The New York Center for Teacher Development, Inc.

In affiliation with the University of Massachusetts Global (Extended Education)

Course Syllabus

Course:	**EDZU 9123**	**Teaching Cybersecurity & Digital Citizenship in a Connected World**
Credit Hours:	3.0 credits / 45 hours	
Instructor:	**Michele Milgrim**	

Course Description

In today's hyperconnected classrooms, students need more than tech skills—they need guidance on how to be responsible digital citizens. This course helps K-12 educators build confidence teaching cybersecurity and online ethics across grade levels and subjects.

Participants will explore real-world tools and strategies for improving student awareness around digital privacy, online safety, social media boundaries, and ethical tech use. Educators will leave with a student-ready mini-lesson, a cybersecurity toolkit, and a tailored implementation plan.

Course Goals

To Know

1. Key concepts in cybersecurity, including password management, phishing awareness, and personal data protection
2. The foundational elements of digital citizenship as defined by ISTE and NY State standards
3. Legal policies and privacy regulations relevant to K–12 education (e.g., FERPA, COPPA, CIPA)

To Understand

1. The educator's role in shaping students' online behavior and digital ethics
2. How social-emotional learning intersects with digital safety and well-being
3. Developmental and cultural considerations when teaching digital topics across grade bands

and To Be Able To

1. Design and deliver a classroom-ready mini-lesson on cybersecurity or digital citizenship
2. Create tailored student-facing resources that promote responsible tech use
3. Advocate for digital safety within their school community through policy, outreach, or curriculum design

Course Outline

I. The Digital Landscape & Citizenship: Understanding Educators' Role in Online Culture

A. Introductions and framing: What does "digital citizenship" mean today?
B. Define digital citizenship using current frameworks and models
C. Examine the educator's role in shaping students' online behavior
D. Review ISTE and NYS standards related to technology and citizenship education
E. Case study comparison: How do students behave online across different contexts?
F. Reflect on your school's current approach to digital citizenship
G. Micro-discussion: What does "citizenship" mean to Gen Z?
H. Draft a personal vision statement for integrating digital citizenship into your classroom

II. Cybersecurity Basics for Educators: Building Awareness and Habits for Digital Safety

A. Introductions and framing: Why cybersecurity matters in education
B. Define key cybersecurity concepts: passwords, phishing, privacy tools
C. Explore best practices for data security in educational settings (including NY Ed-2D compliance)
D. Case examples: How schools respond to cybersecurity threats
E. Simulation activity: Practice identifying phishing attempts
F. Develop a checklist of cyber hygiene habits for students
G. Create a Classroom Cyber Hygiene Toolkit to support student safety

III. Online Ethics, Safety, and SEL: Cultivating Empathy and Responsibility in Digital Spaces

A. Introductions and framing: What does emotional intelligence look like online?
B. Define key concepts: digital empathy, cyberbullying, and ethical online behavior
C. Examine the role of social-emotional learning (SEL) in digital environments
D. Explore challenges around classroom social media use and guidelines
E. Discuss ethical dilemmas in online learning environments
F. Co-create classroom norms for respectful and safe online interactions
G. Draft a Digital Citizenship Contract and SEL-infused lesson for classroom use.

IV. Teaching Students to Be Safe Online: Developmental Approaches to Digital Empowerment

A. Introductions and framing: What does "online safety" mean across grade levels?
B. Define developmental considerations for teaching digital safety from K–12
C. Explore strategies for empowering students as peer mentors in digital spaces
D. Examine culturally responsive approaches to online safety instruction
E. Design a mini-lesson tailored to a specific age group or classroom context
F. Engage in peer feedback forums to refine lesson plans
G. Finalize a ready-to-teach digital safety lesson and resource list for classroom use

V. Policy, Legal Issues, and Capstone: Designing for Compliance, Communication, and Curriculum Integration

A. Introductions and framing: Why do tech policies matter in classroom practice?
B. Define key legal frameworks: FERPA, COPPA, and CIPA in the NYS context
C. Explore how privacy laws shape curriculum design and instructional choices

D. Examine strategies for gaining administrative support and engaging families
E. Annotate curated readings to deepen understanding of tech-related policies
F. Participate in final peer discussion to refine unit planning ideas
G. Develop a Cybersecurity & Digital Citizenship Unit Plan tailored to a specific grade

Methods of Instruction

Educators enrolled in this course will actively engage with digital citizenship and cybersecurity concepts through structured readings, weekly discussions, and reflective writing. Throughout the course, participants will explore strategies for fostering safe, ethical, and developmentally appropriate online behavior in K–12 settings. They will collaborate in peer forums, analyze real-world scenarios, and examine current policies and practices to deepen their understanding. Assignments will guide participants in applying course concepts to their own teaching routines, encouraging thoughtful integration of digital safety and citizenship into classroom instruction. Participants will reflect on their learning, document their instructional planning, and set goals for implementing digital citizenship practices that support student well-being and responsible technology use.

Students will connect with each other throughout the course within forums and various other types of online feedback options built into each class.

Methods of Assessment

In order to earn an A in the course, a student must complete all assigned readings, weekly assignments, and participate in all discussion forums. The student must also submit a full digital citizenship and cybersecurity unit or lesson plan for a selected grade band (K–2, 3–5, 6–8, or 9–12).

In order to earn a B in the course, a student must complete all of the assigned readings, assignments, and participate in all discussion forums.

Instructors are online each day of the course and correspond with students through the course itself, feedback on assignments, and e-mail.

Time Validation

Task / Assignment Description	Time (in hours)
Case study analysis: comparing student behaviors online: Students will read two case studies on online student behavior and write a 2–3 page analysis comparing engagement, participation, and outcomes. They'll draw on course readings and personal experience to reflect on implications for their own teaching.	2.00
Short reflection on your school's current approach: Students will write a short reflection on their school's current approach to family engagement, communication, or digital safety. They'll consider strengths, areas for growth, and how their school's practices align with course themes.	2.00
Micro-discussion: What "citizenship" means to Gen Z: Students will participate in a micro-discussion exploring how Gen Z defines and expresses digital citizenship, drawing	2.00

on course readings and personal observations. They'll respond to a prompt in the discussion forum and engage with at least two peers' posts to deepen the conversation.	
Build a draft vision statement for digital citizenship integration in your classroom: Students will draft a personal vision statement for integrating digital citizenship into their classroom, reflecting on course themes and their school's current practices. They will outline their goals, guiding values, and potential strategies for implementation.	3.00
Interactive simulation: spotting phishing emails: Students will complete an interactive simulation designed to help them identify common features of phishing emails and practice safe digital habits. After engaging with the simulation, they will submit a brief reflection on what they learned and how they might apply it in their school setting.	3.00
Create a checklist of security habits for your students: Students will create a practical checklist of digital security habits tailored to their students' age group and learning environment. The checklist should reflect key concepts from the course and include brief explanations for each habit.	3.00
Classroom Cyber Hygiene Toolkit for student use: Students will design a Cyber Hygiene Toolkit that includes practical tips, routines, and reminders to help their students maintain safe digital practices in the classroom. The toolkit should be age-appropriate, visually clear, and grounded in course concepts.	3.00
Discussion: ethical dilemmas in online learning: Students will participate in a discussion exploring ethical dilemmas in online learning, such as privacy, equity, and academic integrity. They will respond to a prompt and engage with at least two peers' posts to share perspectives and deepen understanding.	3.00
Create classroom norms for online interactions: Students will develop a set of classroom norms to guide respectful and productive online interactions among their students. The norms should reflect course principles and be tailored to the age group and learning environment they teach.	3.00
Digital Citizenship Contract & SEL lesson draft: Students will create a draft Digital Citizenship Contract for their classroom, paired with a short SEL-focused lesson that reinforces responsible online behavior. The contract should outline clear expectations, and the lesson should include an activity or discussion prompt to support student understanding.	3.00
Create a mini-lesson tailored to a grade level: Students will design a mini-lesson on digital citizenship tailored to a specific grade level, incorporating age-appropriate language, activities, and learning goals. The lesson should include a brief outline, key discussion points, and one interactive element to engage students.	3.00
Peer feedback forums: Students will participate in peer feedback forums where they will share a draft assignment and provide constructive responses to at least two classmates. Feedback should focus on clarity, relevance, and alignment with course goals.	3.00
Ready-to-teach lesson plan and resource list: Students will submit a ready-to-teach lesson plan on a digital citizenship topic, complete with learning objectives, instructional steps, and a resource list. The plan should be classroom-ready and reflect key concepts from the course.	3.00
Curated reading + policy annotation: Students will curate a short list of readings related to digital citizenship and annotate a school or district policy that connects to those themes. Annotations should highlight key language, implications for classroom practice, and areas for improvement.	3.00
Final peer discussion: Students will participate in a final peer discussion where they reflect on key takeaways from the course and share how they plan to apply digital	3.00

citizenship concepts in their own teaching. They will respond to a prompt and engage with at least two classmates to exchange ideas and offer support.	
Cybersecurity & Citizenship Unit Plan (gradespan-specific): Students will develop a unit plan focused on cybersecurity and digital citizenship, tailored to a specific grade span such as K–2, 3–5, 6–8, or 9–12. The plan should include learning objectives, key topics, sample activities, and assessment ideas aligned with course themes.	3.00
Total (in hours)	45