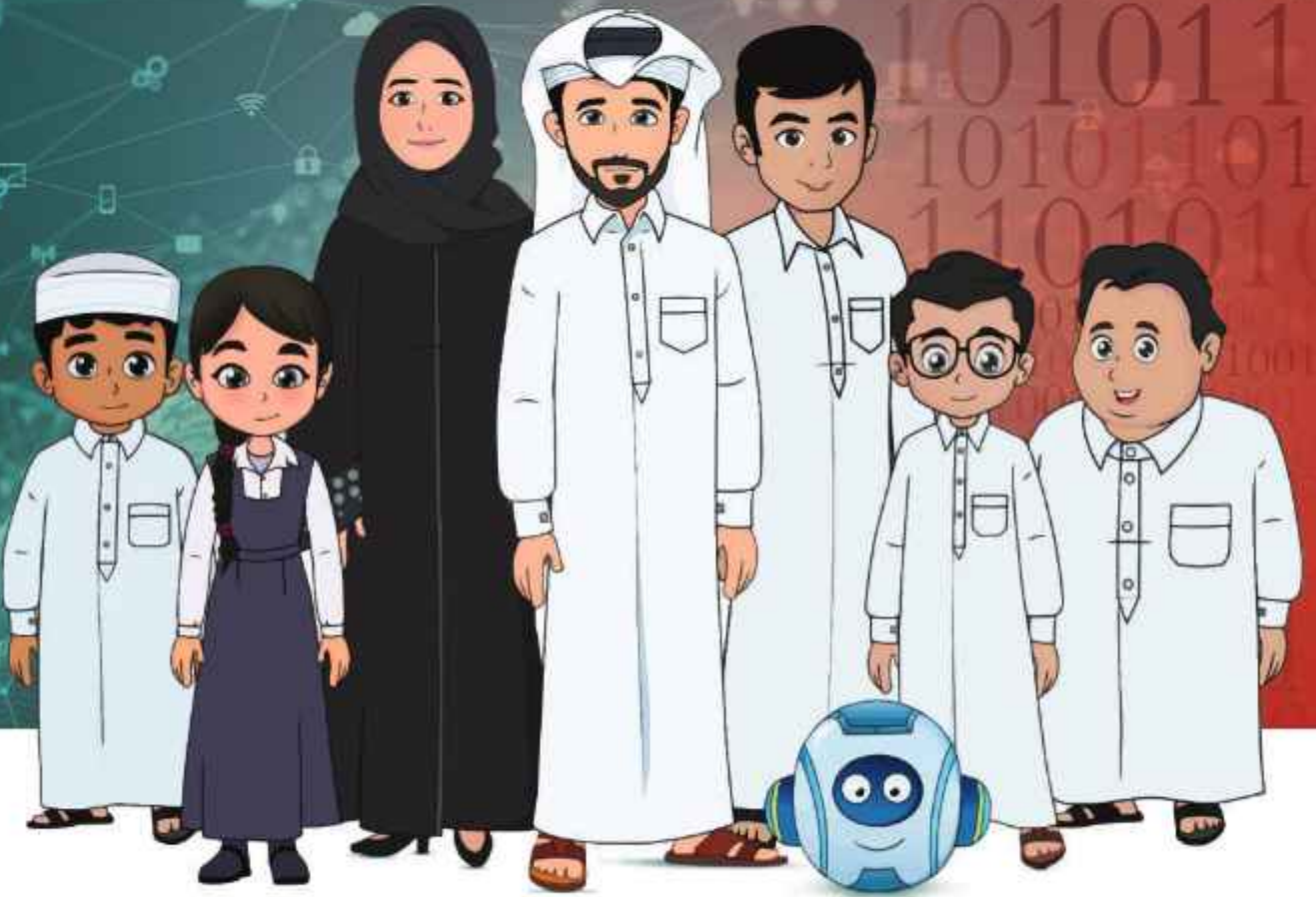




# مناهج الأمن السيبراني التعليمية

## Cyber Security Curricula Education



**Parents Guidebook**





مناهج الأمن السيبراني التعليمية  
Cyber Security Curricula Education

Cyber Security experts at the National Agency for Cyber Security, represented by the Department of National Cyber Excellence, Empowerment Affairs and National Cyber Excellence Sector, in partnership with a group of specialists in the Ministry of Education and Higher Education from the divisions concerned with this aspect, which is represented by the Department of E-Learning and Digital Solutions, the Department of Educational Guidance Department of Information Technology, Department of Curricula and Learning Resources, Department of School Affairs, Department of Programs and Activities, Department of Special Education and Inclusive Education.

#### To contact



وكالة الوطنية للأمن الإلكتروني  
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ [cyberexcellence@ncsa.gov.qa](mailto:cyberexcellence@ncsa.gov.qa)

☎ 00974 404 663 79

☎ 00974 404 663 63

January 2023

Doha, Qatar

### Intellectual Property rights

The National Agency for Cyber Security in the State of Qatar owns the work, and copyright, publishing, printing rights, and all other intellectual property rights are protected by the National Agency for Cyber Security in the State of Qatar.

Additionally, the National Agency for Cyber Security in the State of Qatar owns all rights and exclusive production rights to the educational Cyber Security curricula, including the logo, characters and graphics, videos and infographics, accompanying music, teacher's guide, and parent's guide. As a result, the Agency retains all rights to these materials, and it is prohibited to republish, quote, copy, or transfer them in whole or in part in any form or by any means, whether electronic or mechanical, related to educational Cyber Security curricula and their appendices. As well as utilizing any information storage and retrieval system, current or future, including photographing, recording, or using any of them, unless the agency has given written permission. Anyone who breaks this could face legal consequences.



## Index

<b>First topic: An introductory Overview of Educational Cyber Security Curricula</b>	9
• The electronic platform of the National Agency for Cyber Security	15
• Project overview	16
• Qatar Education System	17
• Elementary school	18
• Middle School	19
• High school	19
• Adult Education	20
• Content for physically and mentally challenged individuals	20
• Educational and Teaching Staff	20
• Students' parents	21
• Project Team	22
• The contribution of the curriculum to the achievement of Qatar's Vision 2030	23
• The anticipated outcomes for students of the Cyber Security educational curricula:	26



<b>Second topic: Guide Policy</b>	27
• The idea of the guide	29
• Guide goals	29
• Justification for drafting the guide	30
• Starting points of the guide	32
<b>Third topic: Characters and topics of Cyber Security educational curricula</b>	31
• First: Characters of the Cyber Security educational curricula	33
• Second: Topics of the educational Cyber Security curricula	45
A- Visual content topics for the Elementary school	45
B- Visual content topics for the middle school	46
C- Visual content topics for high school	47

<b>Fourth topic: Duties of Parents According to the Guideline</b>	49
-How parents interact with the visual content of Cyber Security educational curricula	54
-Parents' notes during the presentation of the visual content	56
<b>Fifth topic: A brief summary of the educational visual contents</b>	61
First: Elementary school	65
• First grade / safe use of the Internet.	67
Second: Middle school	71
• Seventh grade / Malware.	73
Third: High School	77
• Tenth grade/ Evaluate information sources on the Internet.	79
<b>Conclusion</b>	83





First topic

## **An introductory Overview of Educational Cybersecurity Curricula**



Based on the endeavors of the National Agency for Cyber Security in the State of Qatar to build a digitally secure and technologically empowered local community, and in light of the successive and rapid technological developments, and the entry of technology into various aspects of life, including different age groups, the technological security risks facing individuals in general and children and adolescents, in particular, are increasing. Therefore, based on the general objectives of the National Agency for Cyber Security, facing these challenges is by addressing children and adolescents, within the framework of the school environment, with curricula that enhance awareness of digital safety and the concepts and foundations of Cyber Security.

Based on this proposal, the goal of the **“Educational Cyber Security Curricula”** project is to educate children and adolescents in the State of Qatar about the various concepts and foundations related to digital safety and Cyber Security. It is based on the importance of protecting personal data and information and a desire to educate society about Cyber Security. This project is sponsored by the National Agency for Cyber Security in the State of Qatar, it is the first project of its kind in the region, a project that aims to raise digital awareness among all age groups, starting from the first grade of elementary school to the twelfth grade of high school.

The **“Educational Cyber Security Curricula”** project, **in cooperation with the Ministry of Education and Higher Education**, aims to achieve a number of objectives, the most important of which is: educating society in general, children and adolescents in particular about the concept of Digital Citizenship which entails the responsible, moral, and safe use of information and communication technology by individuals as part of the local community and the global community. In addition to educating society in general, and children and adolescents in particular, about the risks of the Internet, whilst training them on the basics of protecting personal data and maintaining the safety of electronic devices. In addition to raising their awareness of general concepts related to Cyber Security and digital safety, and equip the young generation of Qatari youth with the ability to efficiently and safely deal with technological tools.



To accomplish the goals of the project, It employs a variety of educational tools, all of which fall under the umbrella of raising awareness of the significance of Cyber Security in a manner that contributes to achieving the project and the National Agency for Cyber Security's goals of protecting society from Internet risks and data security and privacy. In addition to a guide for teachers and parents, the training tools include training and educational visual products, educational visual content, posters, and infographic designs

The millions of people who use the World Wide Web, including people of all ages and for a variety of purposes, have unprecedented opportunities for human communication and the exchange of information, ideas, and opinions thanks to the current digital revolution. Naturally, the rise in perilous opportunities for all human endeavors reflected this unprecedented advancement. Where a new threat to users emerged, with some of them able to hack into information networks and alter any kind of data. Cybercrime is the practice of causing harm to users in a variety of ways through personal, official, and financial harm.

Many developed nations tended to implement targeted initiatives to provide technological security for all Internet users, mainly to young school and university students, who use the Internet the most, in consideration of the seriousness of this matter and the material, economic, social, and mainly humanitarian losses caused by these crimes.

Among these efforts are The European framework for the safe use of mobile devices and the initiative by the European Union to establish guidelines for the secure use of information networks In 24 European nations, Cyber Security concepts were incorporated into school curricula in 2009.



The National Alliance for Cyber Security was established and the Department of Homeland Security assumed responsibility for raising Cyber Security awareness in the United States. The Department of Homeland Security, the National Institute of Standards and Technology, and institutions working in the field of cyber security collaborated with the US government to launch the National Initiative for Cyber Education on the educational level.

We do not deny that similar measures to ensure cyber security exist in Arab nations; however, the majority of these nations faced issues posed by the absence of a comprehensive cyber security initiative that encompasses all groups, including schoolchildren, university students, parallel education, literacy programs, teachers, and parents. There is also inadequate support and educational initiatives that are incapable of keeping up with communications and information technology developments. This was reflected in the decline of Cyber Security levels among these groups and the higher rate of cyberattacks and crimes committed against Internet users in those countries than in other countries.

Among the most significant and successful experiences in this field, the Ministry of Education and Higher Education in the State of Qatar's experience creating digital educational content that is "interactive"; Its goal is to make students, teachers, and parents more aware of digital technology. And educating them about the most recent developments and challenges in Cyber Security both locally and globally and making content permanently accessible through the Qatar Education System.

The State of Qatar is one of the first Arab and regional countries to realize the importance of Cyber Security and has included it in its strategic plans to protect its citizens and institutions from cyberattacks and information piracy. The strategy of the National Agency for Cyber Security constituted a radical shift in the process of assisting the state to enhance Cyber Security, protect its vital interests, national security, and sensitive infrastructure, spread societal awareness of digital culture, and pay attention to raising a conscious generation of children and youths.

This strategic leap must include all government sectors, whether it is public or private, to achieve the highest level of data security, sustain the necessary developmental abilities of the Infrastructure of information technologies, and build a defense line that consists of highly distinct and ambitious national scientific competencies. As well as the rehabilitation of younger elements in Cyber Security, find and establish partnerships with public and private research, and academic and industrial bodies, and encourage innovation and both local and foreign investments in Cyber Security to reach an unprecedented technological advancement that serves the community as a whole.





## The electronic platform of the National Agency for Cyber Security

As part of its grand strategy for Cyber Security in the State of Qatar, the National Agency for Cyber Security has launched an electronic platform that includes interactive content (videos, short animations, infographic designs, and banner posters) to raise awareness of the concepts of digital safety, the seriousness of cyber threats, and how to deal with them. This platform will be available for use this year inside and outside the State of Qatar in order to achieve the greatest benefit and awareness among adults and children.

Not only that, but within the framework of the national strategy for Cyber Security, the National Agency for Cyber Security, in partnership with the Ministry of Education and Higher Education in the country, is adopting a project for educational Cyber Security curricula within the subject of computing and information technology. The project aims to educate school students, parents, and teachers on the concepts of Cyber Security and safety about the most prominent challenges that they may face during their daily dealings with technology. A copy of the agency's interactive content - which is published on its digital platform - will be uploaded to the Qatar Education System Within the framework of this project, to be viewed by students, teachers, and parents who are targeted by the curriculum project.



## Project overview

To achieve the project's intended impact and the stated objectives effectively and efficiently; The **"Cyber Security Educational Curricula"** project has a unique mix of educational curricula for each age group, so the educational content varies by age. As the desired effectiveness necessitates addressing each age stage with educational content that increases in level with age. Based on this principle, the curricula were divided into three main sections, according to the educational stages approved in the State of Qatar, which are the elementary, middle, and high school stages, and even at the level of one stage each class was addressed with different educational content.

This content incorporates the creation of interactive digital instructional educational curricula, instructive visual content, and an electronic procedural and informative aide for overseeing and utilizing the content. In addition to an infographic that provides a summary of the information, there is a guide for teachers and parents that covers all computing and information technology curricula at all school levels, as well as a table of evaluation questions for students.

The following is an overview of the curricula according to the educational stages approved in the State of Qatar:



## Qatar Education System

After the content was produced in its final form, revised, and reviewed, it was officially approved and uploaded to the Qatar Education System to be permanently available to the target audience.

- A brand-new system in use since the academic year 2021-2022.
- It depends on numerous advanced systems and artificial intelligence.
- It helps to analyze the academic level of each student, his behavior, and his class activity.
- Teachers' performance can be evaluated with the help of the system.
- The system makes it simple for parents and the school to communicate.

تسجيل الدخول









لمعرفة كيفية استخدام نظام قطر للتعليم، سواء كنت معلم، طالب، ولي أمر، يمكنك الضغط على الزر أدناه.

معرفة قطر للتعليم



عزيزي ولي الأمر / الطالب، في حال رغبت في معرفة الحساب الرئيسي، استعادة أو تغيير كلمة المرور، يمكنك الضغط على الرابط أدناه وإتباع الخطوات.

الدخول على الحساب الرئيسي / تغيير كلمة المرور



جدول الفرمات - حساب الطالب



امتحان الذهن - حساب الطالب



التعرف بالواحدة - حساب الطالب



تسجيل الدخول - حساب الطالب



## Elementary school:

The educational curriculum at this stage considers the demographic and psychological characteristics of children, such as being very young age and their lack of experience. In line with children's cognitive abilities for this stage, the design is made in a way that aligns with childhood standards, and it focuses on engaging videos and visual content that captivate their interest. The curricula address basic Cyber Security topics such as ways to protect electronic devices, refraining from sharing personal information with strangers, and creating strong passwords. These topics become more expanded and comprehensive as the children's ages progress.

In order to enhance the attractiveness of the materials offered, and their ability to effectively influence children, the curricula introduce lovely cartoon characters inspired by the Qatari environment, such as a cute robot character, to provide information to children through educational films, posters, and infographic designs, in a way that makes children take these characters as their friends, from whom they derive valuable information and knowledge that they are looking for in the field of Cyber Security.





## Middle School:

In the curricula for middle school students, educational content was developed in line with the expansion of the child's perceptions, knowledge, and ability of absorption, analysis, and comprehension. The educational content at this stage is complementary to the content in the elementary stage and is based on information related to computing and information technology, how to deal with social networking sites, websites, and other relevant information.

In this stage of the curriculum, new, age-appropriate characters were introduced and created to give the films an air of fun and increase suspense and attraction in them.

## High school:

In this stage, topics related to cloud computing, how to deal with it, the basics of file protection, information about electronic attacks, phishing, threats and how to Deal with it, and other relevant information are introduced in an age-appropriate way that considers the children's and adolescents' maturity and capability in analyze and deduction.





## Adult Education:

In the interest of the National Agency for Cyber Security to achieve the deepest impact on the community targeted by the project, educational content was directed to adults so that the project covers the entire target community. Here, the curricula designed for all the same stages were relied upon, so that the same approved content is used in these stages of adult education.

## Content for physically and mentally challenged individuals

Content has been allocated for physically and mentally challenged individuals, proportionate to their cognitive abilities, to qualify them and enable them to safely use the Internet and modern electronic devices, taking into account the variety of special needs of people of determination. This is similar to the content that is intended for students of various age groups.

To ensure the promotion of the concepts of digital citizenship and the consolidation of Cyber Security, Cyber Security educational curricula are directed to all groups and segments of society without exception. They aim to provide a comprehensive understanding of the local community.

## Educational and Teaching Staff:

In light of the fact that achieving the objectives of the program necessitates the assistance of the educational staff, we have provided you, our revered teachers, with this guide, which contains tools to support your perseverance and sincere efforts as well as to enrich your work. As a result, this guide was produced, which contains directive training materials for educational staff in Qatar's public and private schools. Throughout the various educational stages, it is believed that the educational staff has a direct and intimate relationship with children and adolescents. Training and qualifying them helps in creating a teaching environment that can efficiently and effectively deliver educational content to students. As a result, a guide for the various educational stages for the teaching staff was developed on the basis of this proposition.





## Students' parents:

Qualifying and training parents on how to deal with modern technological tools and raising their level of awareness of the concepts of Cyber Security and digital safety constitute direct support for the project's efforts in building a digitally secure society. The presence of qualified parents regarding the safe use of technology will reflect positively on their children's environment as a whole, and therefore on Qatari society in all its segments.

The educational content is approved within the framework of the "Cyber Security Educational Curricula" project, and it is considered an integrated curriculum during the three stages are elementary, middle, and high school, which applies to adult education, as it is a single curriculum and integrated content. Each stage is considered a knowledge entry and a main tool for the next stage, and this integration is in meeting the goals of the project and achieving the desired impact at the community level.



## Project Team:

The success of the project is linked to the availability of a qualified and experienced work team in preparing educational content, and expertise in concepts related to digital safety and Cyber Security as well as the basics of e-learning.

Therefore, the project relies on a group of consultants and experts in the field of Cyber Security at the national agency for Cyber Security.

The National Cyber Excellence Department's team of experts worked with a group of educational experts from the Ministry of Education and Higher Education's departments specializing in this area to prepare the curricula, which include:

- E-learning and digital solutions management.
- Educational guidance management, IT department.
- Management of learning resources and curricula.
- School Affairs Management, Program and Activities Section.
- Management of special education and talent care.

The philosophy of the project team is based on precise specialization, as each task within the framework of the project is assigned to a team of experts so that the foundations of the task intersect with the field of expertise of the work team, as one team specializes in preparing electronic educational content based on the concepts of Cyber Security and digital safety, another team will specialize in how to deliver educational content to the target audience, while another is specialized with design. Through the integration of the expertise and competencies of the work team, the main objective of the project will be achieved, which is to design educational and teaching curricula capable of enhancing awareness of digital safety and Cyber Security amongst the targeted community segments.



## The contribution of the curriculum to the achievement of Qatar's Vision 2030

The Qatar National Vision 2030 is regarded as a road map to transform Qatar into an advanced society capable of sustainable development, with the goal of ensuring that all citizens have access to a high standard of living by 2030.

### **The aim of the vision is to:**

- Identify the long-term outcomes and provide a framework for the development and implementation of national strategies.
- Directing government plans, policies, and strategies, as well as allocating funds and revenues for a common objective.
- Providing a goal and joint direction to private sector businesses and, to some extent, individuals.

### **Qatar's national vision deals with five major challenges, which are:**

- Balance between modernity and preserving traditions.
- Fulfilling current needs without jeopardizing future ones.
- Managing growth.
- Keeping the balance between Qataris and foreigners.
- Adequate environmental supervision.





The Qatar National Vision 2030 aims to build a bridge that connects the past and the present. It portrays a vital society that prioritizes economic and social justice, keeps the environment and people in balance, upholds supreme Islamic values, and has strong family ties as its foundation.

In accordance with this pioneering concept; The “Cyber Security Educational Curricula” project proves to be a useful and effective means of providing educators who are in charge of the next generation with information and an understanding of the significance of Cyber Security. This generation can receive the knowledge that will safeguard them and guarantee an understanding of the technological challenges and how to make the most of technology without putting themselves in danger.

Cyber Security is one of the most important requirements for the future and the digital transformation that the State of Qatar is witnessing, within the framework of its national vision and aspirations for the future, by making Cyber Security an essential element in its national project, given the importance, it entails in the field of information technology and digital transformation, which is linked to every aspect of life. Communication and information technology also studies the computer, biological, cognitive, and social aspects, including the study of the social impact of information technology.

Educational Cyber Security curricula are related to communication and information technology, and related studies and processing of information, exploring weaknesses in data protection and finding technological solutions for them, in addition to the social and educational component for students in their dealings with electronic devices and various websites.



### The most important concepts are as follows:

- Information lifecycle: utilizing and discovering information with self-assurance, independence, and safety.
- Information tools: using digital tools creatively, and choosing technology for a specific purpose safely.
- Information Technologies: Purposeful and creative use of a wide range of digital technologies and mastery of work.
- Technological challenges: exploring the risks of the Internet, the challenges of Cyber Security, and learning how to deal with them in a safe and correct way.
- Achieving harmony between the social and educational aspects, as well as the cognitive and educational aspects, so that students are instructed to preserve the nation's identity and social values, respect the privacy of others and consider social factors when interacting with social networks.



## The anticipated outcomes for students of the Cyber Security educational curricula:

- Choosing and using digital tools for their appropriate ends in everyday situations.
- Use digital tools creatively, respond to communication, produce, process, analyze, share, and display information depending on their level of knowledge.
- Install basic computer programs and applications appropriate to their age.
- Use digital tools in a safe and ethical manner.
- Understanding and realizing the challenges of Cyber Security, and the risks of dealing with the Internet.
- Know how to deal with the problems and risks they might encounter when using the Internet and the various browsing sites.
- Enhancing their technological knowledge and social media management abilities without jeopardizing their social life or family values.





## Second topic

# Guide Policy



## The idea of the guide:

"Parent's Guide" is a set of procedural steps, tips, and instructions provided to parents of students in the educational stages targeted by the project in order to understand the nature of the strategy and the roles assigned to them as a cornerstone in the success of implementation, and to ensure the highest level of performance and results with their students.

We present you this guide with the aim of supporting your efforts in achieving the desired impact of the program by supporting your knowledge. This guide will accompany you, provide you with aid, and assist you in following up on the students' progress in understanding and comprehending the course. Where it explains the objectives that students are expected to learn at the end of each lesson.

Through this guide, you will be able to play your educational role and follow up on the student's progress as desired.

This guide has been designed for you to provide you with cognitive and educational strategies and information with the purpose of assisting you in the tasks required of you.

### Guide goals:

- Raising parents' awareness of the challenges of the digital world and the most important issues related to Cyber Security.
- Drafting clear instructions for parents so that they are aware of what interactive content is, its importance, its role in protecting students' Cyber Security, and the nature of the tasks assigned to them in this regard.
- Supporting parents by providing support and guidance to students for an in-depth understanding of the interactive content.
- Organizing the tasks of parents with regard to their role in students' follow-up and benefit from the content.



## Justification for drafting the guide:

- The need for a guide to help parents understand and implement their tasks in managing interactive content and directing students in this regard.
- Determine the processes and procedures entrusted to parents, given that parents' efforts are considered supportive of teachers' efforts.
- Helping parents understand modern technical information; so that they can support their children cognitively.
- Determining the duties and responsibilities of parents accurately helps to achieve the goals required of them with the highest level of excellence.
- Supporting the programs of the Ministry of Education and Higher Education to raise teachers' awareness of Cyber Security and related educational curricula.

## Starting points of the guide:

- Qatar Vision 2030.
- Successful studies and experiences (international and regional) in computing and information technology curricula.
- Distinguished Qatari experiences in the field of cyber security.



Third topic

**Characters and topics of  
Cyber Security educational  
curricula**





## First: Characters of the Cyber Security educational curricula:

### Teacher

#### The importance of the character in the curricula

A main character who is well-versed in computer technology and delivers knowledge to his students with ease and amusement.

#### Character appearance setting

School

#### Stage

Elementary/ Middle/ High School



## Female Teacher

### The importance of the character in the curricula

The female teacher's character sometimes substitutes the teacher. She is a very nice young woman who loves her students and gives them information in a smooth and enjoyable way.

### Character appearance setting

School

### Stage

Elementary/ Middle/ High School



## Naser

### The importance of the character in the curricula

A main character who is a diligent, courteous, and serious student who always has a lot of information about the subjects covered in the lessons and always participates.

### Character appearance setting

School/ family home

### Stage

Elementary/Middle/ High school



## Rashed

### The importance of the character in the curricula

A nice and calm student who likes to ask questions and deduce information.

### Character appearance setting

School

### Stage

Elementary/Middle/ High school





## Jassim

### The importance of the character in the curricula

A cheerful student who loves to create an atmosphere of fun, jokes with his classmates and his teacher, and is friendly with everyone.

### Character appearance setting

School

### Stage

Elementary/Middle/ High school



## Khaled

### The importance of the character in the curricula

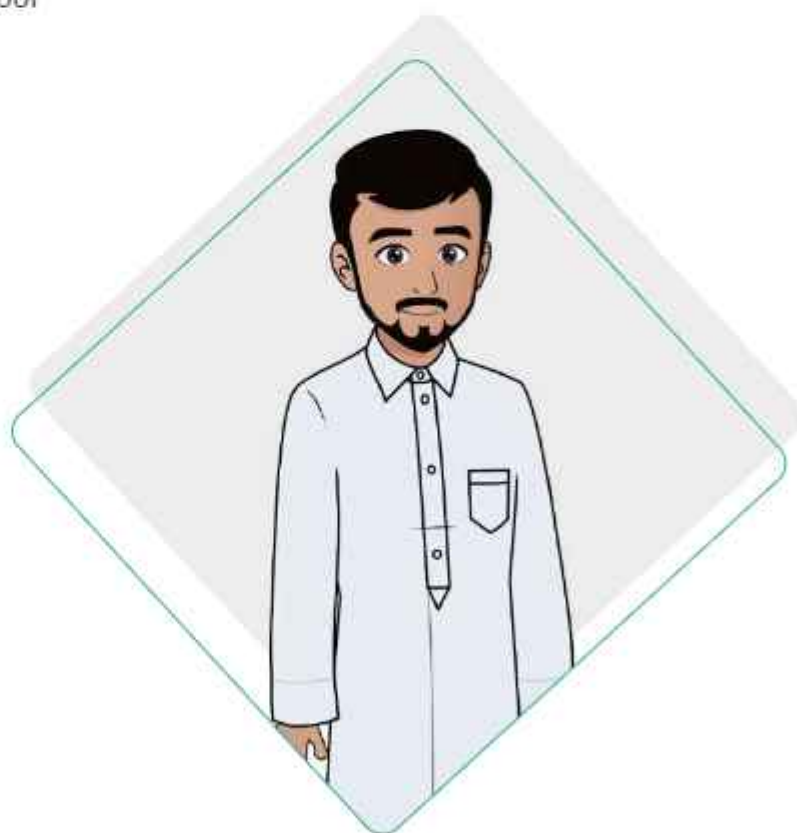
He is an intelligent older brother and is a polite, elegant young man who has extensive knowledge about information technology.

### Character appearance setting

family home

### Stage

Elementary/Middle/ High school



## Fatima

### The importance of the character in the curricula

A main character who is nice and helpful and a hardworking student who knows a lot about data and network security.

### Character appearance setting

family home

### Stage

Elementary/Middle/ High school



## Mohamed

### The importance of the character in the curricula

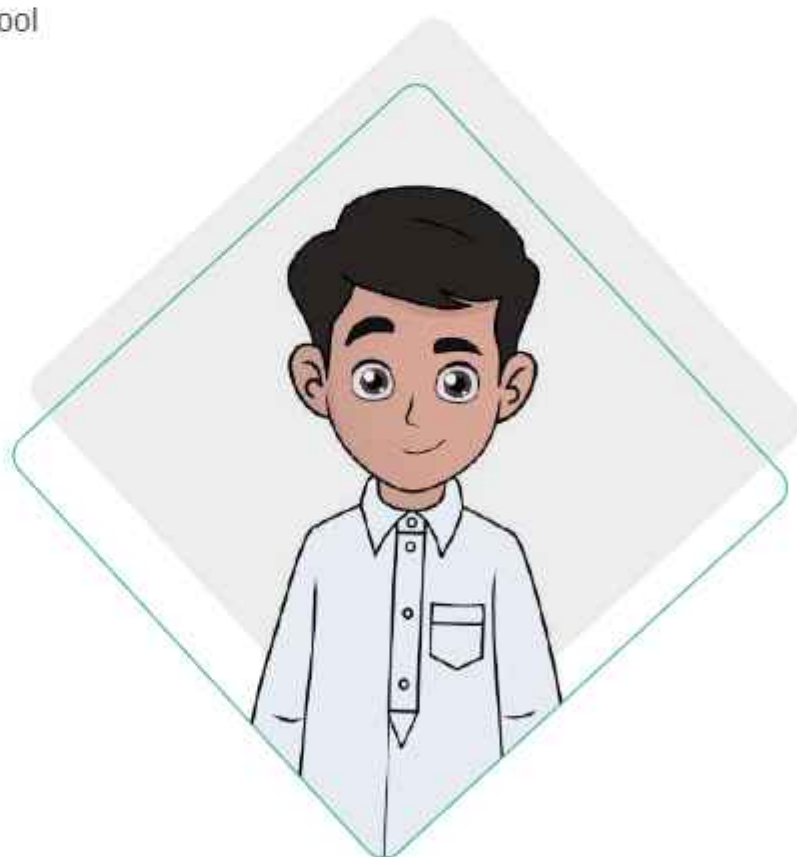
A cheerful child who is interested in learning and asks a lot of questions. He occasionally gets into trouble, but his siblings always help him and correct his mistakes.

### Character appearance setting

family home

### Stage

Elementary/Middle/ High school





## Mariam

### The importance of the character in the curricula

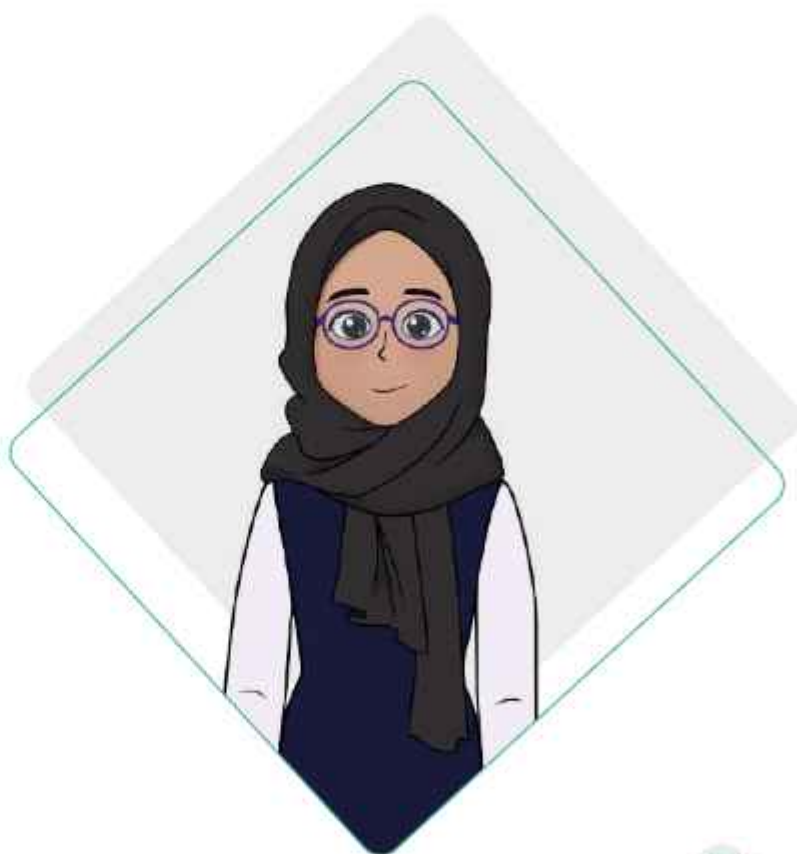
A nice and friendly person, diligent in school, and serious.

### Character appearance setting

Girls school

### Stage

High school



## Aisha

### The importance of the character in the curricula

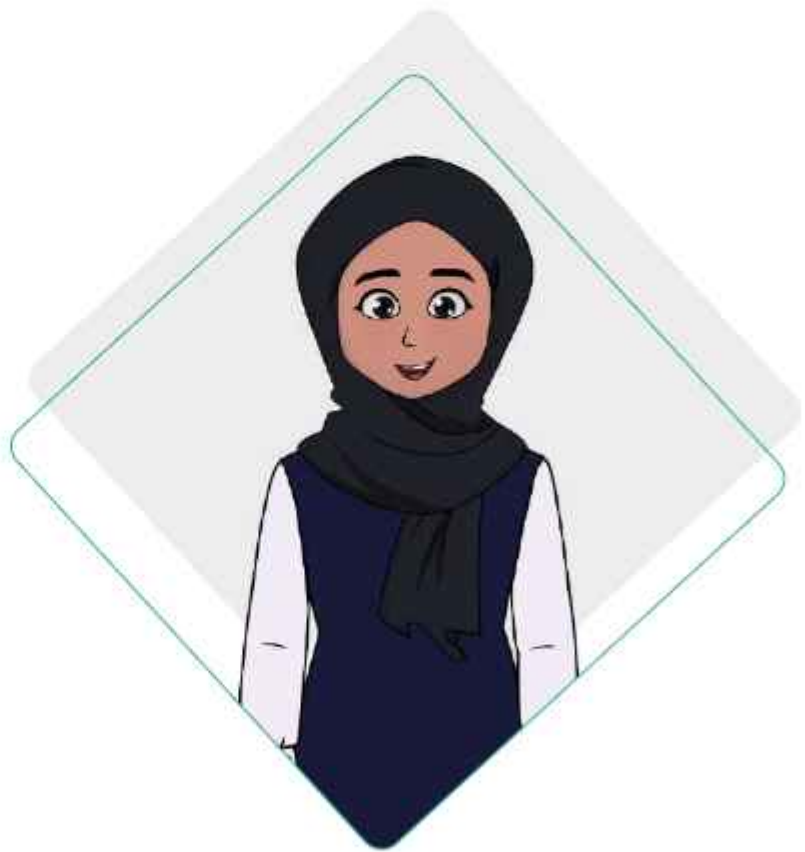
A jovial and rambunctious student who is less diligent than her two friends but who is always looking for information and asking questions.

### Character appearance setting

Girls school

### Stage

High school



## Saleh the Robot

### The importance of the character in the curricula

A main character who appears at the end of each visual content to provide a summary of the lesson and has the same form throughout all the lessons.

### Character appearance setting

School/ family home

### Stage

Elementary/Middle/ High school







## Second: Topics of the educational Cyber Security curricula:

### A- Visual content topics for the Elementary School:

<b>First grade</b>	<ul style="list-style-type: none"><li>• Safe use of the Internet.</li></ul>
<b>Second grade</b>	<ul style="list-style-type: none"><li>• Internet Safe Browsing Rules.</li></ul>
<b>Third grade</b>	<ul style="list-style-type: none"><li>• Safe use of e-mail.</li><li>• Reliable information on the Internet.</li><li>• Copyright.</li></ul>
<b>Fourth grade</b>	<ul style="list-style-type: none"><li>• Your health and the computer.</li><li>• Social isolation.</li><li>• Computer protection.</li><li>• Software licenses.</li></ul>
<b>Fifth grade</b>	<ul style="list-style-type: none"><li>• Intellectual copyrights.</li><li>• Digital piracy.</li></ul>
<b>Sixth grade</b>	<ul style="list-style-type: none"><li>• Online publishing and social media.</li><li>• Cyberbullying.</li></ul>

## B- Visual content topics for the middle school:

<b>Seventh grade</b>	<ul style="list-style-type: none"><li>• Malicious programs.</li><li>• Protecting networks from malicious programs.</li><li>• Social networks.</li><li>• The challenges of social networking.</li><li>• Computer security measures.</li><li>• Network communication protocols.</li></ul>
<b>Eighth grade</b>	<ul style="list-style-type: none"><li>• Data privacy.</li><li>• Children's personal information.</li></ul>
<b>Ninth grade</b>	<ul style="list-style-type: none"><li>• Backup and protecting databases.</li><li>• Backup and protect databases with passwords.</li><li>• Online meetings.</li><li>• Best practices for working online.</li></ul>



## C- Visual content topics for high school:

<b>Tenth grade</b>	<ul style="list-style-type: none"><li>• Evaluating information sources on the Internet.</li><li>• Tracking and privacy.</li><li>• Network security protocols.</li><li>• Security and usability.</li><li>• Surveillance systems.</li><li>• Sensors.</li><li>• Information security in commercial institutions.</li></ul>
<b>Eleventh grade</b>	<ul style="list-style-type: none"><li>• Research and verify the quality of the information.</li><li>• Data collection and verification.</li><li>• Data encryption.</li><li>• System Design - Security issues related to systems.</li><li>• Cloud computing - information security.</li><li>• Are my files safe on cloud storage?</li><li>• Raspberry PI-based projects - Security surveillance systems.</li><li>• Research and verify the quality of information (market study).</li></ul>

## Twelfth grade

- Online payment methods.
- Safe financial transactions over the Internet.
- Internet scams.
- Trust signs and safe connections.
- Digital security.
- The importance of information security and the triangle of protection.
- Cybercrime.
- Personal security precautions.
- Malware detection and removal.
- Ransomware attack.
- Firewall.
- File and folder permissions.
- Digital footprint.
- Digital tracking effects.
- Browsing social networks safely.
- Cyber Security and information security.





## Fourth topic

# Duties of Parents According to the Guideline





## Duties of Parents According to the Guideline

We provide you with this guide to serve as an important building block in supporting your tireless efforts in performing your important and pivotal role in achieving the desired impact of the program, through further enrichment and support for you. This guide will accompany you and provide you with assistance in following up on the understanding and understanding of the course your students.

Dear parent, it is hoped that you will be able to perform your educational role through this guide in the manner required of you in the most complete form, and this is achieved through:

- **Integration between your role at home and the role of a teacher at school:** The parent is entrusted with the responsibility of following up the progress of his children in the educational curriculum offered at school, and monitoring the extent of the positive impact of visual content on their level of awareness of digital space and their behaviors towards it, and integration may occur, for example, but not limited to:

- Checking the strength of the e-mail password (for example, at the primary level).
- Your knowledge of how to manage personal data (for all stages).
- Your follow-up to the student's research methods in reliable sources of information (for the High school stage).
- **Solidarity with the teacher:** The success of the Cyber Security curricula project requires the solidarity and cooperation of the parents with the school for constructive communication and achieving a safe response to any digital problems or issues through the following:
  - Informing the school of any problems or issues related to the digital security of your children.
  - Exchanging phone numbers of the competent authorities for urgent reporting of digital security breaches.

- **Permissions and prohibitions in relation to digital family security:** The teacher and the guardian are both responsible for the list of permissible and prohibitions for children regarding the use of technology, for example, but not limited to:
  - Using social media, and teaching children ways to deal with it.
  - Introducing safe means of communication for children of all ages.
  - Protection of creativity and intellectual property.
  - Introducing malicious programs and ways to protect family computers from them.
  - Electronic payment methods, and the limits of electronic shopping for parents and children.





**The guide also includes a set of tasks that parents must perform, most notably the following:**

- Providing a supportive environment for e-learning for students at home, in a manner that supports school education and its objectives.
- Understand the policies and procedures for dealing with interactive content across the Qatar Education System.
- Helping students organize viewing times for digital content and carrying out the activities required of them.
- Monitoring the extent to which students benefit from digital content and their understanding of the information related to it.
- Effective communication and cooperation with the school and teachers to follow up on the educational performance of students in interactive content and information technology curricula.
- Monitoring students' performance on the various tests related to the interactive content of computing curricula.
- Tracking continuous changes in students' behavior on the Internet, and constantly educating them about new developments and risks.
- Encouraging students to undergo continuous training on e-learning, which is available on the Qatar Education System.

## How parents interact with the visual content of Cyber Security educational curricula:

The visual content of the educational Cyber Security curricula is a modern model for raising students' awareness in the field of technology in an interesting and attractive manner. It comes within the framework of supporting the efforts of parents and families in protecting children and adolescents from the negative practices of technology and the various dangers surrounding them in the digital space and how to avoid them. Parents' dealings with visual content are divided into several stages. So that these stages are integrated to achieve the final goal of the curriculum.

**and the following is an explanation of these stages in detail:**

### The first stage: pre-digital content:

This stage includes the following tools and procedures:

- Watch the episode:**

The parent watches the visual content first on his own, defines its goals, and knows his role in discussing the content with his children.

### The second stage: Watching the visual content with the students:

At this stage, the parent watches the visual content accompanied by the student at home, noting the extent of his interaction and harmony with the content, and taking notes on this matter.



## Third stage: Post presentation:

At this stage, and after presenting the visual content to the students, the parent carries out a number of activities aimed at ascertaining the extent to which the content is absorbed and consolidating the new information in the student, and evaluating his cognitive interaction with it.

**The following is a detailed explanation of these activities, in order:**

### General enrichment questions:

These questions aim to know the students' initial impression of the visual content. The following are examples of these questions. The parent can choose other questions he deems appropriate:

- Was the visual content interesting?
- Who is the character that you liked? And why?
- What did you gain from the content?

### Interactive questions:

These questions aim to stimulate interactive education for students with their families. Asking such questions reveals to the parent the extent to which the student is compatible with the visual content and benefits from it. The following are examples of these questions:

- If you were in Nasser's place and the same thing happened to you, how would you act?
- How do you protect yourself from making the same mistake that Jassim made?
- I think you're going to change your password, right?

## Parents' notes during the presentation of the visual content:

The curriculum project adopts the provision of note cards for parents to write down their observations about the students during the display of the visual content, and after it is presented. This is under the condition that these notes are discussed with the class teacher on periodic dates because these notes are of great importance to the parent and the teacher. This is to monitor the students' interaction with the lesson and the visual content in general.

The following shows the shape of the parent's note card.

Parent's Notes Card							
visual content		Grade		student's name:		Teacher's Name	
Notes before visual content				Notes after the visual content			
Series	The title of the visual content	Student interaction	Accuracy of information	Linking information to reality	Accuracy of observation	The accuracy of the information	Link the information to reality
1							
2							
3							
4							
5							





The parent's notes card allows the teacher to track and monitor the various activities that the students perform during the different stages of the lesson, even at home. positively on the objectives of the lesson. It monitors the activities and interactions of the student and invests this feedback in knowing the individual cognitive and wire difference between the student and guiding each student.

## Characteristics and details of the note card, and an indication on how to deal with it:

### **Monitoring indicators of students' compatibility with visual content:**

This indicator allows the parent to monitor the indicators related to the student's compatibility with the visual content, and to take notes on the student, such as his preoccupation or follow-up on the visual content enthusiastically.

### **Monitoring the level of motivation towards learning among students:**

This is done by measuring the questioning index that the student poses to parents during and after viewing the visual content. Unlike others, some students may ask a lot about the course of the visual content and the information presented in it, and this is directly related to the level of cognitive curiosity which is a positive indicator of the student's ability to learn.

### **Monitoring the level of students' interaction with parents:**

This is done through the indicator of the student's response to the parent's questions during the presentation of the visual content, and in the post-presentation stage. These questions achieve several goals and include test questions aimed at monitoring the level of students' understanding of the visual content information and other supportive ones aimed at consolidating information among students, and the level of Students' interaction with questions varies from one student to another, and the notes card monitors this disparity.



## Understanding visual content:

Students' ability to understand the cognitive content presented through the visual content varies. Some students are able to understand and assimilate the cognitive content quickly with little support from their parents, while other students absorb the cognitive content at a slower speed, and need high-level support from their parents. Therefore, the parent must take notes on this matter.

## General Notes:

The card allows the parent to take any other notes, whether they are related to the behavioral or cognitive aspects of the student.

After the parent finishes taking notes, the points will be evaluated by the teacher according to the scientific approaches adopted in this field, and he will be informed of the results.





Fifth topic

**A brief summary of the  
educational visual contents**



In order for the parent to interact better with the visual content the student is exposed to during the educational stage, and to ensure that he has a good understanding of the content, he must first understand the objectives of the lessons and a brief summary of these visual contents, and sample questions on them, and then cooperate with the teacher in achieving the desired goals of lessons.

**The following are examples of educational visual content for each stage:**





# First Elementary school



## Safe use of the Internet

### Episode 1: First grade- Second semester

#### Episode summary:

This visual content discusses Internet safety, protecting personal information like passwords, pictures, and important information, and how to use the Internet safely, like keeping the family's phone numbers and other information private.

#### First: episode criteria and goals

##### ■ Episode criteria:

- The capacity to identify the risks of using the Internet.
- The capacity to identify the necessary security measures for Internet browsing.
- The capacity to identify personal information that cannot be shared online.

##### ■ Episode goals:

- For the student to know the most prominent rules for the use of the Internet.
- To educate the student about the significance of safeguarding their personal and crucial data.
- For the student to realize the importance of not sharing their personal data with anyone.

## Second: pre-presentation of visual content:

### ■ Preparing visual content:

- Preparing the student in an attractive way through Study conditions, and suitable information questions for their age.

### ■ Personal evaluation questions

- Do you have an idea about the risks of browsing the Internet?
- What is personal data? Give me some examples.
- What do you know about the Internet?
- Do you have an idea about the required rules for browsing the Internet safely?

## Third: During the presentation of visual content

During the presentation the teacher chooses certain timestamps to stop at, then asks questions regarding the events in it and about some of the concepts presented in the visual content.

## Fourth: After presenting visual content

### ■ Final evaluation questions:

- Determine the risks you can face while browsing the Internet.
- Define the necessary rules for browsing the Internet safely?
- What is personal data? Give an example.
- What do you know about viruses?





### ■ Enrichment activities:

**Role play:** The student, in a follow-up form, reenacts the visual content after each selects the desired character, gets asked about the motivation behind the choice, and repeats the process so that all students participate in the activity. The teacher takes notes as the activity is carried out.

### ■ Enrichment questions:

- How can you protect your personal data on the Internet?
- Mention 3 types of viruses that are harmful to computers.
- What would you do if you faced a problem when browsing the Internet?

### **Fifth: Taking notes of the episode:**

The teacher takes notes at the end of each episode and his evaluation of the students in individual and group cards.



## Second Middle school





# Malware

## Episode 1: Seventh grade- Second semester

### Episode summary:

This visual content discusses the dangers posed by malware that is intended to harm devices or corrupt data and prevent devices from functioning properly. Such as: Adware, Spyware, Worms, and Trojans

### First: episode criteria and goals:

#### ■ Episode criteria:

- The ability to define the concept of malware.
- The ability to define the types of malware.

#### ■ Episode goals:

- For students to learn the concept of malware.
- For students to learn the risks of malware.
- For students to give examples of malware.
- For students to be careful of malware when using their electronic devices.

## Second: Pre-presentation of visual content:

### ■ Preparing visual content:

Preparing the student in an attractive way through study conditions, and suitable information questions for their age.

### ■ Personal evaluation questions

- Are all software useful?
- What are malicious software programs?
- Can you protect yourself from malware?

## Third: During the presentation of visual content

During the presentation the teacher chooses certain timestamps to stop at, then asks questions regarding the events in it and about some of the concepts presented in the visual content.

## Fourth: After presenting visual content

### ■ Final evaluation questions:

- What is malware?
- How is malware created?
- Give examples of malware.
- Mention the effects of malware.



### ■ Enrichment activities:

**Roleplay:** The student, in a follow-up form, reenacts the visual content after each selects the desired character, gets asked about the motivation behind the choice, and repeats the process so that all students participate in the activity. The teacher takes notes as the activity is carried out.

### ■ Enrichment questions:

- How does malware harm your data?
- How do you identify malicious software? How do you avoid it when you use the Internet?
- How do you differentiate between malware and beneficial software?

### **Fifth: Taking notes of the episode:**

The teacher takes notes at the end of each episode and his evaluation of the students in individual and group cards.





## Third High school



## Evaluating Information Sources on the Internet

### Episode 1: Tenth grade - first-semester

#### Episode summary:

This visual content talks about how to evaluate information sources on the Internet through 6 basic criteria for evaluating electronic resources, which are: responsible party, purpose, coverage, accuracy, validity, objectivity, and credibility.

#### First: episode criteria and goals

##### ■ Episode criteria:

- The ability to identify reliable sources of information on the Internet.

##### ■ Episode goals:

- Students should be familiar with the method of evaluating information sources on the Internet.
- Students should be able to measure the accuracy of the information they obtain via the Internet.
- Students should obtain information via the Internet from reliable sources.

## **Second: pre-presentation of visual content:**

### **Preparing visual content:**

Preparing the student in an attractive way through study conditions, and suitable information questions for their age.

#### **■ Personal evaluation questions**

- Is all information on the Internet true and accurate?
- Is it possible to determine the accuracy and validity of the information on the Internet?
- Are there sources of information better than others?

## **Third: During the presentation of visual content**

During the presentation the teacher chooses certain timestamps to stop at, then asks questions regarding the events in it and about some of the concepts presented in the visual content.

## **Fourth: After presenting visual content:**

#### **■ Final evaluation questions:**

- What is meant by accurate and objective data?
- List the criteria for evaluating electronic resources.
- Is all the information we get online reliable?
- How do I know if the source of information is correct or not?





### ■ Enrichment activities:

**Student presentation:** With the supervision of the teacher the students create a presentation, where they play a guide to other students to train and educate them about the concepts they learned about from the visual content.

### ■ Enriching questions:

- Give examples of the basic criteria for evaluating electronic resources.
- Do you follow the criteria for evaluating electronic resources when searching for information?
- In your opinion, why is there so much misleading information and data on the Internet?

### **Fifth: Taking notes for the episode:**

The teacher takes notes at the end of each episode and his evaluation of the students in individual and group cards.



## Conclusion





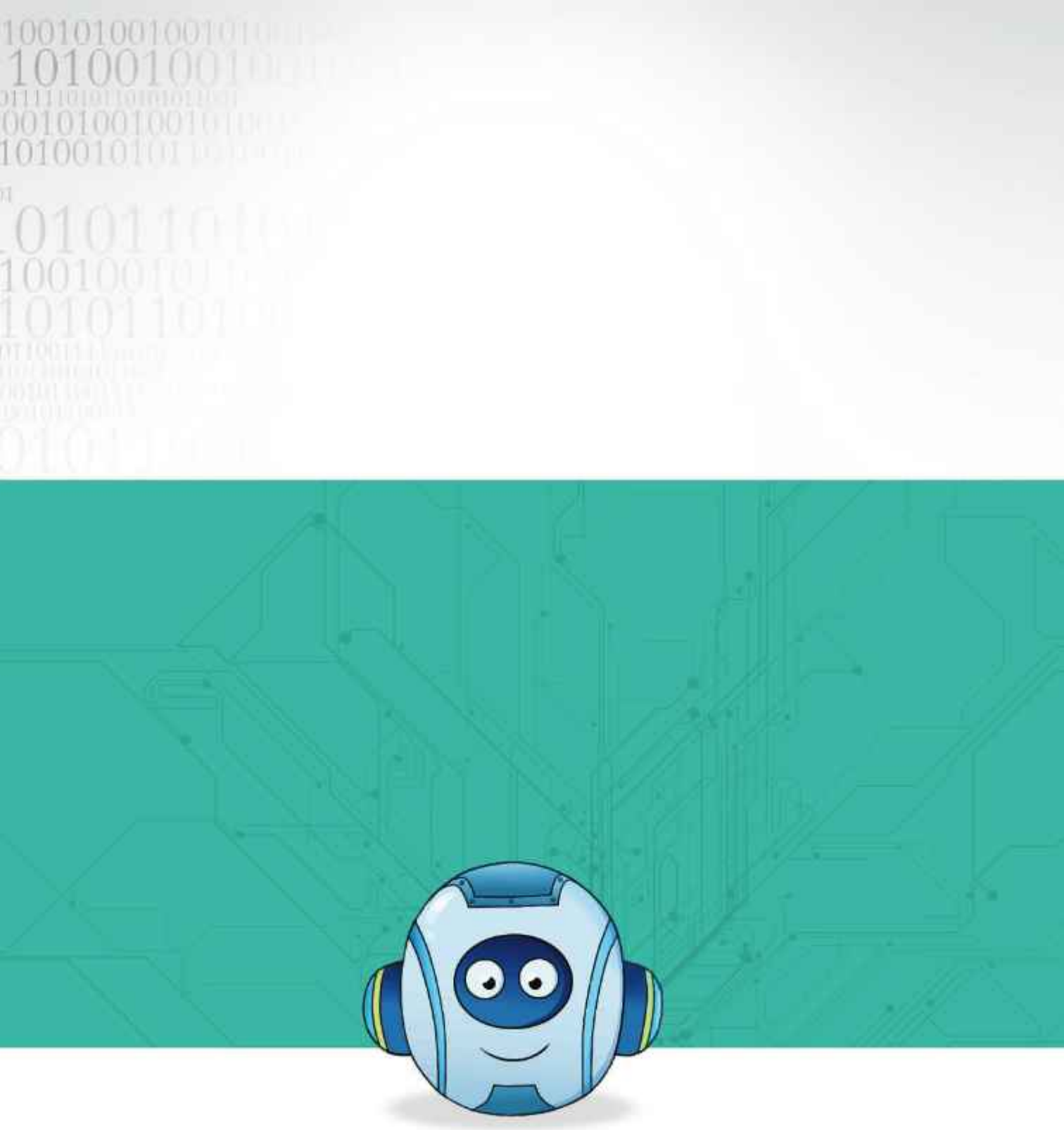
The exceptional experience of the National Agency for Cyber Security, in collaboration with the State of Qatar's Ministry of Education and Higher Education, in the creation of distinctive and efficient interactive content for various grades' educational Cyber Security curricula; It essentially aims to integrate practical reality into the interactive educational environment and to raise awareness of information technology and cyber security among school and university students, educational and educational staff, and parents. It also aims to keep them informed of the most pressing issues and developments in the field locally and globally. In order for the material and curriculum to accurately reflect our current environment. Despite its distinction and provision that exceeds human expectations, the modern digital revolution has negative consequences of extreme danger. Because the majority of Internet users are young people from schools and universities, they are the most vulnerable to threats like hacking and data tampering, and as a result, they are the first to pay attention to and raise their awareness. The parent is regarded as the primary educational partner and emphasizes his contribution to the children's learning success by regularly following up with them and preparing them

for e-learning in a way that complements and advances classroom instruction. In order to get the most out of e-learning opportunities, it also plays a crucial role in creating a conducive homeschooling environment. Because the parent is regarded as one of the most significant aspects of student interaction outside of schools and universities, he or she bears significant responsibility for directing them and keeping them informed of what has been accomplished in the classroom and through the Ministry's electronic platform. We hope that this guide will help the guardian meet his needs and improve his role in putting the Ministry's strategy for the interactive curriculum into action. The strategy should be compatible with approved classroom curricula and the produced interactive content, and everyone should work together to achieve the strategy's desired goals, which can only be accomplished with the cooperation of the educational system at all levels and by including the parent. The guide will be subject to review and scrutiny based on feedback from the educational field. We will work hard to improve and develop it in accordance with current and future digital and educational developments in order to meet the needs and aspirations of this guide in this regard.









 الوكالة الوطنية للأمن السيبراني  
National Cyber Security Agency

وزارة التربية والتعليم العالي  
Ministry of Education and Higher Education  
دولة قطر - State of Qatar