

INTRODUCTION TO DIGITAL TECHNOLOGY

CONTENT REVIEW GUIDE



**Johns Creek High School
Cmdr. Raymond T. Schenk
v1.1 11 December 2018**

This work is the student powered! My amazing students have come together to help assemble a work of information that is aligned by our course standards and put together to provide a fundamental platform for equipping future students at mastering the curriculum for this course.

Their hard work and leadership has made this entire guide possible, and they deserve the credit for amassing a wall of information, in service to their peers. I am forever grateful to their ability to leave a legacy for those come behind them.

INTRODUCTION TO DIGITAL TECHNOLOGY

IT-IDT-1 DEMONSTRATE EMPLOYABILITY SKILLS REQUIRED BY INDUSTRY

Professionalism

Definition of *professionalism*

1: the conduct, aims, or qualities that characterize or mark a profession or a professional person

<https://www.merriam-webster.com/dictionary/professionalism>



Things that show a lack of professionalism:

- Casual clothes, lack of effort in appearance
- Inappropriate language or volume of voice
- Missing deadlines with work
- Lack of motivation towards job responsibilities
- Blaming others for your mistakes
- Missing work
- Disrespectful behavior
- Unethical behavior or tolerance thereof

PROFESSIONALISM SHOULD BE MAINTAINED AT ALL TIMES IN THE WORKPLACE.

Things that indicate strong professionalism:

- Strong work ethic
- Creativity
- Working towards the mission of the company or organization
- Cooperation
- Service to others
- Self-regulation
- Motivated productivity and ambition
- Strong ethical performance
- Humility
- Proper Planning
- Respect for others

LANDING A JOB (AND KEEPING IT!) – INTERVIEW AND PRESENTATION TIPS:

- **Dress for success**
- Be on time for interviews and meetings
- Treat everyone with respect, even the janitors
- Know the company – prepare up front
- Be solution oriented
- Know what you want from the job
- Pre-think out answers:
 - Why do you want this job?
 - Why our company?
 - Tell us about yourself...
 - What is a mistake you've made?
- **BE GENUINE**



Common Outfit Tips

Men:

- Suit: matching jacket and pants, dress shirt, tie, coordinating socks and dress shoes.
 - Dark-colored suit with a light-colored shirt is best.
- Suit should be comfortable and fit well.
- Avoid loud colors or flashy ties.
- Clothing should be neat, clean, and pressed.
- Shower or bathe the morning of the interview.
- Wear deodorant. Don't wear cologne or aftershave.
- Make sure you have fresh breath. Brush your teeth before you leave for the interview, and don't eat before the interview. Don't smoke right before an interview.
- Your hair should be neat, clean, and conservative.

Women

- Suit with a skirt or pants.
- Suit should be comfortable and fit well.
- Interview suits should be simple and dark in color. Anything tight, bright, short, or sheer should be avoided. Knee-length skirts are suggested. Very long skirts, while modest, are considered too trendy for an interview.

- Wear a conservative blouse with your suit. Do not wear bright colors, animal prints, or anything lacy, sheer, or low-cut.
- Make-up and nail polish should be understated and flattering; shades that are neutral to your skin tone are generally advisable. Avoid bright or unusual colors or very long nails.
- Keep your jewelry and hair accessories to a minimum, and stick to those that are not flashy, distracting, or shiny. One ring per hand is best.
- Shoes should be conservative and fairly low-heeled. They should be in reasonably good condition. Don't wear shoes with an open toe or back.
- Your shoes should be neutral (matched to your skin tone). Make sure the heels are not dyed black from your shoes and that there are no snags or runs. Only use the nail polish trick in an emergency; you may want to carry an extra pair of shoes with you instead.



2.2 WORKING ON TEAMS

Principles for solid teamwork

“‘A’ players hire ‘A’ players.” - Steve Jobs

- Check your ego at the door.
- Be respectful
- Value the opinions of others, even if you disagree
- Find common ground
- Leave emotion out of it
- Clarify meaning – a lot!
- Never belittle ideas. Group think is the enemy of progress.
- **Hold focused meetings: mission first**

Spotting a good team:

1. Good leadership
2. They focus on goals and results
3. They communicate well with each other
4. They’re organized
5. Everyone contributes
6. They offer each other support

Ways to Develop Technical Reading and Writing

Reading

- **Survey chapters:** Read a summary, glance at headings & pictures, skim over the first sentence of each paragraph, pick out keywords.
- **Formulate Questions:** Create questions that allow you to summarize the material accurately and concisely, identifying the main topics.
- **Formulate answers to those questions:** Answer the questions you just asked to the best of your ability and call on prior knowledge from reading the summaries.
- **Actually read it:** After you’ve finished doing all this, read the entire thing selectively, so you may answer any of your unanswered questions. Confirm or deny your answers and correct them if incorrect.

Writing

- **Focus on the Tasks:** Ensure your writing is easy to follow, and not excessively wordy.
- **Don't make it personal:** Leave yourself out of the writing.
- **Be clear and concise**
- **Use visual aids:** Whether infographics, charts, or diagrams, they improve the clarity and retention of your writing.
- **Format your text:** No one likes looking at poorly formatted blocks of text. Include paragraph breaks, proper page breaks, inline visual aids, and well-formed paragraphs. Keep it simple, but appealing.

2.6 POST SECONDARY EDUCATION OPTIONS IN INFORMATINO TECHNOLOGY

College Majors Focusing on Technology

- **Computer Science**
- **Computer Programming**
- **Computer Graphics**
- **Artificial Intelligence**
- **Data Modeling**
- **Design Technology**
- **Computer Support Specialist**
- **Web Design**
- **Business Technology**
- **Information Technology Project Management**

IT-IDT-3 DEMONSTRATE EFFECTIVE PROFESSIONAL COMMUNICATION SKILLS (ORAL, WRITTEN, AND DIGITAL) AND PRACTICES THAT ENABLE POSITIVE CUSTOMER RELATIONSHIPS.

Customers bring profit to a company. Customer satisfaction reflects corporate success. Customers talk to their friends and family, and in today's social-media driven environment, can "go viral" at any time. Customer loyalty can mean long term success and can grow a company rapidly. Employees are happier when customers are happy.

General Rules for dealing with customers and clients:

- (Traditional) The customer is always right
- You must stop what you are doing and focus on the customer
- NEVER answer a phone when you are live with a customer
- Greet every customer appropriately
- Be positive and solve the needs of the customer
- Don't lie
- Know your product
- Care about the long-term relationship and needs of your client
- Get to know your client's business
- Anticipate the needs of your client
- Add value to the lives of your customers
- Listen – really *listen* to your clients

Customer Information

The balance between privacy and customer cultivation

Information about your customers can be worth its weight in gold – or cash. Maintaining a client list is critical in sales. You must respect your customer's privacy and protect all information they willingly give you.

Facebook is under immense pressure these days because they did not concern themselves with how their users would react when they realized they were harvesting everything about them for commercial use. Even though they were not directly selling information, they were making more of it available for high-paying businesses and data farms, which is effectively selling your customer information by another means.

There are a lot of ways to maintain customer contact:

- Software mailing lists and email lists (i.e. Constant Contact)
- Hashtag support and notifications
- Social media outreach campaigns and “like” campaigns
- Opt-in text messaging
- 24Hr support lines and chat support
- Hand-written greeting cards

Successful businesses have multiple ways for customers to reach out for help and support.

IT-IDT-4 IDENTIFY, DESCRIBE, EVALUATE, SELECT AND USE APPROPRIATE TECHNOLOGY.

IT-IDT-5 UNDERSTAND, COMMUNICATE, AND ADAPT TO A DIGITAL WORLD

Terminology and Definitions

Input Device - a piece of computer hardware equipment used to provide data to the computer.

Peripheral devices - a device that isn't part of the computer but is an attachment to a computer like a keyboard and a mouse but isn't part of the actual computer (Memory and Microprocessors).

Storage Hardware Devices

Tape drive - a data storage device that reads and writes data on a magnetic tape

Hard drive - data storage device that uses magnetic storage to store and retrieve digital information using one or more rigid rapidly rotating disks. Now refers to either spinning disks or Solid-State Drives (SSD).

Thumb Drive - a small electronic device containing flash memory that is used for storing data or transferring it to or from a computer

Spinning disks - A spinning disk is a mechanism within a hard disk drive to which memory is written. With rotating plates attached to an arm that writes the data

DVD Drives - Component that reads and writes information to DVDs

Firewall: A network device is designed to block unauthorized access while permitting authorized outward communication.

Host-Based Firewall: Software firewall services running on a host computer. Examples include firewalls included with MacOS and Windows operating systems.

Firewalls establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

Different types of firewalls

Proxy firewall

- An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application.
- Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network.

Stateful inspection firewall

- "Traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol.
- Monitors all activity from the opening of a connection until it is closed.

Unified threat management (UTM) firewall

- Combines the functions of a stateful inspection firewall with intrusion prevention and antiviruses. It may also include additional services and often cloud management. UTM's focus on simplicity and ease of use.
- **Personal firewalls** are usually smaller and compact and therefore cheaper. A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

A Personal firewall is important when

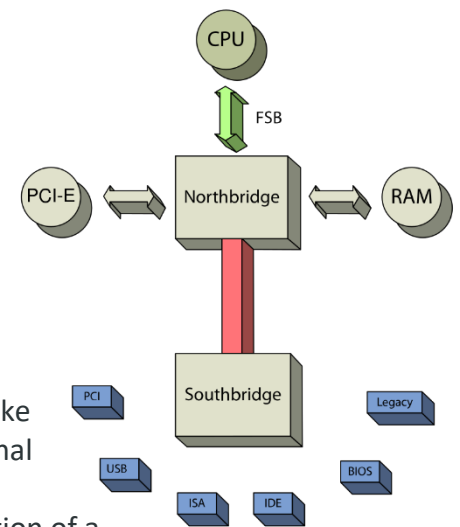
- You surf the internet at home using an 'always on' broadband connection
- You connect to the internet via public Wi-Fi, as in a park, cafe or airport
- You run a home network which needs to be kept isolated from the internet
- You wish to be kept informed when any program on your computer attempts to connect to the internet
- Most Personal Firewalls are highly configurable, so you can easily create security policies to suit your individual needs

What Firewalls actually do?

- Defend resources
- Validate access
- Manage and control network traffic
- Record and report on events
- Act as an intermediary

1. **Random Access Memory (RAM)**- electronic circuits in a computer that can store code and data of running programs.
2. **Read Only Memory (ROM)** – electronic memory that can be written at a factory (typically) and read over and over again once inserted into a circuit board or motherboard to load information for use by a computing system
3. **Programmable Read Only Memory (PROM)** – A memory chip that was writeable once and read-many that began to become usable by others besides manufacturers
4. **Erasable Programmable Read Only Memory (EPROM)** – This was memory chips that could be electrically erased and reprogrammed then read-many. Early BIOS chips in motherboards were EPROMS.
5. **Electrically Erasable Programmable Read Only Memory (EEPROM)** – modern BIOS chips and the root system memory for small devices like cell phones are EEPROM. These chipsets can be flash overwritten electrically to have their software instruction sets updated.
6. **Basic Input Output System (BIOS)** – The first program that runs when you power up your computer. Located (stored) on the computer's BIOS Chip (EEPROM).
7. **CMOS** – Complementary Metal-Oxide Semiconductor – This chip holds the basic settings like the date-time for a computer. It is powered to store its settings by the CMOS battery (wafer battery stored on a motherboard)

8. **Central Processing Unit (CPU)**- the part of a computer (a microprocessor chip) that does most of the data processing
9. **North Bridge** – Connected directly to CPU via the front-side bus. Responsible for tasks requiring the highest performance. (CPU, RAM, PCI-E)
10. **South Bridge** – Often called the I/O Controller Hub (ICH). Connects to the North Bridge, then connects in other busses like PCI, USB, ISA, IDE, the BIOS, Hard Drives, Legacy busses, external devices, keyboard, mouse. This is the slower side.
11. **System Software**- software responsible for the general operation of a computer system, including the operation of hardware, running application software, and file management
12. **Copyright**- a form of protection provided by the laws of the United States to the “original works of authorship.”
13. **Encryption**- a security measure by cryptographical means which secures information even if there are interceptions
14. **Data Mining**- a method in which large databases of popular websites are examined to find user behavior, patterns, and trends
15. **User Interface/ User Experience (UI/UX)**- User interface includes all the parts of the website, apps, or technological device that interact with the user whereas user experience is the emotions and accessibility of a product. The user experience can be modified to be more efficient.
16. **Elements**- all the HTML components of a website
17. **Semantic Elements**- HTML elements which cannot be physically seen on a website
18. **Back End**- all the parts of a website that make it run including applications, web servers, and databases and is usually not visible to the user
19. **Bugs** - the coding mistakes or unnecessary pieces of code that prevent a website/program from working properly
20. **Frameworks** - collection of programs that developers can use to develop software (ex. Ruby on Rails and Bootstrap)
21. **Version Control** - tool used to store changes to code/files on a website or app which allows the user to restore previous versions in case of a bug
22. **Caching** - when a web browser stores information about a website (images/font/etc.) in order for it to load faster when a user revisits the page
23. **Cloud Computing** - the storing and processing of data among several remote servers accessible through the internet as opposed to locally on a computer
24. **Virtual Private Network (VPN)** - networks that allow private networks to use public internet connections in order to improve security
25. **Relational Database Management System (RDBMS)** - systems used to organize data into tables which can then be accessed without the need to reorganize the tables
26. **Hybrid app** - apps that work on different platforms and which are a combination of a native app (stored locally on a device) and a web app (accessible through the Internet)



Computer Virus – Malicious Software that can replicate itself

Malware – Any unwanted software on your computer

Trojan Software – Software that carries a malicious payload, while pretending to be normal software.

Backdoor - A backdoor Trojan is a loophole into the infected computer through remote control. The author gains complete access to, and control over all files and data. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.

Exploits- Exploits are programs that contain data or code that takes advantage of a vulnerability within application software that's running on your computer.

Rootkits-Rootkits extend the longevity of viruses by concealing certain objects or activities in your computer system.

Trojan-Banker - designed to steal your account data for online banking systems, e-payment systems and credit or debit cards.

Trojan-DDoS - conduct DoS (Denial of Service) attacks against a targeted web address. By sending multiple requests – from your computer and several other infected computers – the attack can overwhelm the target address... leading to a denial of service.

Trojan-Downloader - download and install new versions of malicious programs onto your computer – including Trojans and adware.

Trojan-Dropper - Hackers use these programs to install Trojans, malicious programs and/or viruses undetected. Not all antivirus programs can scan all the components in these Trojans.

Trojan-FakeAV - They simulate activity of antivirus software. In reality they simply require money in return for reports of fake threats.

Trojan-Ransom - This type of Trojan can encrypt data on your computer – so that your computer doesn't run correctly, or you can no longer use specific data. The criminal will only restore your computer's performance or decrypt your data, after you have paid them the ransom money that they demand.

Trojan-Spy - Trojan-Spy programs can spy on how you're using your computer – for example, by tracking the data you enter via your keyboard, taking screenshots or getting a list of running applications.

Keyloggers – Malicious code or spyware that logs and sometimes transmits every keystroke you make while operating your computer. Can be used to determine accounts, usernames, and passwords.

NETWORKING DEVICES AND VOCABULARY

Peer-to-Peer Network – All computers equally share resources. Every computer is a peer.

Client-Server Network – Server enables multiple clients to share its resources. Functions are centralized and hosted by a set of network “servers.” Servers also provide security.

LAN – Local Area Network – Single office, home, school, etc.

CAN – Campus Area Network. Because colleges want a fancy network name too!

PAN – Personal Area Network – Individual network (i.e. phone, laptop, tablet, wireless earbuds)
(No association with the flying boys)

WAN – Wide Area Network – Wide geographically, often leased telecommunications services

MAN – Metro Area Network – Metropolitan network, single city or town.

Wireless Access Point (WAP) – Network device that wirelessly connects multiple devices to a given network

Network Standards – Rules that establish interoperability across networks. (OSI Model is largest set of network standards)

Network Security – Software and appliances on networks and computers to prevent and limit unauthorized access to resources.

Network Address – An identifier for a node on a network. Should be unique. Receiving and Internet Protocol Address is how one is considered to be “connected to the Internet.”

Network Diagnostics – Software designed to help users and network administrators monitor and troubleshoot connections to the network or Internet.

NETWORK TOPOLOGIES:

There are two main distinctions:

1. **Physical Network** – How hardware is connected
2. **Logical Network** - How data flows

Bus – 1 Cable, everything connected to that. Single point of failure

Ring – Unit connected in a ring (Common in fiber), single point of failure

Star – Every bus connected to a central hub, single point of failure

Full Mesh – Everyone connected to everyone, most failsafe, multiple paths, **most expensive**

With n devices in full mesh, total number of dedicated links is calculated by $(n(n-1))/2$*

*So if 5 devices are fully meshed, $5*4/2 = 10$ connections required.*

COMMON NETWORK HARDWARE

Switch – Comes in *smart* switches and *dumb* switches. Smart switches have additional software and configuration/monitoring capabilities. Dumb switches are plug-and-play, often for home and small office use. Old names include switching Hub, Bridging Hub, MAC Bridge.

“Switches build networks.”

Routers – Routers connect networks to other networks.

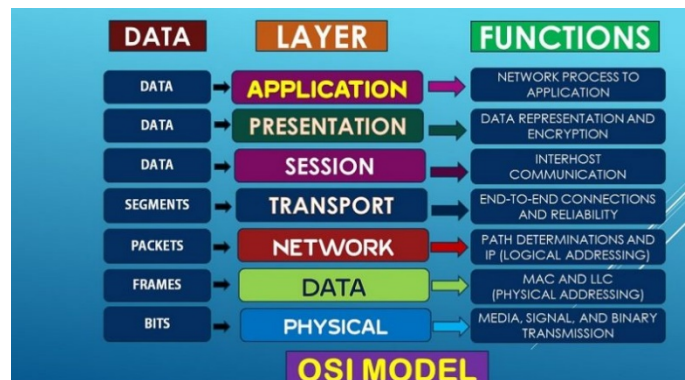
Network Interface Card (NIC) – Hardware that connects a computer to a network. Today most often part of motherboards or main boards.

Network Interface – Software that connects a computing device to a network.

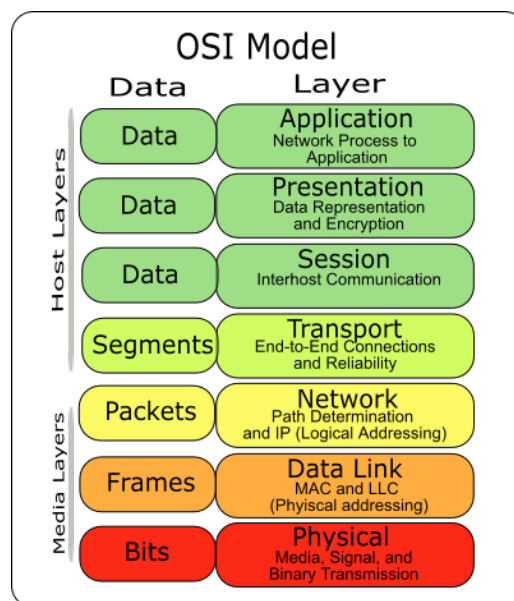
Blacklisting/Whitelisting – Firewalls either blacklist or whitelist. Whitelisting means no site traffic can access network unless it is on the whitelist. Blacklisting means any traffic can enter unless it is on the blacklist. Can also be applied to specific file formats for high-speed guards that do deep packet inspection.

Network Gateway – allows on LAN to link to another LAN

THE OSI MODEL FOR THE INTERNET



<https://proxy.duckduckgo.com/iu/?u=https%3A%2F%2Fkailashafoundation.org%2Fwp-content%2Fuploads%2F2017%2F06%2Fosi-2-806x440.jpg&f=1>



<https://proxy.duckduckgo.com/iu/?u=https%3A%2F%2Fnetworksmania.files.wordpress.com%2F2012%2F03%2Fdata-link.png&f=1>

Layer 7: Application Layer

Services end-user applications. Works with the data, as in a web browser, to display or send information via the presentation layer.

Layer 6: Presentation Layer

Format conversions and encryption/decryption. This is the “file format” layer, where files are reconstituted or broken down depending on which direction of the stack information is moving.

Layer 5: Session Layer

Manages sequence and flow that initiates and tears down connections across networks. Multiple types of connections can occur at Layer 5.

Layer 4: Transport Layer (TCP)

This layer delivers data across the network connections. TCP is the most common example of a transport Layer 4 network protocol. TCP controls error recovery, flow control, and re-transmission controls. Also the Layer of Uniform Datagram Protocol (UDP) Packets.

Layer 3: Network Layer (IP)

The network layer adds the concept of routing. Frame data is inspected to see if it has reached its destination. If so, the data is formatted up to the transport layer. IP Addresses are maintained at this layer. Mapping is achieved through the Address Resolution Protocol (ARP).

Layer 2: Data Link Layer

The data link layer deals in frames. It is the most complex layer of the OSI model, it is often subdivided into two layers, the MAC layer and the Logical Link Control Layer (LLC)

Layer 1: Physical Layer

The physical layer is responsible for the actual transmission of bits. It consists of the actual hardware required to achieve this, including cables, fiber, hubs, repeaters, microwave transceivers, etc.

MORE TERMINOLOGY

UDP Packets – send streaming without the controls of TCP. Live broadcasts. Need fast arrival, but not the delays inherent in TCP guaranteed delivery.

Packet – formatted unit of data carried across packet-switching networks.

Dynamic Host Configuration Protocol (DHCP) Server – A server that assigns IP addresses either dynamically, or statically to devices wishing to join a network.

Domain Name Service – translates domain names into IP addresses so humans don't have to do so. This is how www.mysite.com becomes 60.123.22.123.

IPv4 – Internet Protocol Version 4. Uses 32 bits. World running out of IP addresses despite using internal IP for individual networks. (4.3 billion addresses) Format: 255.255.255.255

IPv6 - Internet Protocol Version 6. Uses 128 bits. 8 Words (8 x 2-bytes) separated by colons. (3.4x10³⁸ available addresses). Format: FF:FF:FF:FF:FF:FF:FF:FF

Secured Socket Layer – hackable precursor to TLS security.

Transport Layer Security (TLS) – Replaced SSL, is a stateful connection. Provides:

- Data encrypted symmetric encryption/decryption
- Authentication via the encryption
- Reliable Data-Message Authentication Codes (MAC ID) to detect unauthorized data modification or loss

THE FIRST ABSTRACTION: HOW COMPUTERS REPRESENT DATA

ANSI - American National Standards Institute – American non-profit organization that develops and maintains standards for industry.

ASCII – American Standard for Information Interchange. Written and developed/maintained by ANSI. ASCII was the world's answer to defeat IBM's EBCDIC

ASCII DIGITS

011 0001	1
011 0010	2
011 0011	3
011 0100	4
011 0101	5

ASCII CHARACTERS (UPPER CASE)

100 0001	A
100 0010	B
100 0011	C
100 0100	D
100 0101	E

ASCII CHARACTERS (LOWER CASE)

110 0001	a
110 0010	b
110 0011	c
110 0100	d
110 0101	e

ASCII CHARACTERS (SPECIAL CASE)

000 0000	Null
111 1111	Delete

- Computers use 7 bits for ASCII (8 bit is 0) – Fits in a single byte
- Extended ASCII uses the extra bit to add more characters but contains ASCII perfectly.
- UNICODE uses between 1 and 4 bytes, *usually* containing a character. It contains all of ASCII and a lot more characters and combinations of accents. It **does not** contain every character of every language, but many say it tries to do so.

Storage Area Network (SAN) – an array of hard drives that ship only with low level block I/O capabilities. Must be formatted and initialized under a specific operating system's disk management protocols. These units are typically very large and expensive.

Network Accessible Storage (NAS) – more affordable hard drive space that can be accessed by users on a network. Many home and small offices use RAID-based NAS devices for storing and/or backing up valuable files.

Virtual Private Network – A network that allows users to access its resources via an encrypted session. VPNs provide security to an organizations network but can be considered a vulnerability to networks hosting users who use them.

IT-IDT-7 USE COMPUTATIONAL THINKING TO ANALYZE AND SOLVE PROBLEMS

PSEUDO CODING


Advantages of pseudocode:

- Pseudocode is understood by the programmers of all types.
- It enables the programmer to concentrate only on the algorithm part of the code development.
- It cannot be compiled into an executable program.

Pseudocode is basically just writing down the logic of your solution to a specific coding using plain English. Pseudocode is a useful thing to learn because it focuses on the building block concepts of programming languages without you having to worry about your word choice.

FLOW CHARTING

Symbol	Purpose	Description
	Flow line	Used to indicate the flow of logic by connecting symbols.
	Terminal(Stop/Start)	Used to represent start and end of flowchart.
	Input/Output	Used for input and output operation.
	Processing	Used for arithmetic operations and data-manipulations.
	Decision	Used to represent the operation in which there are two alternatives, true and false.
	On-page Connector	Used to join different flowline
	Off-page Connector	Used to connect flowchart portion on different page.

	Predefined Process/Function	Used to represent a group of statements performing one processing task.
---	-----------------------------	---

IT-IDT-8 CREATE AND ORGANIZE WEB PAGES THROUGH THE USE OF WEB PROGRAMMING DESIGN TOOLS

HTML

```
<!DOCTYPE html>
```

```
<html>
```

```
  <head>
```

```
    <link href="filename.css" rel="stylesheet" type="text/css" />
```

```
    <title>Title of tab goes here</title>
```

```
  </head>
```

```
  <body>
```

ALL HTML-5 TAGS GO IN THE BODY

```
  </body>
```

```
</html>
```

HTML 5 TAGS

<Header></Header>	Top area for a major section of a web page
<Article></Article>	Most scored for SEO Content
<Nav></Nav>	Holds navigational menus and links
<Footer></Footer>	bottom section of each major section of a web page



Global Selector. Everything on a linked web page is styled with this selector's commands

[tag name] Type Selector. Used to style every tag of the named tagname, Styles every occurrence of the given tag. For example:

```
h2 {  
  
    font-color: red;  
  
}
```

Will style every single h2 tag with a red font.



ID Selector. Used with a name, as in #mainBorder. The html tag styled with this ID would look like this: <div id="mainBorder"> ID selectors are to be used once and only once. This tag is used for a strict 1:1 styling of a single element in a web page.



Class Selector. Used with a name as well. Example is .contentParagraph. The html with this class would look like this: <div class="contentParagraph"> Class selectors can be used 1-to-many. This means this class can be assigned to any number of tags of type class="contentParagraph" as needed. Classes are the most used style selector of all.

A given tag may have an ID and a class.

WEB DESIGN AND COLOR

RGB – Red Green Blue

(255,255,255) = white

((0,0,255) = Blue

(0,0,0) = black

RGBA Adds **Opacity (0-1)**

(255,0,0) = Red

(255,0,0,0) = "Transparent Red"

(0,255, 0) = Green

(0,0,255,0.4) = 40 percent visible blue

IT-IDT-9 DESIGN, DEVELOP, TEST AND IMPLEMENT PROGRAMS USING VISUAL PROGRAMMING.

Scratch Programming was designed by the Lifelong Kindergarten Group at MIT's Media labs.

Scratch is a visual block-programming language.

Scratch was originally built in JavaScript but is being translated into HTML-5.

In scratch it is best to program with only a single green flag, so achieve event driven programming.

The closest thing to writing your own method (abstraction) is a custom puzzle piece, which can be constructed and then reused wherever possible.

IT-IDT-10 DESCRIBE, ANALYZE, DEVELOP AND FOLLOW POLICIES FOR MANAGING ETHICAL AND LEGAL ISSUES IN THE BUSINESS WORLD AND IN A TECHNOLOGY-BASED SOCIETY.

Copyright is stronger in Georgia than Patents.

Software can be copywritten because it is a language.

Using computers to commit crimes is just as bad as committing traditional crimes. Theft is theft.

Cyber-bullying can take on many forms.

Just because something is technically legal, does not make it ethical. Ethics often involves avoiding even the ***appearance*** of impropriety.

IT-IDT-11 EXPLORE HOW RELATED STUDENT ORGANIZATIONS ARE INTEGRAL PARTS OF CAREER AND TECHNOLOGY EDUCATION COURSES THROUGH LEADERSHIP DEVELOPMENT, SCHOOL AND COMMUNITY SERVICE PROJECTS, ENTREPRENEURSHIP DEVELOPMENT, AND COMPETITIVE EVENTS.

FBLA Stands for the Future Business Leaders of America.

FBLA members compete at the regional, state, and national levels.

FBLA colors are blue and gold.

EXTENDED LEARNING

Software Development Life-Cycle (SDLC)

Waterfall – oldest, slowest, very inflexible, Linear

Others: Prototyping, Spiral

Best: Agile

Individuals and Interactions over processes and tools

Working Software over comprehensive documentation

Customer Collaboration over contract negotiation

Responding to Change over following a plan

Runs in Sprints, is Iterative, Incremental and evolutionary

Scrum is a specific software development agile methodology. 3-9 members. 2-4 weeks max sprints. Daily scrums are 15-min re-planning meetings.