Introduction

The Ohio Department of Education’s Office of Learning and Instructional Strategies is in the process of revising the Ohio’s Model Curriculum for Computer Science.

The State Board of Education adopted Ohio’s Learning Standards and Model Curriculum for Computer Science in December 2018. Implemented in the 2019-2020 (FY2020) school year, the purpose of Ohio’s Learning Standards and Model Curriculum for Computer Science is to provide guidance to schools and districts. Ohio educators, many of whom engage daily with Ohio students, led the process to create Ohio’s Learning Standards and Model Curriculum for Computer Science.

The review and revision process presents an opportunity for families, computer science professionals, community members and other educators, to provide suggestions for improving the model curriculum through a public comment survey, open March 2 through Mar. 18.

In the Fall of 2021, the public was invited to provide comments on the current standards and model curriculum. Advisory group members, who have an educational background or professional experience in computer science, met several times to discuss the public comment and make suggestions for revisions. The advisory group then provided direction and guidance to the working groups of Ohio educators, who worked to write the revisions.

The following is a draft of the revised model curriculum available for viewing and public comment. This document contains the revisions to the model curriculum for the strands Network and the Internet and Impacts of Computing. This model curriculum is address new proposed standards and therefore new content.

In your review, please focus on the content of the statements. All materials will be going through additional technical edits, but because of the timeline outlined in HB110, the Department wanted to make these drafts available for public comment at this time.

To see the model curriculum adopted by the Ohio State Board of Education in 2018 please visit the Model Curriculum for Computer Science.
Overview of the Computer Science Standards Framework

Ohio’s Computer Science Standards are organized by strands, topics and content statements.

Kindergarten through Grade 8 - Content statements are organized by grade level. Below is an example of a content statement for kindergarten and its corresponding content statement code. This content statement addresses the topic of Devices within the Computing Systems strand.

**Computing Systems**

*Devices*

**CS.D.K.a** With guidance, identify and label commonly used devices and their components, explaining their connection to different tasks, to perform a variety of tasks.
Computer Science Model Curriculum: Cybersecurity Networks and the Internet (NI) DRAFT

Networks and the Internet, Grade 1-3

<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

**NI.C.1.b** Identify, use and discuss examples of how devices can be used with good and bad intentions.

**Expectations for Learning**

**LEARNING PROGRESSION**

Building on NI.C.1.a, students will discover the use of devices, specifically that devices can be used with both good and bad intentions. This concept will progress through grade 5.

**IMPORTANT CONCEPTS**

- Decision making when using technology
- There are intended and unintended consequences of device use

**KEY SKILLS/PROCEDURES**

- Use devices appropriately
- Log in and out of applications (apps) and devices

**Content Elaborations**

**CLARIFICATIONS**

In grade 1, students may still require assistance with their passwords and online navigation. Focus on the names and purposes of different devices and their uses. Students should be able to recognize bad intentions, such as taking unwanted photos and sharing personal information.

**CONTENT FOCUS**

The focus is on appropriate device intentions and use. Students will begin to use devices and digital resources as a natural part of their educational experience.

**COMPUTER SCIENCE PRACTICES**

*Practice 7. Communicating About Computing*

3. Articulate ideas responsibly by observing intellectual property rights and giving appropriate attribution.
## Expectations for Learning

**LEARNING PROGRESSION**

In grade 3, students will explore and explain grade appropriate examples of unsafe content. In grade 4, students describe the effects of malicious content. In grade 5, students will analyze the inappropriate use of online services.

### IMPORTANT CONCEPTS

- Personal information is valuable and both private and sharable
- Personal (private) information should be protected
- Threats including malware, ransomware and others are connected to the online environment

### KEY SKILLS/PROCEDURES

- Describe malware and pop-ups
- Describe and identify online threats
- Describe and identify social engineering concepts
- Understand and Practice Cyber Hygiene

### Content Elaborations

**CLARIFICATIONS**

Students often do not know what happens when you click a link on a web page and should be taught that they could lead to inappropriate websites. Students should know the different types of pop-up messages and their meaning. Students need to know that some pop-up messages are not safe and could lead to improper websites or download malicious content. Students should know that there are many appropriate uses for pop-up messages and windows.

### CONTENT FOCUS

The focus is on students understanding different types of digital threats to personal and public information and why understanding basic cyber hygiene and awareness is important for all students. Students should be able to discuss examples of mitigation of digital threats including malware and pop-ups.

### COMPUTER SCIENCE PRACTICES

*Practice 3. Recognizing and Defining Computational Problems*

1. Identify complex, interdisciplinary, real-world problems that can be solved computationally.
# Networks and the Internet, Grade 4-5

<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

**NI.C.4.b** Describe and explain safe usage of various online services such as web, email, video, gaming, Cloud Services, and networked drives.

## Expectations for Learning

**LEARNING PROGRESSION**

In grade 3, students learned to explore and explain grade appropriate examples of unsafe content. In grade 4, students describe the effects of malicious content. In grade 5, students will analyze the appropriate and inappropriate use of online services.

**IMPORTANT CONCEPTS**

- Online services have different purposes and methods of use
- Devices can be used for proper or improper purposes
- Not all online services are safe

**KEY SKILLS/PROCEDURES**

- Define and describe malware and pop-ups
- Explain how to protect yourself from malware, pop-ups and other threat vectors
- Describe the effects of malware and the use of malware to access private information

## Content Elaborations

**CLARIFICATIONS**

Many devices can connect to the internet (cloud services) to share information and access applications (Apps). Students should understand that using websites, email, video gaming, cloud services and networked drives share information that adds to the need for secure practices.

**CONTENT FOCUS**

The focus is on students identifying and securing personal information and being aware of consequences related to unsecure information, malware and other online threat vectors.
### Computer Science Model Curriculum: Cybersecurity Networks and the Internet (NI) DRAFT

<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

#### COMPUTER SCIENCE PRACTICES

- **Practice 2. Collaborating Around Computing Practice**
  4. Evaluate and select technological tools that can be used to collaborate on a project.

- **Practice 5. Creating Computational Artifacts**
  2. Create a computational artifact for practical intent, personal expression, or to address a societal issue.
  3. Modify an existing artifact to improve or customize it.

#### Ni.C.5.b

- Explore and utilize various online services such as web, email, video, gaming, Cloud Services and networked drives.

#### Expectations for Learning

**LEARNING PROGRESSION**

In grade 4, students describe the effects of malicious content. In grade 5, students will analyze the use of online services. In grade 6, students will recognize the effects of malicious content and other online threats.

**IMPORTANT CONCEPTS**

- Using online services such as web, email, video, gaming, Cloud Services and networked drives
- There are appropriate levels of information sharing appropriate to different online services

**KEY SKILLS/PROCEDURES**

- Understand the use of devices and software in connected environments
- Explore the use of different tools and uses of computing systems
- Explore the need for security for these systems

**Content Elaborations**

**CLARIFICATIONS**

Students should understand that using websites, email, video gaming, cloud services and networked drives adds to the need for secure practices.

**CONTENT FOCUS**

Explore and experiment with different uses of devices, software and connected systems. Students should discuss the information each of these systems store and what they share with other systems. Students should also understand how the information in the systems is secured.
## Computer Science Model Curriculum: Cybersecurity Networks and the Internet (NI) DRAFT

### Networks and the Internet, Grade 8

<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

#### NI.C.8.c

**Expectations for Learning**

**LEARNING PROGRESSION**

In previous grades, students developed a general understanding that private information should be protected from malware threats, online services and unauthorized access. By the end of grade 8, students should recognize different threat actors and threat vectors that are commonly employed.

In future grades, students will be able to infer, articulate and employ best practices for threat mitigation.

**IMPORTANT CONCEPTS**

- There are different types of threat actors that operate differently with different motivations
- There are different threat vectors commonly employed to access information or disrupt services

**KEY SKILLS/PROCEDURES**

- Identify the types of threat actors and their objectives
- Identify common threat vectors
- Discuss cyber hygiene and threat mitigation

---

#### COMPUTER SCIENCE PRACTICES

**Practice 2. Collaborating Around Computing**

4. Evaluate and select technological tools that can be used to collaborate on a project.

**Practice 5. Creating Computational Artifacts**

2. Create a computational artifact for practical intent, personal expression or to address a societal issue.
3. Modify an existing artifact to improve or customize it.
## Content Elaborations

### CLARIFICATIONS

Students will begin to work more independently. Previously, they will and have been working with computing, data systems, and devices like Raspberry Pi’s, Arduinos and other devices. Now students should become more aware of online threats and threat actors.

### CONTENT FOCUS

Understand and discuss different threat vectors that are used by the different threat actors and their motives.

### COMPUTER SCIENCE PRACTICES

*Practice 7. Communicating About Computing.*

2. Describe, justify, and document computational processes and solutions using appropriate terminology consistent with the intended audience and purpose.

### Expectations for Learning

#### LEARNING PROGRESSION

In previous grades, students developed a general understanding about basic encryption. By the end of grade 8, students should recognize different encryption methods. In future grades, students will be able to utilize various encryption techniques to protect data.

#### IMPORTANT CONCEPTS

- Encryption is a key concept in password and personal data security
- Encryption is needed to protect data in transit and at rest
- Understanding encryption could lead students into more advanced cyber security topics

#### KEY SKILLS/PROCEDURES

- Identify the goals of encryption
- Identify types and explain uses of encryption
- Discuss the uses of encryption
- Use encryption methods to solve problems
### Content Elaborations

**CLARIFICATIONS**

There are many classic examples of encryption that can be engaging and interesting to both teachers and students. Discuss how encryption can solve problems in computing and protect assets.

**CONTENT FOCUS**

As students leave grade 8, they should know and understand what personal data is, why it is important to them and why it is important to protect personal identifiable information.

Students should also understand that information and data can be protected using encryption methods and other processes. This includes the idea of the CIA triad; a concept that focuses on the balance between the confidentiality, integrity and availability of data under the protection of your information security program.

**COMPUTER SCIENCE PRACTICES**

*Practice 7. Communicating About Computing*

1. Describe, justify, and document computational processes and solutions using appropriate terminology consistent with the intended audience and purpose.
<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
<th>Cybersecurity</th>
</tr>
</thead>
</table>

**NI.C.9-12.F.c**  
Compare and contrast examples of various threat actors, such as nation-states, cyber terrorist groups, organized crime, or hacktivists and the threat vectors used.

**NI.C.9-12.F.d**  
Explore and utilize examples of encryption methods, e.g., Vigenere, Bacon's cipher, and Enigma.

---

**Expectations for Learning**

**LEARNING PROGRESSION**

In previous grades students began to employ best practices for threat mitigation. By the end of the foundational level of 9-12, students will compare threat actors and threat vectors that are used. In previous grades, students should recognize different encryption methods. In future grades, students will be able to utilize various encryption techniques to protect data.

**IMPORTANT CONCEPTS**

- Threat actors are those parties that plan and execute threats
- Threat vectors are ways threat actors enter a network or system
- Encryption is a concept that allows information to help protect files, networks and systems

**KEY SKILLS/PROCEDURES**

- Discuss threat vectors and the threat actors behind attacks
- Discuss how encryption help to secure files, networks and systems

**Content Elaborations**

**CLARIFICATIONS**

Threat actors could be nation-states, cyber terrorists, hacktivists or organized crime.

**CONTENT FOCUS**

By the end of grade 12, students should understand what data they should share and when it should be shared. They should exhibit good digital citizenry as it applies to cyber security hygiene, awareness and safe browsing. They also should know how to connect safely to online services using a Virtual Private Networking (VPN).

Students should also understand that information and data can be protected using encryption methods and other processes. This includes the idea of the CIA triad; a concept that focuses on the balance between the confidentiality, integrity and availability of data under the protection of your information security program.
<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

**COMPUTER SCIENCE PRACTICES**

*Practice 3. Recognizing and Defining Computational Problems*

1. Identify complex, interdisciplinary, real-world problems that can be solved computationally.

<table>
<thead>
<tr>
<th>NI.C.9-12.A.c</th>
<th>Expectations for Learning</th>
</tr>
</thead>
</table>

Compare and contrast examples of various threat actors, such as nation-states, cyber terrorist groups, organized crime, or hacktivists and the treat vectors used.

<table>
<thead>
<tr>
<th>NI.C.9-12.A.d</th>
<th>LEARNING PROGRESSION</th>
</tr>
</thead>
</table>

In the foundational level of 9-12, students researched types of threat actors. In the advanced level of 9-12, students should focus on a deeper level of understanding of how and why various threat actors break the law, what individuals and groups hope to gain or change by their actions and the mitigation of physical security attacks, such as social engineering, security policies and malicious actors.

**IMPORTANT CONCEPTS**

- Compare encryption methods with a focus on real-world examples
- Compare types of threat actors and their objectives
- Use safe browsers and cyber practices to protect personal information
- Explore and discuss real-world scenarios including social engineering and other cyber threat vectors

**KEY SKILLSPROCEDURES**

- Discuss threat vectors and the threat actors behind attacks
- Discuss the interrelationship between the CIA (confidentiality, integrity and availability) triad; a concept that focuses on the balance between the confidentiality, integrity and availability of data under the protection of information security programs

**Content Elaborations**

**CLARIFICATIONS**

Cybersecurity assessment examples may include full- or limited-scope penetration tests, hardware analysis and source code audits. Undesired outcomes include false senses of security that may result from improperly conducted assessments.

**CONTENT FOCUS**

Researching malware includes understanding the different classes of malware (e.g., potentially unwanted programs, ransomware, rootkits, trojans, viruses, worms) and the reasoning for its application by an adversary. Mitigations may include configuring file permissions, configuring host- network-based firewalls and using encryption technology for...
Computer Science Model Curriculum: Cybersecurity Networks and the Internet (NI) DRAFT

<table>
<thead>
<tr>
<th>Strand</th>
<th>Networks and the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>network communications. Mitigation strategies include reducing the potential vulnerabilities caused by social engineering of humans, which is an attack vector present in all systems, including hardware, software and networks.</td>
</tr>
</tbody>
</table>

COMPUTER SCIENCE

Practice 3. Recognizing and Defining Computational Problems
1. Identify complex, interdisciplinary, real-world problems that can be solved computationally.

1. Systematically test computational artifacts by considering all scenarios and using test cases.

Impacts of Computing, Kindergarten-Grade 2

<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

IC.SLE.K.b With guidance and support, discuss examples of appropriate and inappropriate behavior online, including cyberbullying, and the steps to keep yourself and others safe or out of harm’s way.

Expectations for Learning

LEARNING PROGRESSION
In kindergarten through second grade, student discussions should focus on examples of what to do when someone is hurtful online and what behavior should be modeled when online.

IMPORTANT CONCEPTS
- Guidelines and practices to stay safe on the internet
- Students should be aware of what private information is, what students should and should not share and what are potential consequences of sharing private information

KEY SKILLS/PROCEDURES
- Identify appropriate and inappropriate online behavior
- Apply the concepts of online safety
## Computer Science Model Curriculum: Cybersecurity Networks and the Internet (NI) DRAFT

<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

### Content Elaborations

**CLARIFICATIONS**

Students need to make good choices when they interact with others online. They also need to understand that in addition to interaction with others, it is important that they use websites and other apps as they were intended.

Some online behavior is illegal, and students could be held responsible for their actions online.

**CONTENT FOCUS**

Students should understand the appropriate and inappropriate behavior to use when operating online. Students should also know who to talk to if they feel threatened or to report inappropriate behavior.

**COMPUTER SCIENCE PRACTICES**

- **Practice 3.** Recognizing and Defining Computational Problems.
  2. Decompose complex, real-world problems into manageable subproblems that could integrate existing solutions or procedures.

- **Practice 6.** Testing and Refining Computational Artifacts.
  1. Systematically test computational artifacts by considering all scenarios and using test cases.

### Expectations for Learning

**LEARNING PROGRESSION**

In kindergarten through second grade, student discussions should focus on examples of what to do when someone is hurtful online and what behavior should be modeled when online.

**IMPORTANT CONCEPTS**

- Students give examples of people in authority, such as a principal, teacher or police officer with whom they might share private (privileged) information
- Students know who to contact for help when they feel unsafe or witness inappropriate online behavior

---

IC.SLE.1.b Discuss examples of appropriate and inappropriate behavior online, including cyberbullying, and the steps to keep yourself and others safe and out of harm's way.
<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

**KEY SKILLS/PROCEDURES**
- Recognize when students should report observed inappropriate online behavior to those in authority
- Understand and discuss ways to keep yourself and others safe online
- Students should understand.

**Content Elaborations**

**CLARIFICATIONS**
Students need to make good choices when they interact with others online. They also need to understand that in addition to interaction with others, it is important that they use websites and other apps as they were intended.

Some online behavior is illegal, and students could be held responsible for their actions online.

**CONTENT FOCUS**
Students should understand the appropriate and inappropriate behavior to use when operating online. Students should also know who to talk to if they feel threatened or to report inappropriate behavior.

**Computer Science Practices**

*Practice 3. Recognizing and Defining Computational Problems.*
2. Decompose complex real-world problems into manageable subproblems that could integrate existing solutions or procedures.

*Practice 6. Testing and Refining Computational Artifacts.*
1. Systematically test computational artifacts by considering all scenarios and using test cases.
<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

**IC.SLE.2.b**

Compare and contrast appropriate and inappropriate behavior online, including cyberbullying, and the steps to keep yourself and others safe and out of harm's way.

**Expectations for Learning**

**LEARNING PROGRESSION**

In kindergarten through second grade, student discussions should focus on examples of what to do when someone is acting inappropriately online and what behavior should be modeled when online.

**IMPORTANT CONCEPTS**

- Students know whom to contact if they experience inappropriate behavior while online.
- Students know what steps to take when they experience inappropriate behavior online.

**KEY SKILLS/PROCEDURES**

- Recognize when students should report observed inappropriate online behavior to those in authority
- Understand and discuss ways to keep yourself and others safe online
- Students should understand.

**Content Elaborations**

**CLARIFICATIONS**

Students need to make good choices when they interact with others online. They also need to understand that in addition to interaction with others, it is important that they use websites and other apps as they were intended.

Some online behavior is illegal, and students could be held responsible for their actions online.

**CONTENT FOCUS**

Students should understand the appropriate and inappropriate behavior to use when operating online. Students should also know who to talk to if they feel threatened or to report inappropriate behavior.

**COMPUTER SCIENCE PRACTICES**

*Practice 1. Fostering an Inclusive Computing Culture*

2. Address the needs of diverse end-users during the design process to produce artifacts with broad accessibility and usability.

3. Employ self- and peer-advocacy to address bias in interactions, product design and development methods.
Impacts of Computing, Grade 3-4

<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

IC.SLE.3.d Explain why different types of information might need to be protected, describing common safeguards for protecting personal information.

**Expectations for Learning**

**LEARNING PROGRESSION**

In grade 3, students will learn about what information should be shared and how to keep their information secure. In grade 4, students will be introduced to the idea that there are tradeoffs between allowing information to be public versus keeping information private. In grade 5, students will learn about their digital footprint.

**IMPORTANT CONCEPTS**

- Students should know what personally identifiable information (PII) is.
- Individuals should be careful what personally identifiable information (PII) they share online or in-person.

**KEY SKILLS/PROCEDURES**

- List examples of personally identifiable information (PII).
- Explain the dangers of sharing personally identifiable information.

**Content Elaborations**

**CLARIFICATIONS**

At this level, student discussions focus on examples of personally identifiable information and how to keep personal information, including private and public information, safe online.

**CONTENT FOCUS**

Research and describe potential effects of the positives and negatives for making information public.

**COMPUTER SCIENCE PRACTICES**

*Practice 3. Recognizing and Defining Computational Problems.*

1. Decompose complex real-world problems into manageable subproblems that could integrate existing solutions or procedures.

*Practice 6. Testing and Refining Computational Artifacts.*

1. Systematically test computational artifacts by considering all scenarios and using test cases.
### Practice 7. Communicating about Computing

2. Describe, justify, and document computational processes and solutions using appropriate terminology consistent with the intended audience and purpose.

<table>
<thead>
<tr>
<th>Strand</th>
<th>Impacts of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Safety, Law and Ethics</td>
</tr>
</tbody>
</table>

**IC.SLE.4.d** Describe tradeoffs between allowing information to be public and keeping information private and secure.

**Expectations for Learning**

**LEARNING PROGRESSION**

In grade 3, students will learn about what information should be shared and how to keep their information secure. In grade 4, students will be introduced to the idea that there are tradeoffs between allowing information to be public versus keeping information private. In grade 5, students will learn about their digital footprint.

**IMPORTANT CONCEPTS**

- Personal identifiable information (PII)
- Steps to keeping personal identifiable information (PII) secure

**KEY SKILLS/PROCEDURES**

- List examples of personal identifiable information (PII)
- Explain the dangers of sharing personally identifiable information

**Content Elaborations**

**CLARIFICATIONS**

Student discussions should focus on examples of personally identifiable information and how to keep personal information, both private and public, safe online.

**CONTENT FOCUS**

Students to be able to effectively manage their digital identities. Students should understand that online information does not go away, and that information online can affect the students’ real lives, even in future years.

**COMPUTER SCIENCE PRACTICES**

*Practice 3. Recognizing and Defining Computational Problems.*

1. Identify complex, interdisciplinary, real-world problems that can be solved computationally.