K-12 BLUEPRINT

Safeguarding Our Students: Cybersecurity for K-12 Educators | November 2023

Safeguarding Our Students: Cybersecurity for K-12 Educators

Cybersecurity Action Plan

Module 1 →

Module 2 →

Module 3 →

Module 4 →

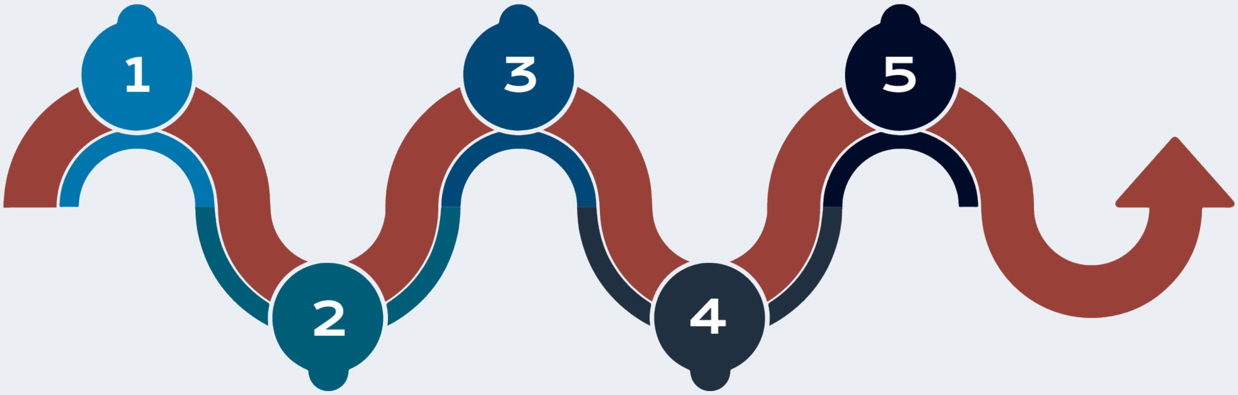
Module 5 →

Module 1

After completing the faculty meeting scenario, which topics have you self-identified as areas for growth in this course?

What are your current strengths, and where could you take meaningful action toward change?

Map out your personal course journey by marking the areas where you would like to focus your learning:



Paste screenshots, images, text, or links from Module 1 for each of the following:

	Use the spaces below for text or links	Use the spaces below for screenshots and images
Something that surprised you		
Something that resonated with you		
Something you want to know more about		
Something you want to share with your team		

Module 2

Using Passwords and Identity Authentication

Follow the steps outlined in this lesson to create a strong, unique password for your classroom device or school account.

If you choose to write down your password as you work, make sure to delete or shred what you have written when you finish. That's a secure practice!

Mark each completed step for creating a strong, unique password:

□ Find a memorable phrase

□ Remove spaces

□ Add uppercase letter(s)

□ Add number(s)

□ Add special character(s)

Identify colleagues or members of your school's IT team that can help answer the following questions. Record any notes, ideas, or resources for future reference.

Is single sign-on (SSO) an option for the school services I regularly use? If so, which SSO provider should I use?

Which school services require different accounts and passwords?

What is the protocol for resetting my password for different accounts?

Protecting Personally Identifiable Information

In your own words, how would you explain phishing, phishing techniques, and spam messages?

Write what you would say to a colleague to convey your understanding of cybersecurity threats.

The AEIOU-Y strategy uses questions you can ask yourself when deciding if a message is a phishing or smishing attempt.

Fill in the table with questions you might ask yourself. For each question, record "look for" examples from the course.

	Strategic questions to ask	Things to look for
A		
E		
I		
O		
U		
Y		

Identify colleagues or members of your school's IT team that can help answer the following questions. Record any notes, ideas, or resources for future reference.

What should I do if I suspect a message is a phishing attempt? Who should I contact?	
What steps should I follow if I accidentally fall for a phishing message?	
What steps should I follow if a student falls for a phishing message on a school device?	

Maintaining Online Privacy

Mark any of the following statements from the lesson that are true for you:

- □ I know how our school's student directory information is shared.
- □ I know where to check media release permissions if I want to share an image or video of a student online.
- □ I know the process for using a new, not-previously-approved learning app or service with students.
- □ There's someone I can contact if I want to use a new online app or service with my students and I'm unsure about what information to share.
- □ I know whether I'm allowed to create student accounts for online apps and services.

Look back on the statements above that are unmarked. Which members of your school's IT support team can help? What are your next steps? Record any notes, ideas, or resources for future reference.

As you complete this module, think about the precautions you currently take to ensure the privacy of your own information and information about your students. Reflect on which ideas from Module 2 you want to begin implementing more regularly.

Choose one idea and make a plan:

What are your next steps?

When will you begin?

What resources do you need?

Who can help you get there?

Module 3

Securing Devices and Creating Backups

Get to know your school’s protocols for regularly updating classroom devices and backing up data.

Write down any notes, follow-up questions, or steps you’ll need to take.

Having a Response Plan

Reflect on what you learned about cyber incident responses. Mark the statements from the course that apply to you:

- □ **Plan Overview:** I know where to locate and read through my school's cybersecurity incident response plan (IRP).
- □ **Incident Types:** I know the different types of cybersecurity incidents that the plan covers, such as data breaches, malware infections, phishing attacks, and denial of service (DoS) attacks.
- □ **Reporting Procedures:** I know how to report a suspected or confirmed cybersecurity incident, including whom to contact and what information to provide.
- □ **Incident Classification:** I understand how incidents are classified based on severity and impact, as this will determine the response strategy.
- □ **Roles and Responsibilities:** I am familiar with my role and responsibilities in the event of a cybersecurity incident, including any specific tasks or actions I need to take according to my school's IRP.
- □ **Chain of Command:** I know the chain of command for cybersecurity incidents and whom to contact at different stages of the response.
- □ **Communication Protocols:** I know the communication channels and procedures I should follow for notifying relevant personnel, such as IT staff, administrators, and law enforcement, if necessary.
- □ **Incident Escalation:** I understand when an incident needs to be escalated to higher authorities or external agencies, and I know who to contact.
- □ **Incident Recovery:** I am aware of the steps involved in recovering from a cybersecurity incident, including restoring systems and data.
- □ **Incident Documentation:** I understand how the school wants me to document cybersecurity incidents, including the timeline of events and actions taken.
- □ **Legal and Regulatory Requirements:** I am aware of the legal and regulatory obligations related to my role in incident reporting and response.
- □ **Policy Updates:** I know how to stay informed about updates and changes to the school's cybersecurity policies and incident response plan.

Look back on the statements that are unmarked. Which members of your school’s IT support team can help? What are your next steps? Record any notes, ideas, or resources for future reference.

As you complete this module, think about the precautions you currently take to maximize the security of your classroom devices. Reflect on which ideas from Module 3 you want to begin implementing more regularly.

Choose one idea and make a plan:

What are your next steps?

When will you begin?

What resources do you need?

Who can help you get there?

Module 4

Teaching Students about Cybersecurity

The information your students need to know about cybersecurity depends largely on their age, prior knowledge, and daily interactions with technology.

Record the topics from the course that you identified as cybersecurity ideas your students need to know the most.

Which programs or curricula from this module best aligned to the topics you identified above? Paste images, text, and links to save these teaching resources for future reference.

Cybersecurity topic	Resource text or links	Screenshots and images

Information Sharing and Collaboration

Which information sharing groups are best aligned to your personal cybersecurity needs and goals as an educator?

Mark the organizations you would like to explore further:

□ K12 SIX □ MS-ISAC □ SchoolSafety.gov

What impact might this have on your classroom cybersecurity efforts?

Make a list of next steps you'll take to join a collaboration, and which team members can help.

As you complete this module, think about the cybersecurity teaching resources that you saved. Which one are you most excited about? Reflect on the ideas from Module 4 that you want to begin implementing right away.

Choose one idea and make a plan:

How will this fit into your existing curriculum?

When will you begin? How much time will you need?

What materials will you need to gather?

Is there anyone at your school that would be an expert resource?

Module 5

Course Wrap Up

Take a few minutes to review the lists of goals, action items, and next steps that you have recorded in your Action Plan.

Prioritize the action items you want to complete in the near term. Where do you want to be now?

↓

Where do you want to be 6 months from now?

↓

Where do you want to be a year from now?

From this final reflection, write a commitment statement. Include your commitment to what you want to accomplish next, what resources you'll need, and the team members to help you get there.

Commitment Statement