

Course: Cyber Citizenship  
PEIMS Code: N1260001  
Abbreviation: CYBERC  
Grade Level(s): 9-12  
Number of Credits: 0.5

*Course description:*

Today's student's main means of communication is cyber-based. Studies show that 95 percent of all teens are now online with an average of ten hours and forty-five minutes spent online daily. (<http://kff.org/disparities-policy/press-release/daily-media-use-among-children-and-teens-up-dramatically-from-five-years-ago/>; <http://www.pewinternet.org/fact-sheets/teens-fact-sheet/>) The evolution of technology has taken issues that were once overt and visible in the classroom to the abstract world of online communication.

This course will educate students regarding evolving platforms of social media and familiarize them with their use. It will highlight the controversial issues associated with social media, including the laws regarding social media, inappropriate usage, and online harassment. Overall, this course will educate students in maintaining a responsible online digital footprint. Activities in this course include the analysis and application of various forms of social media platforms, a study of laws concerning online aggression and safety, and the use of learned technology that will further engage students in academics.

*Essential knowledge and skills:*

(a) Introduction

- (1) Cyber Citizenship will address social media platforms such as Facebook, Twitter, Instagram, Snapchat, LinkedIn, and Tumblr. Students will learn appropriate online anonymity and cyber safety, in addition to the mechanics associated with the various platforms.
- (2) Students will learn to make informed decisions using digital tools and appropriate applications. By using online research and information resources such as journals, newspapers, or authoritative databases, students will synthesize knowledge and create solutions that exhibit digital leadership.
- (3) Cyber Citizenship will prepare students for the societal demands of increased use of online technology through communication and collaboration, critical thinking, problem solving and decision making as well as promote positive digital citizenship. Students will be expected to exhibit a positive attitude toward using technology that supports collaboration, learning,

and productivity. Students must demonstrate personal responsibility and exhibit leadership for digital citizenship. The goal of the process is to provide students an authentic platform to demonstrate effective application of digital applications with an ability to identify and resolve cyber conflict among their peers.

(4) Students will acquire a knowledge of the significance of their digital footprint while learning to take control of their personal online identity, and to demonstrate responsibility for a life-long positive online reputation.

(b) Knowledge and Skills

- (1) The student evaluates the benefits and risks of sharing information online. The student is expected to:
  - (A) identify and demonstrate online behaviors that reflect negative risks shared online such as cyber-bullying, sexting, stalking and harassing;
  - (B) demonstrate an understanding of ethical responsibilities of online usage;
  - (C) identify and list the benefits of healthy and safe online usage;
  - (D) research current cyber issues in the media; and
  - (E) generate and demonstrate positive solutions to current cyber issues.
- (2) The student demonstrates an understanding of their digital footprint in both a positive and negative context. The student is expected to:
  - (A) identify and understand the application and use of various social media platforms;
  - (B) demonstrate appropriate behaviors and risks associated with each platform;
  - (C) create appropriate online content for each of the major platforms;
  - (D) demonstrate the use of embedded features that mitigate risk in each platform; and
  - (E) make decisions based on a variety of interactions via their social media platforms.
- (3) The student applies an understanding of online safety within cyber platforms. The student is expected to:
  - (A) analyze the student's current online behaviors;
  - (B) recognize and demonstrate defensive online behaviors to prevent exploitation;
  - (C) identify methods of protecting one's online security and identify;
  - (D) examine the negative effects and consequences of sharing personal information online; and
  - (E) acknowledge the importance of never sharing one's location on the Internet.

- (4) The student understands the importance of cyber laws and the ramifications of the student's online behavior in relation to those laws. The student is expected to:
  - (A) identify cyber laws and how they vary from state to state;
  - (B) identify the nature of and understand penalties associated with violations of cyber laws, citing recent court cases;
  - (C) collaborate with local city or town authorities to demonstrate the need for cyber laws to be approved and maintained;
  - (D) recognize the importance of protecting one's passwords by securing accounts and acquiring knowledge regarding the different types of authentication; and
  - (E) identify the risks associated with sharing location services through Internet and social media applications and take appropriate steps to mitigate un intended sharing of location.
- (5) The student evaluates leadership qualities and the transfer of those qualities from the cyber world to face-to-face interaction. The student is expected to:
  - (A) identify and demonstrate behavioral strategies that enable the student to face the pressures of today's media-driven society;
  - (B) explain practical ways to balance social media with the student's daily life;
  - (C) comprehend social media's effect on human interaction; and
  - (D) recognize the importance of mentorship and appropriate cyber usage in helping the student reach goals.
- (6) The student identifies spam and phishing in order to keep private information protected online. The student is expected to:
  - (A) navigate and enable filters on their email programs;
  - (B) identify the characteristics and signs of a dangerous or unsecure website;
  - (C) discuss the importance of virus protection software;
  - (D) compare and contrast various anti-viral software;
  - (E) investigate the processes to file a claim to a legitimate source of guidance and protection, such as the federal trade commission, against an online identity thief; and
  - (F) understand the importance of website certificates as indicators of an authenticated website.
- (7) The student exhibits behaviors that protect the student from cybercrime. The student is expected to:
  - (A) demonstrate knowledge of how to protect online accounts by researching online security measures beyond passwords;

- (B) activate and employ a firewall in order to maintain safety from cybercriminals;
  - (C) identify behaviors to protect one's self from cybercrimes such as hacking, theft, cyberstalking, and identify theft;
  - (D) describe appropriate behaviors for encountering public wireless internet access such as refraining from using public internet for sensitive information, personal banking, and confidential correspondence;
  - (E) demonstrate knowledge of the two-step verification process in order to prevent cybercriminals from using a stolen password; and
  - (F) research the process of reporting fraudulent activity with local law enforcement agency in the case of compromised identity.
- (8) The student maintains the safety of their data by avoiding data loss. The student is expected to:
- (A) identify various ways data can be lost or corrupted, such as computer malfunctions, theft, viruses, spyware, accidental deletion, and natural disasters;
  - (B) perform the three-step process for data back-up, including making copies of data, selecting the hardware or method to store data, and safely storing the backup device;
  - (C) locate and describe the functions of links to backup utilities in various operating systems; and
  - (D) analyze the various options of external and internal hardware available to save and store data.

*Description of specific student needs this course is designed to meet:*

Equip students with the skills and resources to treat each other respectfully when they use cyber technologies, and empower students with the skills to use cyber technologies to embrace a successful future.

*Major resources and materials:*

These resources are recommended but not limited to Journals, databases, social media outlets, blogs, and experts in the fields of social media, health and technology.

<https://www.common sense media.org/educators/cyberbullying-toolkit>

Common Sense Education provides informative classroom material for the classroom. Videos, discussion guides, and presentations that bring engagement among students. Cyberbullying Toolkit – Standing up, Not Standing by is one example of how Common Sense fits within Cyber Citizenship.

**Cyberbullying Prevention and Response: Expert Perspectives:** edited by Justin W. Patchin, Sameer Hinduja

<http://cyberbullying.us/tag/cyberbullying-research/>

This document is a nine-page summary – filled with as much useful information as possible – to equip educators and parents to spot cyberbullying, respond to it appropriately and meaningfully, and to prevent its future occurrence among the children and teenagers they care for.

*Suggested course activities:*

Engage in virtual social media applications enabling them to learn cyber safety as well as positive digital leadership. Students must make decisions based on a variety of interactions via their social media platforms. The decision outcome will reflect a possible point based end result for a particular task. Students will also learn safety measures and consequences through guest expert's lectures in the field of cyber safety.

Sample Activity – Each class will use a virtual social media account created by the teacher. Students will be given tasks that will confront them with real life scenarios each student must respond to. An example might be receiving a friend request from a “stranger” who claims to attend their school and/or a task to create a post that meets the requirements of the particular assignment.

Activity – Students will create a cyber safety assembly for their school. Each class contributes to a section of a 30-minute assembly to be taken place toward the end of the school year. Peer-to-peer education results in a positive outcome.

*Suggested methods for evaluating student outcomes:*

Rubrics, participation and group discussions are standard methods for evaluating student outcomes. Within this course the activities suggested below will not only engage students, but will also provide a direct impact on the entire school.

Daily, the students will be required to create an example of a social media post with guidelines for students to follow. These postings could be written in a journal format that allows students to visualize a positive timeline of their “posts” throughout the course.

Weekly role playing activities provide students with hands on social media practice skills. Students are given a situation based on social media topics discussed in class. Students must work in groups to formulate the most appropriate response and present/role play their solution to the class.

Throughout the course, each class will be required to brainstorm and develop an impactful method of teaching the rest of the student body about cyber-citizenship. Ideally, each school will celebrate Cyber Citizenship Week. During this week the students will execute their plan of action demonstrating positive cyber citizenship and education to the student body.

Example: Each student will interview ten students outside their class with previously chosen questions regarding their online usage. The class will compile the data and create posters and other visual media



that will demonstrate their school's online statistics during Cyber Citizenship Week. A student chosen from the class will read one of the statistics each day over the morning/afternoon announcements.

*Teacher qualifications:*

Technology Applications Certified Educator  
§231.253 Technology Applications, Grades 9-12

*Additional information:*

This curriculum will establish a schoolwide climate that is conducive to positive interactions among students. This course has the potential to prove that schoolwide efforts are more effective in addressing online aggression and safety than classroom components alone. This course has the potential to encourage students to spread the message of maintaining a positive digital footprint amongst their peers, thus creating a school-wide atmosphere that is inclusive, responsible, and conflict-free.

Course created by:  
*Lauren Galley, President*  
*Girls Above Society*  
<http://www.girlsabovesociety.org>