Computer Science Essential Concepts

And Subconcepts

Computer Concepts: Networks and the Internet

Kindergarten - Highschool

Computer Science Essential Concepts and Subconcepts

The Arizona Computer Science Standards for grades kindergarten through twelve are organized into five Essential Concepts:

- **Computing Systems:** This involves the interaction that people have with a wide variety of computing devices that collect, store, analyze, and act upon information in ways that can affect human capabilities both positively and negatively. The physical components (hardware) and instructions (software) that make up a computing system communicate and process information in digital form. An understanding of hardware and software is useful when troubleshooting a computing system that does not work as intended. Computing Systems has three subconcepts, they are: Devices, Hardware and Software, and Troubleshooting.

- **Networks and the Internet (with Cybersecurity):** This involves the networks that connect computing systems. Computing devices do not operate in isolation. Networks connect computing devices to share information and resources and are an increasingly integral part of computing. Networks and communication systems provide greater connectivity in the computing world by providing fast, secure communication and facilitating innovation. Networking and the Internet must also consider Cybersecurity. Cybersecurity, also known as information technology security, involves the protection of computers, networks, programs, and data from unauthorized or unintentional access, manipulation, or destruction. Many organizations, such as government, military, corporations, financial institutions, hospitals, and others collect, process, and store significant amounts of data on computing devices. That data is transmitted across multiple networks to other computing devices. The confidential nature of government, financial, and other types of data requires continual monitoring and protection for the sake of continued operation of vital systems and national security. This concept has two subconcepts within it, they are: Cybersecurity, and Network Communication and Organization.

- **Data and Analysis:** This involves the data that exist and the computing systems that exist to process that data. The amount of digital data generated in the world is rapidly expanding, so the need to process data effectively is increasingly important. Data is collected and stored so that it can be analyzed to better understand the world and make more accurate predictions. This concept has three subconcepts, they are: Collection, Visualization and Transformation, Storage, and Inference and Models

- **Algorithms and Programming:** Involves the use of algorithms. An algorithm is a sequence of steps designed to accomplish a specific task. Algorithms are translated into programs, or code, to provide instructions for computing devices. Algorithms and programming control all computing systems, empowering people to communicate with the world in new ways and solve compelling problems. The development process to create meaningful and efficient programs involves choosing which information to use and how to process and store it, breaking apart large problems into smaller ones, recombining existing solutions, and analyzing different solutions. This concept has 5 subconcepts, they are: Algorithms, Variables, Control, Modularity, and Program Development

- **Impacts of Computing:** This involves the effect that computing has on daily life. Computing affects many aspects of the world in both positive and negative ways at local, national, and global levels. Individuals and communities influence computing through their behaviors and cultural and social interactions, and in turn, computing influences new cultural practices. An informed and responsible person should understand the social implications of the digital world, including equity and access to computing. This concept has 3 subconcepts, they are: Culture, Social Interactions, and Safety, Law, and Ethics

Concepts are categories that represent major content areas in the field of computer science. They represent specific areas of disciplinary importance rather than abstract, general ideas. Each essential concept is supported by various subconcepts that represent specific ideas within each concept. Figure 1 provides a visual representation of the Essential Concepts and the supporting subconcepts.

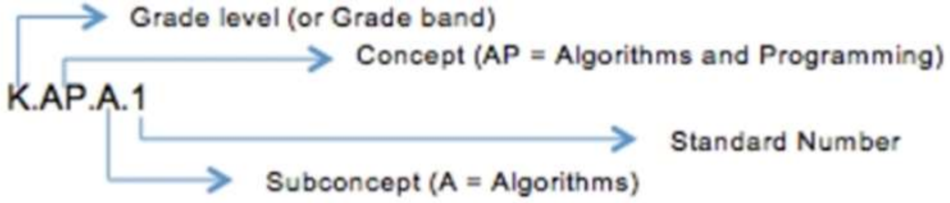
Figure 1: Computer science essential concepts and subconcepts

Computing Systems	**Networking and the Internet**	**Data and Analysis**	**Algorithms and Programming**	**Impacts of Computing**
Devices *Hardware and Software* *Troubleshooting*	*Network Communication and Organization* *Cybersecurity*	*Collection* *Storage* *Visualization and Transformation* *Inference and Models*	*Algorithms* *Variables* *Control* *Modularity* *Program Development*	*Culture* *Social Interactions* *Safety, Law, and Ethics*

The pages following break the concepts and subconcepts down by Concept, from Kindergarten through High School. Each Concept is labeled and separated from the next. This will allow teachers to more easily track progression within the standards.

Each standard will list the grade level, the concept, the subconcept, and the standard number. Figure 2 provides an example of the coding for, and how to read, a standard:

Figure 2: Standard Coding Scheme for Standards


Grade level (or Grade band)
Concept (AP = Algorithms and Programming)
K.AP.A.1
Standard Number
Subconcept (A = Algorithms)

Concept: Networks and the Internet (NI)

Subconcept: Cybersecurity (C)	
K.NI.C.1	**Explain that a password helps protect the privacy of information.** *Connecting devices to a network or the Internet provides great benefit, care must be taken to use authentication measures, such as strong passwords, to protect devices and information from unauthorized access. This is an essential first step in learning about cybersecurity. Usernames and passwords, such as those on computing devices or Wi-Fi networks, provide a way of authenticating a user's identity. For example, students should enter a password independently and commit to keeping their password private.* *Practice(s):* Communicating About Computing: 7.2
Subconcept: Network, Communication, and Organization (NCO)	
K.NI. NCO.1	**With teacher guidance, students define computer networks and how they can be used to connect people to other people, places, information, and ideas.** *Small, wireless devices, such as cell phones, communicate with one another through a series of intermediary connection points, such as cellular towers. This coordination among many computing devices allows a person to voice call a friend or video chat with a family member. For example, kindergarten students understand that they are part of non-computing networks such as family, class, school, etc. Kindergarten students should be able to explain that devices are connected, though details about connection points are not expected at this level.* *Practice(s): Communicating About Computing: 7.3*
Subconcept: Cybersecurity (C)	
1.NI.C.1	**Explain what passwords are and why we use them to protect personal information (e.g., name, location, phone number, home address) and keep it private.** *Connecting devices to a network or the Internet provides great benefit, care must be taken to use authentication measures, such as strong passwords, to protect devices and information from unauthorized access. This is an essential first step in learning about cybersecurity. For example, first grade students should be able to accurately enter a password to log on to a program and understand the importance of keeping passwords private in order to protect their personal information.* *Practice(s):* Communicating About Computing: 7.2

Subconcept: Network, Communication, and Organization (NCO)	
1.NI. NCO.1	**With teacher guidance, students discuss how computer networks can be used to connect people to other people, places, information, and ideas.** *Small, wireless devices, such as cell phones, communicate with one another through a series of intermediary connection points, such as cellular towers. This coordination among many computing devices allows a person to voice call a friend or video chat with a family member. Details about the connection points are not expected at this level. For example, students will participate in a class discussion about how different networks connect people, places, things and information, such as a phone call to grandma in another state, using Facetime or Skype to connect with a content area expert, connecting devices via Bluetooth, or accessing an online game through Wi-Fi.* *Practice(s): Communicating About Computing: 7.2*
Subconcept: Cybersecurity (C)	
2.NI.C.1	**Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.** *Connecting devices to a network or the Internet provides great benefit, care must be taken to use authentication measures, such as strong passwords, to protect devices and information from unauthorized access. This is an essential first step in learning about cybersecurity. They should appropriately use and protect the passwords they are required to use. Usernames and passwords, such as those on computing devices or Wi-Fi networks, provide a way of authenticating a user's identity. For example, students learn to not share passwords and not use anyone else's password.* *Practice(s):* Communicating About Computing: 7.2
Subconcept: Network, Communication, and Organization (NCO)	
2.NI. NCO.1	**Students can discuss how computer networks can be used to connect people to other people, places, information, and ideas.** *Small, wireless devices, such as cell phones, communicate with one another through a series of intermediary connection points, such as cellular towers. This coordination among many computing devices allows a person to voice call a friend or video chat with a family member. Details about the connection points are not expected at this level. For example, students will participate in a class discussion about how different networks connect people, places, things and information, such as a phone call to grandma in another state, using conferencing software to connect with a content area expert, or accessing an online game via Wi-Fi.* *Practice(s): Communicating About Computing: 7.2*
Subconcept: Cybersecurity (C)	
3.NI.C.1	**Identify real-world cybersecurity problems and how personal information can be protected.** *Just as we protect our personal property online, we need to protect our devices and the information stored on them. Information can be protected using various security measures. These measures can be physical and/or digital. For example, discussion topics could be based on current events related to cybersecurity or topics that are applicable to students and the programs/devices they use such as adding passwords to lock devices.* *Practice(s): Communicating about Computing, Recognizing and Defining Computational Problems: 7.1, 3.1*

Subconcept: Network, Communication, and Organization (NCO)	
3.NI.NCO.1	**Model how information flows in a physical or wireless path to travel to be sent and received is sent and received through a physical or wireless path.** *There are physical paths for communicating information, such as Ethernet cables, and wireless* paths (Wifi). *Often, information travels on a combination of physical and wireless paths. Wireless paths originate from a physical connection point and travel through multiple devices and wired or wireless connections to their end point. Models could include visual, physical, or* alternate representations. *Practice(s): Developing and Using Abstractions: 4.3*
Subconcept: Cybersecurity (C)	
4.NI.C.1	**Discuss real-world cybersecurity problems and how personal information can be protected.** *Just as we protect our personal property online, we also need to protect our devices and the information stored on them. Information can be protected using various security measures. These measures can be physical and/or digital. For example, discussion topics could be based on current events related to cybersecurity or topics that are applicable to students and the programs/devices they use.* *Practice(s): Communicating about Computing, Recognizing and Defining Computational Problems: 7.2, 3.3*
Subconcept: Network, Communication, and Organization (NCO)	
4.NI.NCO.1	**Model how information is decomposed, transmitted as packets through multiple devices over networks and reassembled at the destination.** *There are physical paths for communicating information, such as Ethernet cables, and wireless paths, such as Wi-Fi. Often, information travels on a combination of physical and wireless paths. Information is broken down into smaller pieces called packets, which are sent over the network and reassembled at the destination. Routers and switches are used to properly send packets across paths to their destinations.* *Practice(s): Developing and Using Abstractions: 4.4*
Subconcept: Cybersecurity (C)	
5.NI.C.1	**Identify solutions to real-world cybersecurity problems and how personal information can be protected.** *Just as we protect our personal property online, we also need to protect our devices and the information stored on them. Information can be protected using various security measures. These measures can be physical and/or digital. For example, discussion topics could be based on current events related to cybersecurity or topics that are applicable to students and the programs/devices they use.* *Practice(s): Communicating about Computing, Recognizing and Defining Computational Problems: 7.2, 3.1*

Subconcept: Network, Communication, and Organization (NCO)	
5.NI. NCO.1	**Analyze the advantages and disadvantages of various network types.** *There are physical paths for communicating information, such as Ethernet cables, and wireless paths, such as Wi-Fi or cellular data. The choice of device and type of connection will affect the path information travels and the potential bandwidth (the capacity to transmit data or bits in a given timeframe).* *Practice(s): Developing and Using Abstractions, Collaborating Around Computing: 4.1, 2.4*
Subconcept: Cybersecurity (C)	
6.NI.C.1	**Identify multiple methods of encryption to secure the transmission of information.** *Encryption can be as simple as letter substitution or as complicated as modern methods used to secure networks and the Internet. The students will identify different methods of encoding and decoding for encryptions used to hide or secure information. Examples of encryption methods could include: Substitution ciphers (mono-alphabetic or polyalphabetic) and Caesar ciphers.* *Practice(s):* Developing and Using Abstractions: 4.4
6.NI.C.2	**Identify different physical and digital security measures that protect electronic information.** *Information that is stored online is vulnerable to unwanted access. Examples of physical security measures to protect data include keeping passwords hidden, locking doors, making backup copies on external storage devices, and erasing a storage device before it is reused. Examples of digital security measures include secure router admin passwords, firewalls that limit access to private networks, and the use of a protocol such as HTTPS to ensure secure data transmission.* Practice(s): Communicating About Computing: 7.2
Subconcept: Network, Communication, and Organization (NCO)	
6.NI. NCO.1	**Discuss how protocols are used in transmitting data across networks and the Internet.** *Protocols are rules that define how messages are sent between computers. They determine how quickly and securely information is transmitted across networks and the Internet, as well as how to check for and handle errors in transmission. The priority at this level is understanding the purpose of protocols and how they enable secure and errorless communication. Knowledge of the details of how specific protocols work is not expected. For example, students could discuss their protocols or processes for communicating with their friends. They can discuss handshakes, turn-taking, whispering vs yelling, etc. The students can compare these protocols with how computers communicate.* Practice(s): Developing and Using Abstractions: 4.4

Subconcept: Cybersecurity (C)	
7.NI.C.1	**Evaluate multiple methods of encryption for the secure transmission of information.** *Encryption can be as simple as letter substitution or as complicated as modern methods used to secure networks and the Internet. The students will examine the different levels of complexity used to hide or secure information. For example, students explore different methods of securing messages using methods such as Caesar ciphers or steganography (i.e., hiding messages inside a picture or other data).* *Practice(s):* Developing and Using Abstractions: 4.4
7.NI.C.2	**Explain how physical and digital security measures protect electronic information.** *Information that is stored online is vulnerable to unwanted access. Examples of physical security measures to protect data include keeping passwords hidden, locking doors, making backup copies on external storage devices, and erasing a storage device before it is reused. For example, digital security measures include secure router admin passwords, firewalls that limit access to private networks, and the use of a protocol such as HTTPS to ensure secure data transmission.* Practice(s): Communicating About Computing: 7.2
Subconcept: Network, Communication, and Organization (NCO)	
7.NI. NCO.1	**Compare and contrast models to understand the many protocols used for data transmission.** *Protocols are rules that define how messages are sent between computers. They determine how quickly and securely information is transmitted across networks and the Internet, as well as how to check for and handle errors in transmission. For example, students should examine how data is sent using protocols to choose the fastest path, to deal with missing information, and to deliver sensitive data securely. The priority at this level is understanding the purpose of protocols and how they enable secure and errorless communication. Knowledge of the details of how specific protocols work is not expected.* Practice(s): Developing and Using Abstractions: 4.4
Subconcept: Cybersecurity (C)	
8.NI.C.1	**Apply multiple methods of encryption to model the secure transmission of information.** Encryption can be as simple as letter substitution or as complicated as modern methods used to secure networks and the Internet. Students should encode and decode messages using a variety of encryption methods, and they should understand the different levels of complexity used to hide or secure information. For example, students could secure messages using methods such as Caesar cyphers or steganography (i.e., hiding messages inside a picture or other data). They can also model more complicated methods, such as public key encryption, through unplugged activities. *Practice(s):* Developing and Using Abstractions: 4.4

8.NI.C.2	**Evaluate how various physical and digital security measures protect electronic information and how a lack of such measures could lead to vulnerabilities.** Information that is stored online is vulnerable to unwanted access. Examples of physical security measures to protect data include keeping passwords hidden, locking doors, making backup copies on external storage devices, and erasing a storage device before it is reused. Examples of digital security measures include secure router admin passwords, firewalls that limit access to private networks, and the use of a protocol such as HTTPS to ensure secure data transmission. Examples of vulnerabilities include password strength, awareness of how data is used, as well as threats to personal and professional data. Practice(s): Communicating About Computing: 7.2
Subconcept: Network, Communication, and Organization (NCO)	
8.NI. NCO.1	**Develop models to illustrate the role of protocols in transmitting data across networks and the Internet.** Protocols are rules that define how messages are sent. They determine how quickly and securely information is transmitted across networks and the Internet, as well as how to check for and handle errors in transmission. Students should model how data is sent using protocols to choose the fastest path, to deal with missing information, and to deliver sensitive data securely. For example, students can be given a data transmission scenario and asked to determine which protocol should be used and why. The priority at this level is understanding the purpose of protocols and how they enable secure and errorless communication. Knowledge of the details of how specific protocols work is not expected. Practice(s): Developing and Using Abstractions: 4.4
Subconcept: Cybersecurity (C)	
HS.NI.C.1	**Describe how sensitive data can be affected by malware and other attacks.** *Network security depends on a combination of hardware, software, and practices that control access to data and systems. Potential security problems, such as denial-of-service attacks, ransomware, viruses, worms, spyware, and phishing, present threats to sensitive data. Students might reflect on case studies or current events in which governments or organizations experienced data leaks or data loss as a result of these types of attacks.* *Practice(s): Communicating About Computing: 7.2*
HS.NI.C.2	**Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.** *Security measures may include physical security tokens, two-factor authentication, and biometric verification. The timely and reliable access to data and information services by authorized users, referred to as availability, and is ensured through adequate bandwidth, backups, and other measures. Students should systematically evaluate different security measures based on the requirements or constraints of a situation, such as through a cost-benefit analysis. Eventually, students should include more factors in their evaluations, such as how efficiency affects feasibility or whether a proposed approach raises ethical concerns, and make recommendations based on their analysis.* *Practice(s): Recognizing and Defining Computational Problems: 3.3*

HS.NI.C.3	**Compare various security measures, considering tradeoffs between the usability and security of a computing system.** *Choosing security measures involves tradeoffs between the usability and security of the system. The needs of users and the sensitivity of data determine the level of security implemented. Students might discuss computer security policies in place at the local level that present a tradeoff between usability and security, such as a web filter that prevents access to many educational sites but keeps the campus network safe.* *Practice(s): Testing and Refining Computational Artifacts: 6.3*
Subconcept: Network, Communication, and Organization (NCO)	
HS.NI. NCO.1	**Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.** *Each device is assigned an address that uniquely identifies it on the network. Routers function by comparing IP addresses to determine the pathways packets should take to reach their destination. Switches function by comparing MAC addresses to determine which computers or network segments will receive frames. Students could use online network simulators to experiment with these factors.* *Practice(s): Developing and Using Abstractions: 4.1*