Cyberwise

Junior Cycle Short Course in Cyber Security

Specification for Junior Cycle Short Course

UCD DUBLIN
School of Education
School of Computer Science

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

NCSC

www.cyberwise.ie

This short course has been developed in accordance with the NCCA template and guidelines.

Table of Contents

Introduction to Junior Cycle

Junior cycle education places students at the centre of the educational experience, enabling them to actively participate in their communities and in society and to be resourceful and confident learners in all aspects and stages of their lives. Junior cycle is inclusive of all students and contributes to equality of opportunity, participation, and outcome for all.

The junior cycle allows students to make a greater connection with learning by focusing on the quality of learning that takes place and by offering experiences that are engaging and enjoyable for them, and relevant to their lives. These experiences are of a high quality, contribute directly to the physical, mental, and social wellbeing of learners, and where possible, provide opportunities for them to develop their abilities and talents in the areas of creativity, innovation, and enterprise. The learner's junior cycle programme builds on their learning to date and actively supports their progress in learning and in addition, supports them in developing the learning skills that will assist them in meeting the challenges of life beyond school.

Rationale

In today's digital age, cyber security is a critical issue that affects all aspects of modern society. As technology continues to advance and becomes increasingly integrated into our daily lives, it is essential that students understand the complex and interconnected nature of cyber threats and how they relate to personal, social, and global well-being. This multidisciplinary and interdisciplinary cyber security short course allows students to develop a holistic understanding of cyber security, which will better prepare them for this ever evolving, technological landscape.

This short course allows students to develop an understanding of the multiple dimensions of cyber security and to appreciate the importance of interdisciplinary collaboration. Students learn about the history and evolution of cyber security technology and its impact on society over time. They investigate the different types of cyber-attacks and the measures that are taken to defend against them. Additionally, students learn about the role of government, private industry, and civil society in addressing cyber security issues.

Students are encouraged to work independently and collaboratively to inquire about and critically engage with contemporary issues relating to online privacy and security, digital citizenship, and online ethics, helping them appreciate the importance of cyber resilience, digital literacy, digital citizenship, and the responsible use of technology. Distinct, but complementary, to the Coding and Digital Media Literacy short courses, this Cyber Security short course also gives students a foundation to pursue future studies or career in this field.

Aim

The aims of this Cyber Security short course are for students to develop:

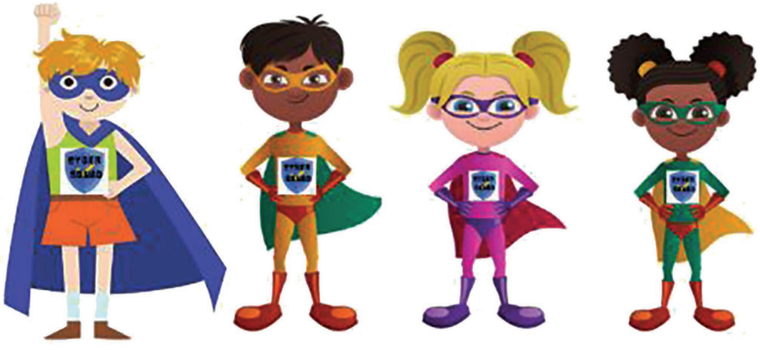
- a holistic understanding of cyber security by drawing on perspectives and skills from across the subject disciplines.
- cyber resilience by preparing students to navigate the digital world in a safe and responsible manner.
- a knowledge base for potential future studies or career opportunities in the field of cyber security.

Overview: Course

The Unifying Element in this Cyber Security Short Course supports the subsequent three strands. It gives conceptual context and space for deeper inquiry, critical engagement, and self-reflection and, combined with the other three strands, reflects the multi and interdisciplinary nature of the course.

Strand 1: *Exploring Cyberspace,* Strand 2: *Cyber Security Solutions,* and Strand 3: *Cyber Security in a Global Village,* have been designed to build upon each other. *Strand 1: Exploring Cyberspace* is a foundational unit giving a general orientation to the foundations and scope of cyber security and can be a useful place to begin. However, when designing Units of Learning, links should be made across the three strands and the Unifying Element.

The Classroom Based Assessment for the Cyber Security Short Course requires students to reflect over their learning process. Employing the regular use of digital portfolios, written journals, or blogs will significantly support conceptual continuity and understanding, metacognitive reflection, and assessment and will be a valuable resource for students when working on their CBA.



Overview of Unifying Element and associated Strands:

Unifying Element:

Students explore relevant philosophical implications of cyber security, psychological factors that drive human behaviour in relation to cyber security, and current and potential careers relating to different aspects of cyber security in order to develop a holistic understanding of cyber security and its multidimensional aspects.

Strand 1: Exploring Cyberspace

This strand enables students to explore and understand the different elements of cyberspace and in turn how this can be exploited for economic, social, political, and criminal ends.

Strand 2: Cyber Security Solutions

This strand allows students to examine the actions and habits individuals, governments, and businesses can take to pre-empt cyber-attacks and maintain good cyber hygiene. Students are encouraged to work independently and collaboratively to solve problems directly related to their own lives and communities.

Strand 3: Cyber Security in a Global Village

This strand allows students to explore legislation and government bodies such as the National Cyber Security Centre, the Citizens Advice Bureau, and the Garda Siochana that are tasked with responding to cyber-crimes and cyber-attacks.

The learning outcomes in this short course are aligned with the level indicators for Level 3 of the National Framework of Qualifications.

The course has been designed for approximately 100 hours of student engagement.

Learning Outcomes

Learning outcomes are statements that describe what knowledge, understanding, skills and values students should be able to demonstrate having completed this junior cycle short course. The learning outcomes set out in the following tables apply to all students and represent outcomes for students at the end of their period of study (approximately 100 hours). The outcomes are numbered within each strand. The numbering is intended to support teacher planning in the first instance and does not imply any hierarchy of importance across the outcomes themselves.

Unifying Element

Students learn about	**Learning outcomes** Students should be able to
Philosophical implications in Cyber Security Social, ethical, political, and economic considerations of cybersecurity Our roles, rights and responsibilities in cyberspace	U.1 Critically engage, evaluate, and reflect on the implications cyberspace has for **privacy, security** and **freedom** and their associated concepts. U.2 Collaboratively create, inquire, and reflect upon philosophical questions that arise when exploring cyberspace and cyber security. U.3 Recognise the interdisciplinary and complex nature of cyberspace and the personal, local, national, and global role it has in our lives.
Cyberpsychology (Internet or Web Psychology) and Social Engineering *Why people fall for online scams, how to design systems that encourage secure behaviour, and the impact of data breaches on trust and behaviour*	U.4 Investigate how the discipline of cyberpsychology explains human behaviour in relation to cyber security. U.5 Explore how computers and Internet technology impact the way people think and behave at both an individual and a group level. U.6 Examine how society has changed after a cyber security event.
Careers in Cyber Security	U.7 Investigate career opportunities in cyber security. U.8 Identify qualities, skills, and qualifications that are suitable for a career in cyber security. U.9 Evaluate if a career in cyber security is of interest to you. U.10 Examine the portrayal of people in cyber security in popular culture.

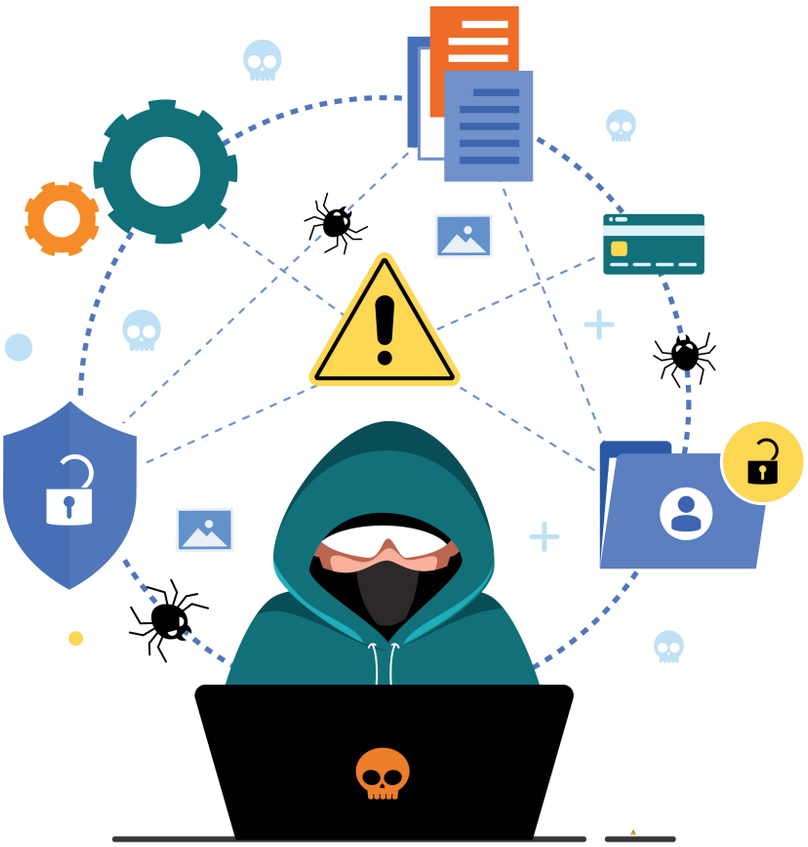
STRAND 1: **Exploring Cyberspace**

Students learn about	**Learning outcomes** Students should be able to
Making Sense of Cyberspace	1.1 Consider the variety of uses of cyberspace for different stakeholders e.g., individuals, communities, businesses, and governments etc. 1.2 Discuss the core functions of cyber security and appreciate its importance in society. 1.3 Understand the concept of cyber hygiene and the key steps for good cyber hygiene.
Data is the new oil	1.4 Consider what data is, and what makes data politically, economically, and personally valuable. 1.5 Investigate the ways data is legally collected. 1.6 Reflect on the concept of privacy and the value they place on their own privacy. 1.7 Access and amend privacy settings appropriately on a variety of relevant digital media platforms and software apps.
Cyber Events *Operational; Security; Incidents; Disaster; Compliance; Improvement* *Examples include but are not limited to hacking, phishing, malicious software, distributed denial of service (DDOS)*	1.8 Describe types of cyber events. 1.9 Explore examples of political, economic, social, and personal cybercrime. 1.10 Investigate how cyber security breaches occur for individuals, institutions, and businesses.

STRAND 2: **Cyber Security Solutions**

Students learn about	**Learning outcomes** Students should be able to
Who goes my way?	
Examples include but are not limited to Caesar cipher, Turing's Enigma machine	2.1 Explore the historical role of passwords and encryption to secure valuable information.
	2.2 Develop an understanding of the properties of codes and how they are different to ciphers.
	2.3 Identify the factors needed to make a successful encryption.
	2.4 Describe the features of strong passwords or passphrases and identify different strategies or tools for their safety and maintenance.
Enabling screen locks, changing default passwords, using passphrases, multi-function authentication (MFA) and password managers	2.5 Demonstrate how to improve personal online account security.
Buliding Security	2.6 Describe and evaluate different ways to back-up data.
	2.7 Outline the role of the Firewall in cyber security and know how to implement and maintain a firewall.
	2.8 Explain how to improve their home router security against malicious cyber activity by taking some simple steps.
	2.9 Evaluate the benefits and risks of using public WIFI systems and consider cyber security methods that could be used to protect their data, such as a VPN.

Students learn about	**Learning outcomes** Students should be able to
Spotting Cyber Attacks	2.10 Investigate the impact of different types of malware used to attack individuals, businesses, organisations, and governments.
	2.11 Discern between fake profiles and messages and authentic online communications.
	2.12 Know how to authenticate data before sharing and how to block and report unwanted communication.
	2.13 Explore current methods used by cybercriminals to access sensitive data such as PINS and passwords.



STRAND 3: **Cyber security in a Global Village**

Students learn about	**Learning outcomes** Students should be able to
Communication and Crisis Management	3.1 Describe some of the high-profile cyber security crises in modern times in Ireland and the role of government in the response.
	3.2 Evaluate the risks to cyber security during a crisis.
	3.3 Explain how individuals can plan for and respond to a cyber security attack.
	3.4 Outline how an organisation can plan for and respond to a cyber-attack at local level, corporate level, through policies, response plans, communication plans and simulation exercises.
	3.5 List examples of how the Irish Government communicates cyber security threats during a crisis.
Regulation and Legislation *General Data Protection Regulation (GDPR)*	3.6 Understand the principles of cyber security legislation.
	3.7 Compare voluntary versus mandatory regulation, and ethical versus government regulation.
	3.8 Describe the positive and negative implications of regulation around cyber security.
	3.9 Review examples of national, European, and international cyber security legislation.
Reporting breaches of Cyber Security	3.10 Recognise when something is a threat and should be reported.
	3.11 Identify who or what organisation you should contact and how to contact them.
Illegal content, financial transaction, fraud, leak of personal information, and extortion.	3.12 Know how to report online crime or threats in a range of contexts.

Links

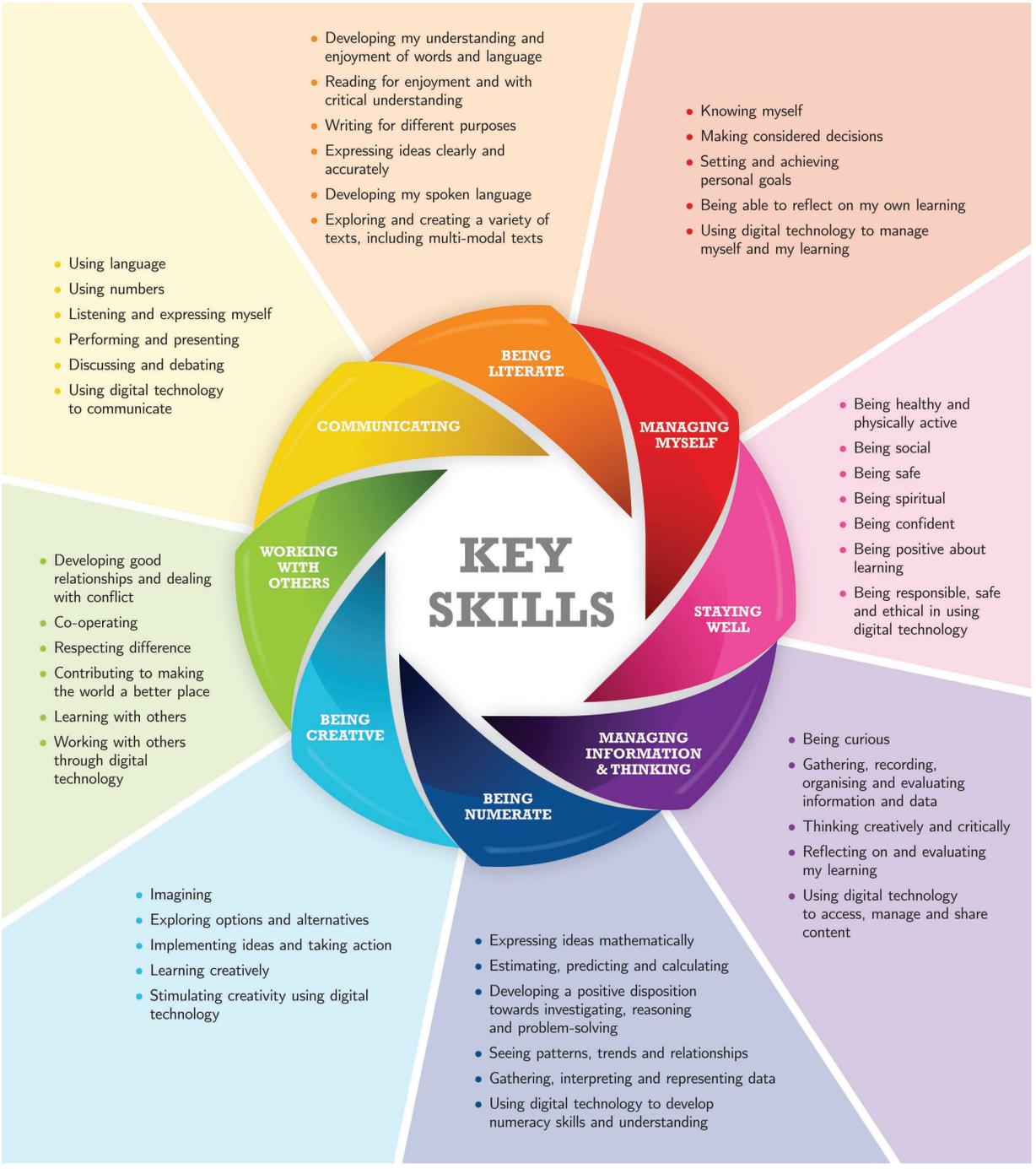
a) Statements of learning

These statements describe what students should know, understand, value and be able to do at the end of their time in junior cycle. It is possible for a short course to contribute to the learning described in a number of statements. *For the purpose of providing a clear description of the short course, developers should identify the statements of learning (three/four maximum) to which the course relates most immediately and significantly.*

Statement	Examples of relevant learning in the course
SOL 5: The student has an awareness of personal values and an understanding of the process of moral decision making.	Students learn about laws, regulations, and codes of conduct relating to cyber security and how they align with personal and societal values. They will also investigate and discuss real-world examples of ethical dilemmas and challenges in the field of cyber security.
SOL 15: The student recognizes the potential uses of mathematical knowledge, skills and understanding in all areas of learning.	Students explore the historical role of passwords and encryption to secure valuable information. They also investigate the role of codes in cyber security, such as cryptography, data transmission and data storage. They analyse data and reflect on the ways personal data has economic value.
SOL 19: The student values the roles and contribution of science and technology to society, and their personal, social, and global importance.	Students analyse the interplay between technology and society, including how technology shapes social norms and behaviours, and how society shapes the development and use of technology. They investigate and discuss the current and emerging cyber security technologies and their potential implications for personal, social, and global security.
SOL 24: The student uses technology and digital media tools to learn, communicate, work and think collaboratively and creatively in a responsible and ethical manner.	Across each of the strands students engage in a variety of creative and collaborative projects using technology and digital media to gather and evaluate data. They critically reflect before applying their knowledge about cyber security to their own lives.

b) The eight key skills of junior cycle

In addition to their specific content and knowledge, the subjects and short courses of junior cycle provide students with opportunities to develop a range of key skills. The junior cycle curriculum focuses on eight key skills: Being literate; Managing myself; Staying well; Managing information and thinking; Being numerate; Being creative; Working with others and Communicating.



Key Skill	Key Skill Element	Student learning activity
Being literate	Writing for different purposes	Students engage in a wide range of independent and collaborative learning activities that support the development of their written skills. For example, creating user guides for non-technical audiences helps students understand the importance of clear, concise, and user-friendly communication in the field of cyber security.
Managing myself	Making considered decisions	Students identify potential cyber security risks and evaluate the likelihood and impact of each risk. They develop a risk management plan that prioritises the risks and outlines the actions to be taken to mitigate them. This develops students' analytical, decision-making, and problem-solving skills.
Staying well	Being responsible, safe and ethical in using digital technology	Using scenarios from any given strand or unifying element, students examine the impact of specific online behaviours and legislation on themselves, their own community, businesses, and politics at national and international levels. This develops students' understanding of digital citizenship and their ability to be responsible, safe, and ethical in using digital technology.
Managing information and thinking	Reflecting on and evaluating my learning	Students create a portfolio of their work throughout the course and reflect on the progress they made, what they learned, and how they applied this learning in real-world scenarios. This develops students' metacognitive skills and their ability to evaluate their own learning in a comprehensive way.
Being numerate	Using digital technology to develop numeracy skills and understanding	Students investigate the importance of encryption and decryption in cyber security, and the mathematical principles that underpin them. They will work with real world data to assess the impact of real-world cyber security incidents. This develops students' understanding of data analysis and statistics, as well as their ability to use digital technology to analyse and interpret data.

Key Skill	Key Skill Element	Student learning activity
Being creative	Exploring options and alternatives	Students explore a case study of a real-world cyber security incident and analyse the different options and alternatives that were available to the organisation at the time of the incident. They evaluate the effectiveness of the actions taken and suggest alternative actions that could have been taken to mitigate the threat. This develops students' critical thinking and problem-solving skills by exploring options and alternatives in a real-world context.
Working with others	Developing good relationships and dealing with conflict	Students will engage in discussions, debate, and collaboratively inquire around cyber security issues. These include critically engaging with philosophical questions relating to privacy, security, and freedom that develops students' collaborative, critical thinking, communication and conflict resolution skills.
Communicating	Performing and presenting	Students work independently and collaboratively on cyber security project presentations, using topics selected from the strands and unifying elements. These may be digital or in-class presentations or performances. Students will take different roles and perspectives as they engage with a range of issues that arise from a particular scenario, such as a data breach or cyber-attack. This develops students' understanding of, and confidence with the skills that contribute to engaging and informative performances and presentations.

Assessment and Reporting

Essentially, the purpose of assessment and reporting at this stage of education is to support learning. Some learning outcomes lend themselves to once-off assessment, others to assessment on an ongoing basis as students engage in different learning activities. Examples of learning activities that support opportunities for formative assessment in this Cyber Security short course include:

Digital Portfolio / Written Journal /Blog

Students should aim to produce a portfolio of work that allows them to demonstrate their practical and theoretical learning throughout the cyber security short course. It should show how the student practically applied their learning to their own or others cyber hygiene habits, and how learning about wider issues in cyber security helped to inform their understanding of cyberspace and the personal, local, national and global role it has in our lives. It should also capture the students' reflective learning, documenting their experience of learning how to learn as they progress through the cyber security short course. Students can draw upon this work when completing their Classroom-Based Assessment.

Individual and Group Project Work

The multidisciplinary and interdisciplinary nature of this cyber security curriculum affords opportunities for students to engage with individual and group project work from a variety of subject perspectives.

- Conducting a security audit of their own digital devices and networks: Students learn about the potential security threats to their devices and how to identify and mitigate these risks. They could then conduct a security audit of their own devices and networks and create a plan to improve their security.
- Developing a cyber-security awareness campaign: Students could work in groups to develop a cyber-security awareness campaign aimed at their peers, parents, or community. This could include creating posters, flyers, videos, and presentations to educate others about the importance of cyber-security and how to stay safe online.
- Investigating cybercrime: Students could research a real-world cybercrime, such as a data breach, phishing scam, or ransomware attack. They could then present their findings to the class, including how the crime was committed, who was affected, and what could have been done to prevent it.
- Designing a secure password policy: Students could work in groups to research and analyse different password policies and best practices. They could then design a secure password policy for a fictional company, including guidelines for creating strong passwords, regularly changing passwords, and using two-factor authentication.

Case Studies

Supporting strong student engagement with contemporaneous real world events, the Learning Outcomes of this cyber security short course are well facilitated using case studies.

- The Impact of Cyber Attacks on Small Businesses: Students can research and analyse real-life cyber-attacks on small businesses and their effects on the business operations, finances, and reputation.

- Cybercrime and the Law: Students can investigate and analyse different types of cybercrime, the laws and regulations that are in place to prevent them, and the effectiveness of these laws in protecting citizens.
- Social Engineering and Cyber security Awareness: Students can create an awareness campaign about the dangers of social engineering and the importance of being vigilant when online. They can create posters, flyers, and videos to spread the message.
- Secure Online Banking and Shopping: Students can research and analyse the security measures in place for online banking and shopping, and the importance of being vigilant when using these services.
- The Future of Cyber security: Students can research and analyse the latest advancements and developments in cyber security technology and discuss the potential impact on society in the future.

Classroom-Based Assessment

Classroom-Based Assessments are the occasions when the teacher assesses the students in the specific assessment(s) that are set out in the subject or short course specification. When there is more than one teacher of this short course, the teachers gather examples of student work and compare their judgments with other colleagues. Junior cycle short courses will have one Classroom-Based Assessment and the student's achievement in the Classroom-Based Assessment will be recorded on the student's Junior Cycle Profile of Achievement (JCPA).

Cyber Security Classroom-Based Assessment

This Classroom-Based Assessment is designed to foster student agency and build upon the work they have accomplished in their portfolio, group projects, or case studies in relation to the three strands and unifying elements.

- Students are required to create a digital presentation summarising their learning journey on a course-related topic.
- The presentation should highlight key challenges and successes as learners and demonstrate practical application of learning to support personal or others' cyber hygiene habits.
- Students should reference relevant case studies, policies, and research to demonstrate how learning about broader cyber security issues informs their understanding of cyberspace and its role at personal, local, national, and global levels.
- Students should demonstrate how the exploration of philosophical implications, psychological factors, and/or career considerations within the unifying element have contributed to their knowledge and insights related to their chosen topic.
- Student choice is encouraged, and presentations can be digital or in-person, wherever possible.

It is essential students explicitly reference the connections to their previous work, emphasising how the CBA complements and expands upon their ongoing learning process. Consequently, the CBA is an integral part of their continuous learning journey, rather than a standalone event.

To support this approach, students should be encouraged to reflect on their previous work and explicitly integrate it into their digital portfolio, written journal, or blog. These reflections should serve as a foundation for their CBA, allowing them to demonstrate the progression and application of their knowledge and skills in cyber security.
Student choice should still be encouraged, providing flexibility for digital or in-person presentations.

Features of Quality

Level 3: The 4 descriptors are Exceptional, Above expectations, In line with expectations and Yet to meet expectations.

Cyber Security Classroom-Based Assessment Rubric

INVESTIGATING			
Exceptional	**Above Expectations**	**In Line with Expectations**	**Yet to Meet Expectations**
Demonstrates a comprehensive and sophisticated investigation of the chosen area of cyber security. Utilises a wide range of credible sources, including scholarly articles, case studies, and expert opinions. Analyses complex issues and demonstrates critical thinking skills in evaluating evidence. Makes insightful connections between the chosen area of cyber security and the unifying element.	Conducts a thorough investigation of the chosen area of cyber security. Incorporates a variety of reliable sources to support arguments and claims. Shows good analytical skills in evaluating evidence and presenting arguments. Establishes connections between the chosen area of cyber security and the unifying element.	Conducts a satisfactory investigation of the chosen area of cyber security. Uses credible sources to support arguments and claims. Demonstrates basic analytical skills in evaluating evidence. Establishes some connections between the chosen area of cyber security and the unifying element.	Conducts a limited or incomplete investigation of the chosen area of cyber security. Relies on few or unreliable sources to support arguments and claims. Demonstrates minimal analytical skills in evaluating evidence. Fails to establish meaningful connections between the chosen area of cyber security and the unifying element.

COMMUNICATING			
Exceptional	**Above Expectations**	**In Line with Expectations**	**Yet to Meet Expectations**
Presents ideas and information in a highly engaging and compelling manner. Demonstrates exceptional clarity, coherence, and organisation of thoughts. Utilises a variety of multimedia tools effectively to enhance understanding and engagement. Communicates complex concepts with precision and in a way that is accessible to the audience. Displays outstanding verbal and non-verbal communication skills.	Presents ideas and information in a clear and well-structured manner. Demonstrates good clarity, coherence, and organisation of thoughts. Uses multimedia tools effectively to support understanding and engagement. Communicates concepts effectively to the audience. Displays strong verbal and non-verbal communication skills.	Presents ideas and information in a satisfactory manner. Demonstrates reasonable clarity, coherence, and organisation of thoughts. Uses multimedia tools adequately to support understanding and engagement. Communicates concepts adequately to the audience. Displays satisfactory verbal and non-verbal communication skills.	Presents ideas and information in a confusing or disorganised manner. Lacks clarity and coherence in expressing thoughts. Fails to effectively use multimedia tools to support understanding and engagement. Communicates concepts poorly to the audience. Displays weak verbal and non-verbal communication skills.

KNOWLEDGE AND UNDERSTANDING			
Exceptional	**Above Expectations**	**In Line with Expectations**	**Yet to Meet Expectations**
Demonstrates an exceptional level of knowledge and understanding of the chosen area of cyber security.	Demonstrates a strong level of knowledge and understanding of the chosen area of cyber security.	Demonstrates a satisfactory level of knowledge and understanding of the chosen area of cyber security.	Demonstrates a limited level of knowledge and understanding of the chosen area of cyber security.

Assessment Arrangements

Assessment practices, whether as part of ongoing assessment or the Classroom-Based Assessment, are a key feature of teaching and learning in schools. Assessment arrangements for students, e.g. the support provided by a special needs assistant or the support of assistive technologies, should be in line with the arrangements the school has put in place to support the student's learning throughout the year.

Where a school judges that a student has a specific physical or learning difficulty, appropriate assessment arrangements may be put in place to remove, as far as possible, the impact of the disability on the student's performance in the Classroom-Based Assessment. Such accommodations which enable all students to access curriculum and assessment are based on specific needs.

Comprehensive guidelines for schools and an interactive version of the Inclusive Education Framework provide further information on supportive assessment practices.

Appendix:
Level indicators for Level 3 of the National Framework of Qualifications (QQI)

This short course has been developed in alignment with the level indicators for Level 3 of the National Framework of Qualifications. Usually, for Level 3 certification and awards, the knowledge, skill and competence acquired are relevant to personal development, participation in society and community, employment, and access to additional education and training.

This short course has been developed in accordance with the NCCA template and guidelines.

NFQ Level	3
Knowledge Breadth	Knowledge broadly moderate in range
Knowledge Kind	Mainly concrete in reference and with some comprehension of relationship between knowledge elements
Know-how and skill Range	Demonstrate a limited range of practical and cognitive skills and tools
Know-how and skill Selectivity	Select from a limited range of varied procedures and apply known solutions to a limited range of predictable problems
Competence Context	Act within a limited range of contexts
Competence Role	Act under direction with limited autonomy; function within familiar, homogeneous groups
Competence Learning to learn	Learn to learn within a managed environment
Competence Insight	Assume limited responsibility for consistency of self-understanding and behaviour

Cyberwise

www.cyberwise.ie

School of Education
School of Computer Science

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications