FREEHOLD REGIONAL HIGH SCHOOL DISTRICT
OFFICE OF CURRICULUM AND INSTRUCTION
FRHSD PATHWAY PROGRAMS CURRICULUM

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals

Grade Level: 12

Credits: 5.0

BOARD OF EDUCATION ADOPTION DATE: August 27, 2025

FREEHOLD REGIONAL HIGH SCHOOL DISTRICT

Board of Education

Mr. Pete Bruno, President
Mr. Michael Messinger, Vice President
Mr. Carl Accettola
Mrs. Jamie Bruno
Ms. Joan Butcher-Farkas
Ms. Diana Cappiello
Mrs. Liz Higley
Mrs. Kathie Lavin
Ms. Amanda McCobb

Central Administration

Dr. Nicole Hazel, Superintendent
Dr. Shanna Howell, Chief Academic Officer
Dr. Oscar Diaz, Administrative Supervisor of Curriculum and Instruction
Ms. Stephanie Mechmann, Administrative Supervisor of Curriculum and Instruction
Ms. Jennifer Okerson, Administrative Supervisor of Curriculum and Instruction
Mr. Brian Simpson, Administrative Supervisor of Curriculum and Instruction

Curriculum Writing Committee

Ms. Cindy Bravaco
Mr. Michael Cappiello
Ms. Kimberly Cincotta
Mr. Brian Gadaleta

Supervisors

Mr. Michael K. Dillon
Ms.Kristine Jenner

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals

Course Description

The Cybersecurity Fundamentals course, a course from Fairleigh Dickinson University - Early College Dual Enrollment Program, is a comprehensive introduction to the essential principles, technologies, and practices that form the backbone of effective cybersecurity. In an era where digital threats continue to evolve, this course equips participants with the foundational knowledge required to build a solid understanding of cybersecurity concepts. The course explores the role of IT governance in maintaining a resilient cybersecurity posture and the ethical considerations in cybersecurity. The course employs a blend of lectures, hands-on labs, case studies, and practical exercises to provide participants with a holistic learning
Experience.

Learning Outcomes/Course Objectives

1. Students will be introduced to the fundamental concepts of cybersecurity, taxonomy, threats, attacks, and vulnerabilities.
2. Students will learn the type of system attacks, actors and attack vectors related to computers and network security.
3. Students will learn different defense tools available to secure computers and networks from attacks. Tools will include firewalls, Intrusion Detection System and others. Countermeasure and mitigation strategy will be explored.
4. Data Protection and Privacy to examine strategies for safeguarding data, ensuring privacy compliance, and implementing encryption techniques.
5. Students will be able to document network security and explore issues arising from connecting networks to the Internet.
6. Students will be able to document Cryptography and encryption techniques to secure communications over networks.
7. Explore the role of governance in maintaining a resilient cybersecurity posture and ensuring compliance with industry standards and regulations.
8. Discuss ethical considerations in cybersecurity, emphasizing responsible and lawful
behavior in the cybersecurity profession.

Course Sequence and Pacing

Unit Title	Content Statement / Unit Focus OR Section Focus	Suggested Pacing
Unit 1: Building Your Personalized Cybersecurity Learning Plan	Section 1.1: Topic 1: Reflecting on Past Experiences Section 1.2: Certification Preparation (Google Certificate, CompTIA+, etc.)	5 Sessions
Unit 2: Preparing for your Cybersecurity Career	Section 2.1: Topic 1: Resume Building Section 2.2: Topic 2: Interviewing Skills Section 2.3: Topic 3: Building a Personal Brand Section 2.4: Topic 4: College Advising Section 2.5: Topic 5: Career Planning Section 2.6: Certification Preparation (Google Certificate, CompTIA+, etc.)	20 Sessions
Unit 3: CSCI_2157 Cybersecurity Fundamentals: Modules 1, 2 &3: Fairleigh Dickinson University	Section 3.1: CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University **Module 1** ● Information Technology Building Blocks ● CIA Principle - Confidentiality, Integrity, and Availability ● Fundamental concepts of cybersecurity, taxonomy, threats, attacks, and vulnerabilities. Type of system attacks, actors, and attack vectors related to computers and network security. ● Defense tools available to secure computers and networks from attacks. Tools will include firewalls, Intrusion Detection System, and others. ● Countermeasures and mitigation strategies will be explored. Section 3.2: CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University **Module 2**	70 Sessions

	● Data Protection and Privacy to examine strategies for safeguarding data, ensuring privacy compliance, and implementing encryption techniques. ● Network security and explore issues arising from connecting networks to the Internet. ● Cryptography and encryption techniques to secure communications over networks. Section 3.3: CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University **Module 3** ● The role of IT governance in maintaining a resilient cybersecurity posture and ensuring compliance with industry standards and regulations. ● Ethical considerations in cybersecurity 3.4: Certification Preparation ● Google Certificate, ● CompTIA+	
Unit 4: Cybersecurity Capstone Project	Section 4.1: Capstone Kickoff & Project Planning Section 4.2: Designing a Secure Network Architecture Section 4.3: Risk Assessment and Threat Modeling Section 4.4: Cybersecurity Policy & Legal/Ethical Issues Section 4.5: Testing & Defense Simulation Section 4.6: Final Presentation & Reflection	25 Sessions

Support Resources

Supporting resources and appendices for this curriculum are available. These include a Resource Catalog of standards-aligned activities, common formative assessment and interdisciplinary items for performance expectations and objectives in this course.

- Cybersecurity PAthway Program Resource Catalog
- Appendix A: Accommodations and Modifications for Various Student Populations
- Appendix B: Assessment Evidence
- Appendix C: Interdisciplinary Connections

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Suggested Pacing: 5 sessions** **Unit 1: Building Your Personalized Cybersecurity Learning Plan** **Section 1.1: Topic 1: Reflecting on Past Experiences**
NJSLS-SS Performance Expectations
9.4.12.CI.3: Investigate new challenges and opportunities for personal growth, advancement and transition
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
Identify strengths, such as problem-solving skills, programming proficiency, or a strong interest in ethical hacking

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Suggested Pacing: 1 session** **Unit 1: Building Your Personalized Cybersecurity Learning Plan** **Section 1.2: Certification Preparation (Google Certificate, CompTIA+, etc.)**
NJSLS-SS Performance Expectations
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
Students will perform: ●Programming for cyber security tasks ●Frameworks and controls that inform security operations ●Use security information and event management (SIEM) tools for cybersecurity ●Detect and respond to incidents using an intrusion detection system ●Perform packet capture and analysis ●Use AI to boost productivity

HONORS Fairleigh Dickinson University

CSCI_2157 Cybersecurity Fundamentals **Unit 2: Preparing for your Cybersecurity Career** **Section 2.1: Topic 1: Resume Building**	**Suggested Pacing: 3 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Create a professional cyber security resume tailored to specific roles and career goals.	

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Unit 2: Preparing for your Cybersecurity Career** **Section 2.2: Topic 2: Interviewing Skills**	**Suggested Pacing: 3 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.6 Identify transferable skills in career choices and design alternative career plans based on those skills.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Develop effective interview techniques and strategies to confidently navigate different types of cyber security job interviews.	

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Unit 2: Preparing for your Cybersecurity Career** **Section 2.3: Topic 3: Building a Personal Brand**	**Suggested Pacing: 3 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Explain the importance of a personal brand and how to build one that reflects individual strengths, values, and career aspirations.	

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Unit 2: Preparing for your Cybersecurity Career** **Section 2.4: Topic 4: College Advising**	**Suggested Pacing: 3 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Explore and evaluate different college programs, scholarships, and financial aid options related to cybersecurity education.	

HONORS Fairleigh Dickinson University

CSCI_2157 Cybersecurity Fundamentals **Unit 2: Preparing for your Cybersecurity Career** **Section 2.5: Topic 5: Career Planning**	**Suggested Pacing: 3 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Apply strategies for effective job searching, networking, and planning a cybersecurity career path.	

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Unit 2: Preparing for your Cybersecurity Career** **Section 2.6: Certification Preparation (Google Certificate, CompTIA+, etc.)**	**Suggested Pacing: 5 sessions**
NJSLS-SS Performance Expectations	
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Students will perform: ●Programming for cyber security tasks ●Frameworks and controls that inform security operations ●Use security information and event management (SIEM) tools for cybersecurity ●Detect and respond to incidents using an intrusion detection system ●Perform packet capture and analysis ●Use AI to boost productivity	

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Unit 3 CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University** **Section 3.1: Module 1 (Introduction to IT Components, Core Cybersecurity Principles, Key Cybersecurity Concepts, Understanding Attacks and Threat Actors, Cybersecurity Tools and Defenses & Responding to Threats and Mitigating Risk)**	**Suggested Pacing: 20 sessions**
NJSLS-SS Performance Expectations	
9.3.IT-PRG.7 Demonstrate software testing procedures to ensure quality products. 9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements. 9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Review the basics of cybersecurity by exploring how technology works, understanding key security principles, identifying threats and attacks, and using tools and strategies to protect computers and networks.	
■ Identify and describe the basic building blocks of information technology including hardware, software, and network components.	
■ Explain the CIA Triad (Confidentiality, Integrity, Availability) and how it forms the foundation of cybersecurity principles.	
■ Define and discuss key cybersecurity concepts, including threats, attacks, vulnerabilities, and the overall taxonomy of cyber risks.	
■ Recognize different types of system attacks, attack vectors, and threat actors commonly associated with computer and network security breaches.	

■ Identify and describe key cybersecurity defense tools, such as firewalls and Intrusion Detection Systems (IDS), and explain how they are used to protect systems and networks.

■ Develop and evaluate basic countermeasures and mitigation strategies to reduce cybersecurity risks and respond to potential threats effectively.

HONORS Fairleigh Dickinson University
CSCI_2157 Cybersecurity Fundamentals **Suggested Pacing: 20 sessions**
Unit 3 CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University
Section 3.2: Module 2 (Data Protection and Privacy, Network Security Basics & Introduction to Cryptography)

NJSLS-SS Performance Expectations

9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.

Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:

Demonstrate understanding of how to protect data and networks, use encryption to keep information secure.

■ Describe strategies for data protection and privacy, including methods for safeguarding personal and organizational data, ensuring compliance with privacy laws, and applying encryption techniques.

■ Explain key concepts in network security and analyze common vulnerabilities and risks associated with connecting networks to the Internet.

■ Demonstrate an understanding of cryptography, including how encryption techniques are used to secure communications and protect data integrity.

HONORS Fairleigh Dickinson University
CSCI_2157 Cybersecurity Fundamentals **Suggested Pacing: 15 sessions**
Unit 3 CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University
Section 3.3: Module 3 (IT Governance and Cybersecurity & Ethics in Cybersecurity)

NJSLS-SS Performance Expectations

9.4.12.CI.3 Investigate new challenges and opportunities for personal growth, advancement and transition
9.3.IT.4 Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.
9.4.12.DC.3 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:

■ Understand how IT governance supports effective cybersecurity practices
■ Evaluate the ethical responsibilities involved in protecting information systems, ensuring compliance, and making decisions that impact individuals and society.

■ Explain the role of IT governance in supporting a strong and resilient cybersecurity framework, including how it helps organizations comply with industry standards and regulatory requirements.

■ Analyze ethical considerations in cybersecurity, such as responsible use of information, the impact of security decisions on privacy and society, and the ethical responsibilities of cybersecurity professionals.

HONORS Fairleigh Dickinson University
CSCI_2157 Cybersecurity Fundamentals **Suggested Pacing: 15 sessions**
Unit 3 CSCI_2157 Cybersecurity Fundamentals - Fairleigh Dickinson University
Section 3.4: Certification Preparation (Google Certificate, CompTIA+, etc.)

NJSLS-SS Performance Expectations
9.2.12.CAP.7 Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
Students will perform: ●Programming for cyber security tasks ●Frameworks and controls that inform security operations ●Use security information and event management (SIEM) tools for cybersecurity ●Detect and respond to incidents using an intrusion detection system ●Perform packet capture and analysis ●Use AI to boost productivity

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Suggested Pacing: 4 sessions** **Unit 4 Cybersecurity Capstone Project** **Section 4.1: Capstone Kickoff & Project Planning**
NJSLS-SS Performance Expectations
8.1.12.NI.2: Evaluate security measures to address various common security threats.
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
●Understand project expectations, define team roles, and plan the timeline. ●Review the cybersecurity lifecycle (Identify, Protect, Detect, Respond, Recover).

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Suggested Pacing: 5 sessions** **Unit 4 Cybersecurity Capstone Project** **Section 4.2: Designing a Secure Network Architecture**
NJSLS-SS Performance Expectations
8.1.12.NI.2: Evaluate security measures to address various common security threats.
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
●Design a network that includes routers, firewalls, user access controls, and encryption methods. ●Apply the CIA Triad to their design.

HONORS Fairleigh Dickinson University **CSCI_2157 Cybersecurity Fundamentals** **Suggested Pacing: 4 sessions** **Unit 4 Cybersecurity Capstone Project** **Section 4.3: Risk Assessment and Threat Modeling**

NJSLS-SS Performance Expectations
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:
●Identify potential threats, attack vectors, and vulnerabilities. ●Propose basic risk mitigation strategies.

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals **Unit 4 Cybersecurity Capstone Project** **Section 4.4: Cybersecurity Policy & Legal/Ethical Issues**	**Suggested Pacing: 4 sessions**
NJSLS-SS Performance Expectations	
9.3.IT.4 Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
Develop an internal cybersecurity policy addressing data protection, user behavior, and response plans. Analyze the ethical and legal responsibilities of cybersecurity professionals.	

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals **Unit 4 Cybersecurity Capstone Project** **Section 4.5: Testing & Defense Simulation**	**Suggested Pacing: 4 sessions**
NJSLS-SS Performance Expectations	
9.3.IT-SUP.5 Demonstrate the use of networking concepts to develop used in a network.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
●Evaluate system resilience through testing and simulated incidents. ●Refine designs based on outcomes and feedback.	

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals **Unit 4 Cybersecurity Capstone Project** **Section 4.6: Final Presentation & Reflection**	**Suggested Pacing: 4 sessions**
NJSLS-SS Performance Expectations	
9.4.12.CI.1 Demonstrate the ability to reflect, analyze and use creative skills and ideas.	
Standards-Aligned Objectives. Instruction and assessment will align to the following objectives:	
●Synthesize project findings into a coherent presentation. ●Reflect on teamwork, technical learning, and future cybersecurity goals.	

HONORS Fairleigh Dickinson University CSCI_2157 Cybersecurity Fundamentals	
Career Readiness, Life Literacies, and Key Skills	Unit

9.2.12.CAP.1	Analyze unemployment rates for workers with different levels of education and how the economic, social, and political conditions of a time period are affected by a recession.	
9.2.12.CAP.2	Develop college and career readiness skills by participating in opportunities such as structured learning experiences, apprenticeships, and dual enrollment programs.	
9.2.12.CAP.3	Investigate how continuing education contributes to one's career and personal growth.	
9.2.12.CAP.4	Evaluate different careers and develop various plans (e.g., costs of public, private, training schools) and timetables for achieving them, including educational/training requirements, costs, loans, and debt repayment.	
9.2.12.CAP.5	Assess and modify a personal plan to support current interests and postsecondary plans.	
9.2.12.CAP.6	Identify transferable skills in career choices and design alternative career plans based on those skills.	
9.2.12.CAP.	Use online resources to examine licensing, certification, and credentialing requirements at the local, state, and national levels to maintain compliance with industry requirements in areas of career interest.	
9.2.12.CAP.8	Determine job entrance criteria (e.g., education credentials, math/writing/reading comprehension tests, drug tests) used by employers in various industry sectors.	
9.2.12.CAP.9:	Locate information on working papers, what is required to obtain them, and who must sign them.	
9.2.12.CAP.10	Identify strategies for reducing overall costs of postsecondary education (e.g., tuition assistance, loans, grants, scholarships, and student loans).	
9.2.12.CAP.11	Demonstrate an understanding of Free Application for Federal Student Aid (FAFSA) requirements to apply for postsecondary education.	
9.2.12.CAP.12	Explain how compulsory government programs (e.g., Social Security, Medicare) provide insurance against some loss of income and benefits to eligible recipients.	
9.2.12.CAP.13	Analyze how the economic, social, and political conditions of a time period can affect the labor market.	
9.2.12.CAP.14	Analyze and critique various sources of income and available resources (e.g., financial assets, property, and transfer payments) and how they may substitute for earned income.	
9.2.12.CAP.15	Demonstrate how exemptions, deductions, and deferred income (e.g., retirement or medical) can reduce taxable income.	
9.2.12.CAP.16	Explain why taxes are withheld from income and the relationship of federal, state, and local taxes (e.g., property, income, excise, and sales) and how the money collected is used by local, county, state, and federal governments.	
9.2.12.CAP.17	Analyze the impact of the collective bargaining process on benefits, income, and fair labor practice.	
9.2.12.CAP.18	Differentiate between taxable and nontaxable income from various forms of employment (e.g., cash business, tips, tax filing and withholding).	
9.2.12.CAP.19	Explain the purpose of payroll deductions and why fees for various benefits (e.g., medical benefits) are taken out of pay, including the cost of employee benefits to employers and self-employment income.	
9.2.12.CAP.20	Analyze a Federal and State Income Tax Return.	
9.2.12.CAP.21	Explain low-cost and low-risk ways to start a business.	
9.2.12.CAP.22	Compare risk and reward potential and use the comparison to decide whether starting a business is feasible.	
9.2.12.CAP.23	Identify different ways to obtain capital for starting a business.	
9.4.12.CI.1	Demonstrate the ability to reflect, analyze and use creative skills and ideas.	
9.4.12.CI.2	Identify career pathways that highlight personal talents, skills and abilities.	
9.4.12.CI.3	Investigate new challenges and opportunities for personal growth, advancement and transition	
9.4.12.CT.1	Identify problem-solving strategies used in the development of an innovative product or practice.	
9.4.12.CT.2	Explain the potential benefits of collaborating to enhance critical thinking and problem solving.	

9.4.12.CT.3	Collaborate with individuals to analyze a variety of potential solutions to climate change effects and determine why solutions may work better than others (e.g., political. economic, cultural).	
9.4.12.CT.4	Enlist input from a variety of stakeholders (e.g., community members, experts in the field) to design a service learning activity that addresses a local or global issue (e.g., environmental justice).	
9.4.12.CT.5	Participate in online strategy and planning sessions for course-based, school-based or other projects and determine the strategies that contribute to effective outcomes.	
9.4.12.DC.1	Explain the beneficial and harmful effects that intellectual property laws can have on the creation and sharing of content.	
9.4.12.DC.2	Compare and contrast international differences in copyright laws and ethics.	
9.4.12.DC.3	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.	
9.4.12.DC.4	Explain the privacy concerns related to the collection of data (e.g.,cookies) and generation of data through automated processes that may not be evident to users.	
9.4.12.DC.5	Debate laws and regulations that impact the development and use of software.	
9.4.12.DC.6	Select information to post online that positively impacts personal image and future college and career opportunities.	
9.4.12.DC.7	Evaluate the influence of digital communities on the nature, content and responsibilities of careers, and other aspects of society.	
9.4.12.DC.8	Explain how increased network connectivity and computing capabilities of everyday objects allow for innovative technological approaches to climate protection.	
9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities and utility for accomplishing a specific task.	
9.4.12.TL.2	Generate data using formula-based calculations in a spreadsheet and draw conclusions about the data.	
9.4.12.TL.3	Analyze the effectiveness of the process and quality of collaborative environments.	
9.4.12.TL.4	Collaborate in online learning communities or social networks or virtual worlds to analyze and propose a resolution to a real-world problem.	
9.4.12.GCA.1	Collaborate with individuals analyze a variety of potential solutions to climate change effects and determine why solutions may work better than others (e.g., political. economic, cultural).	
9.4.12.IML.1	Compare search browsers and recognize features that allow for filtering of information.	
9.4.12.IML.2	Evaluate digital sources for timeliness, accuracy, perspective, credibility of the source, and relevance of information, in media, data, or other resources.	
9.4.12.IML.3	Analyze data using tools and models to make valid and reliable claims, or to determine optimal design solutions.	
9.4.12.IML.4	Assess and critique the appropriateness and impact of existing data visualizations for an intended audience.	
9.4.12.IML.5	Evaluate, synthesize and apply information on climate change from various sources appropriately.	
9.4.12.IML.6	Use various types of media to produce and store information on climate change for different purposes and audiences with sensitivity to cultural, gender and age diversity.	
9.4.12.IML.7	Develop an argument to support a claim regarding a current workplace or societal/ethical issue such as climate change.	
9.4.12.IML.8	Evaluate media sources for point of view, bias and motivations.	
9.4.12.IML.9	Analyze the decisions creators make to reveal explicit and implicit messages within information and media.	