visual Literacy, and Information Literacy. These are critical skills that require students to become knowledgeable on how to use technology in an effective manner, use media to create products that advance thinking, and evaluate, locate, and synthesize information through the use of technology (NCREL, 2003).

Technological literacy is defined as the ability to appropriately select and responsibly use technology (Blake, 2017). Included within this definition are the skills needed to be able to expose knowledge, decode content, employ information, apply ethical standards, and evaluate the validity of data.

With the infusion of ubiquitous technology throughout education at all levels, information security skills and the principles of cyberethics are taking on ever greater importance especially in novice users of technology. When schools give young students access to advanced technology, they must also provide a clear set of guidelines to demonstrate appropriate use. As argued by Niekerk, Reid, and Thomson (2013), teaching cyber security from an early age is the best possible way of improving its awareness among the public. In order to make this happen, instructors and students need an understanding of such issues as the protection of data, programs, and information stored on disks, networks, hard drives, etc., as well as the issues of privacy, ethics, and copyright protection. By intentionally infusing the principles of digital citizenship (information security and cyberethics) into daily practice, educators at all levels can positively impact learner engagement and understanding.

Based upon the recommendations of experts in the field, this chapter will provide you with a set of strategies to develop information security and cyberethics awareness within courses that teach, utilize, and advocate for technology integration.

EXPANDING TECHNICAL LITERACY: RESPONSIBLE USE AND AWARENESS

Technology access for children occurs at an earlier point and at a faster rate than ever before (Anderson, 2016). However, access to technology does not does not indicate that these young users know how to use it responsibly or how to protect themselves from online dangers (Dutt-Doner, et. al, 2006). Increasingly, young adults and adolescents are both the "victims and perpetrators of crime and abuse enabled by information technology" in the areas of academic dishonesty, copyright issues, software piracy, online threats, fraud, sexual misconduct, and the creation and distribution of malicious code (McQuade, 2007, B29).