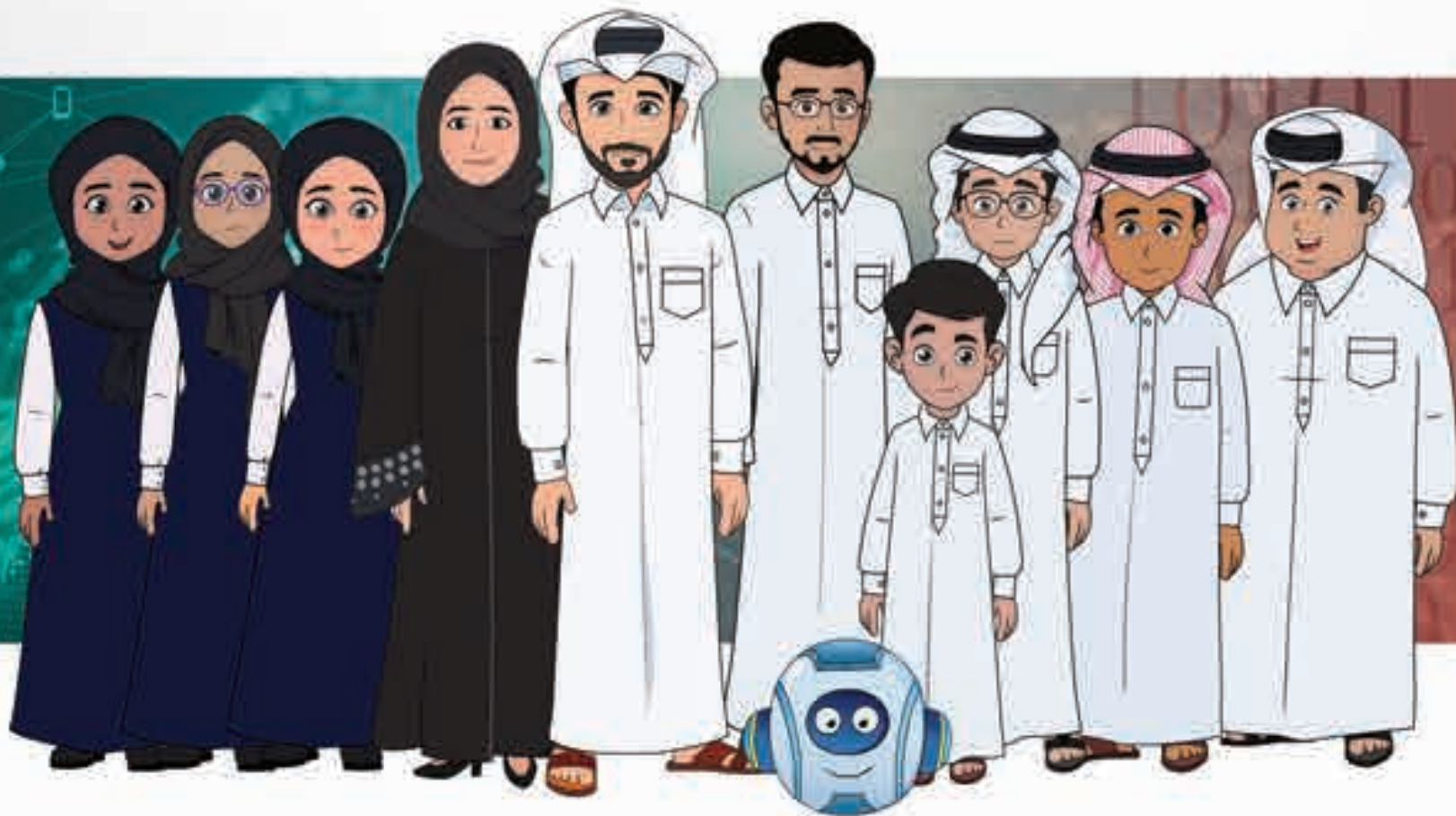
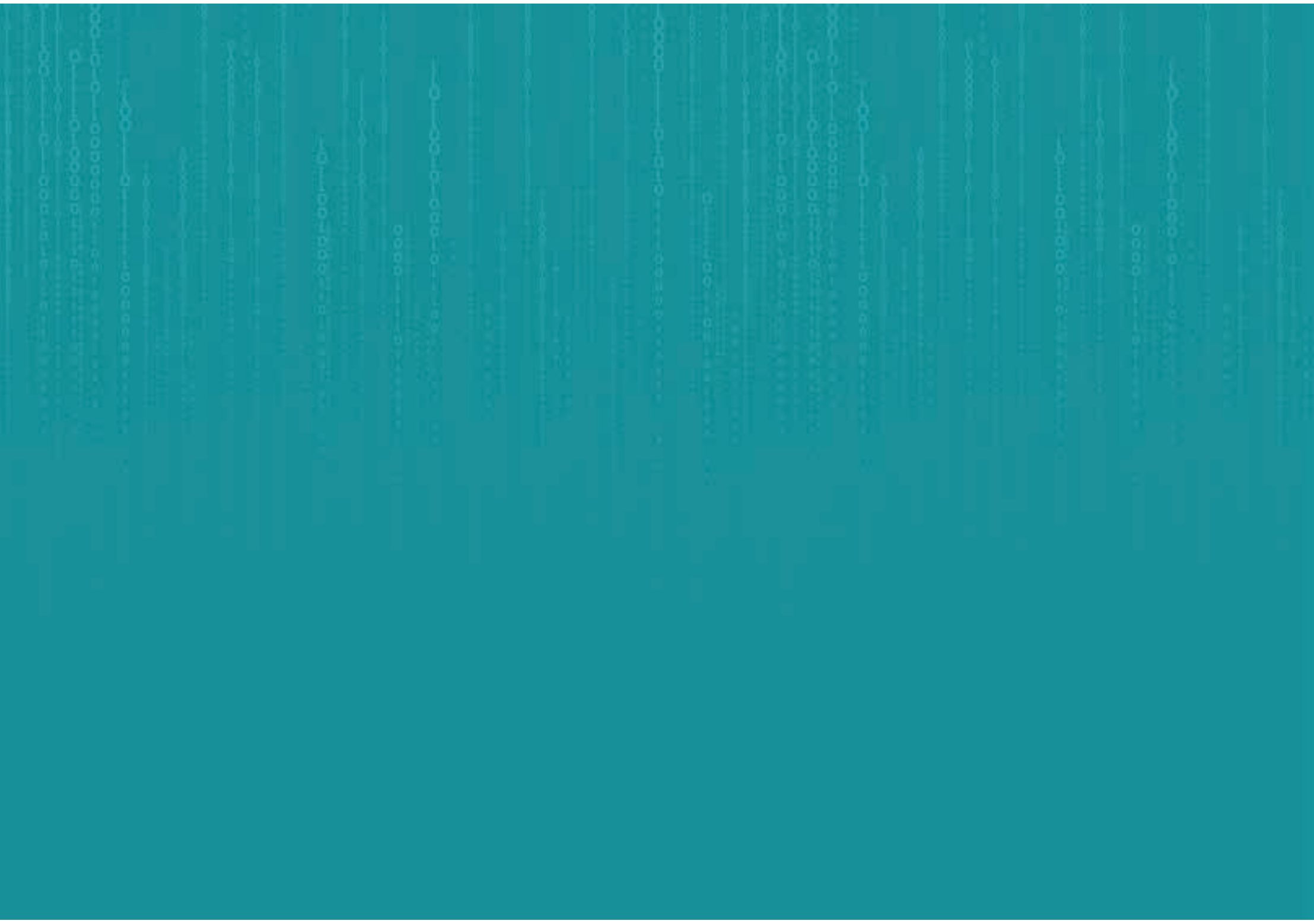




مناهج الأمن السيبراني التعليمية

Cyber Security Curricula Education





Index

Preface

Digital indicators for Qatar

Global Cyber Security

Cyber Security in the State of Qatar

The National Agency for Cyber Security's Online Platform

Cyber Security Education Curriculum Project (Overview)

Vision

What will the intended students be taught?

The importance of educational Cyber Security curricula

Cyber Security educational curricula tools

Topics and characters of educational Cyber Security curricula

Creating interactive materials for Cyber Security curricula

- Assessment of how well students use interactive materials
-

- Assessment methods
-

- Feedback
-

The Ministry of Education and Higher Education's online platform (LMS)

Work teams

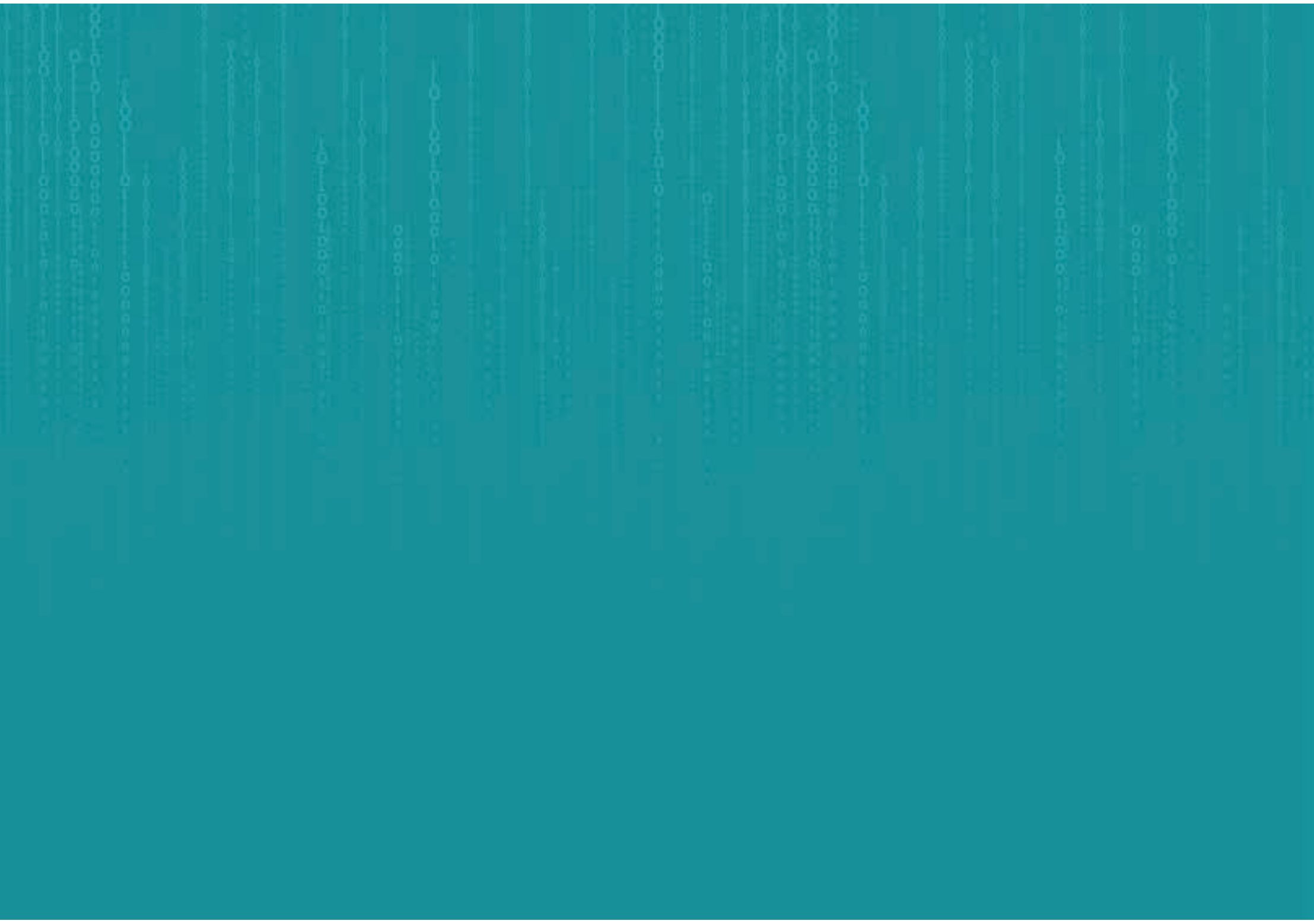
Teacher's guide

Parent's guide

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

Where might a plan for Cyber Security reach?

Conclusion



Preface

With the number of Internet users now exceeding half of the world's population, discussion of the rights associated with their presence on the network has become a topic of interest, research and study due to the necessity of achieving privacy and personal security without the occurrence of abuses that affect users' security or threatens their digital safety as well as the national security of their countries.

Because of the security risks posed by these developments, the State of Qatar was compelled to keep up with these rapid advancements in digital technology in order to safeguard its Internet users, particularly children and adolescents.

In this regard, Qatar relied on a precise scientific method to define the advantages and disadvantages of using the Internet and raise awareness of digital culture. With intention of creating a secure society and that both socially and digitally supporting the realizing Qatar's National Vision in 2030.

Consequently, and in light of the overall goals of the National Agency for Cyber Security; an integrated strategy to raise awareness of digital safety and the fundamentals and concepts of

Cyber Security is the only way to meet these developments and challenges and its focus in various segments of the community. The agency's digital platform for the purpose of directing appealing interactive visual content is its most prominent tool in general. On a specific note, a project to develop Educational Cyber Security Curricula for children and adolescents in various national schools was launched.

In the State of Qatar, the educational cyber security curricula designed for this significant age group aims to increase student's awareness of the various concepts, and foundations associated with digital safety and Cyber Security. This project is the first of its kind in the region, targeting all age groups, from the first grade of primary school to the twelfth grade of secondary school. This is based on the idea that educating a new generation about the dangers of cyber attacks, how to deal with them and how to assess their risk in a way that secures state institutions and achieves digital well-being; a goal that Qatar Vision 2030 aims to achieve by dedicating all of the state's resources to making it a reality that is taught in schools and implemented in practice on its land.



Cyber security in the state of Qatar

Cyber security has become one of the costs associated with rehabilitating a nation's infrastructure due to the growing reliance on information and communication technology (ICT) and the Internet by individuals, businesses, institutions and governments, particularly in vital sectors like the energy and financial sectors, to provide services more quickly and efficiently. In addition, cyberspace presents challenges that make it possible for individuals and businesses to have their data penetrated and harmed, at the same time it has folds of opportunities and possibilities for expansion in the future.

Based on the objectives of the National Communication and Information Technology Strategy 2015, which aims to protect the national vital information infrastructure and provide a safe environment for various sectors to provide integrated and secure electronic services, the State of Qatar has been eager to face these challenges and the risks and threats that exist now and in the future.

For this purpose, the "National Committee for Information Security," established in accordance with the Prime Minister's Resolution No. (18) for the year 2013 to organize a governance structure for collectively addressing cyber security concerns at the highest levels of government.

In 2021, the State of Qatar ranked third in the Arab world in the Global Cyber security Index "GCI" issued by the International Telecommunication Union "ITU", after the Kingdom of Saudi Arabia and the Sultanate of Oman, followed by the UAE, Kuwait and Bahrain.



The National Agency for Cyber security's Online Platform

Based on the previous objectives, and within the framework of the National Agency for Cyber security in the State of Qatar which aims to build a digitally safe local community and with the tremendous technological acceleration and the entry of technology into various aspects of the lives of citizens of all ages, the frequency of risks and threats arising from the use of the Internet has increased. As a result, the National Agency launched a national cyber security strategy to protect Qatari citizens and educate them about the concept of "digital citizenship," which is the responsible, ethical, and safe use of information and communication technology by individuals as members of the local community and global citizens.

This is why the National Agency for Cyber security launched a digital platform with interactive content (videos, short animations, infographic designs, and banner posters) as part of its strategy to raise awareness of digital safety concepts, the severity of cyber threats, and how to deal with them. In order to increase the benefit and awareness of the platform among adults and children, it will be made available to the general public for use both within and outside of the State of Qatar.

In addition, as part of the country's cyber security strategy, the National Agency for Cyber security is collaborating with the Ministry of Education and Higher Education to implement a project for computer and information technology-related educational cyber security curricula.

The project aims to educate schoolchildren, their parents, and teachers about cyber security and digital safety concepts, as well as the most significant obstacles they might encounter in their daily use of technology. A copy of the agency's interactive content, which is available on its digital platform, will be uploaded to the Ministry's LMS platform as part of this project for viewing by the curriculum project's target audience (students, teachers, and parents).



Cyber security Education Curriculum Project (Overview)

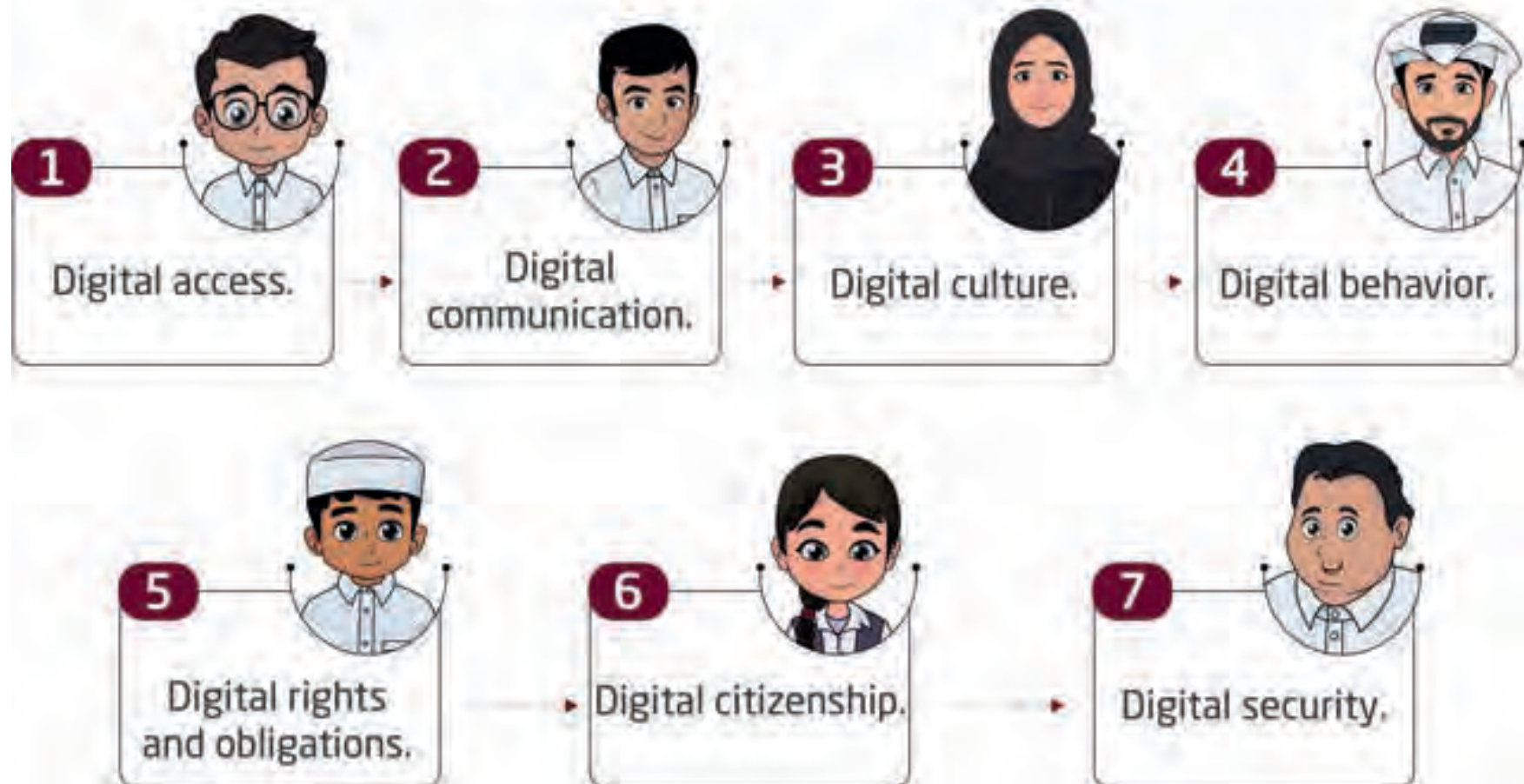
The State of Qatar believes that the only real way to protect against the dangers posed by technology is to raise a generation of children and teenagers who are capable of using technology responsibly, comprehending its risks and coping with them. As a result, the State has increasingly relied on educational institutions, teachers, and parents to educate students about the benefits and drawbacks of digital technology.

This is by promoting the concept of "digital citizenship," which was created as a result of the rapid development of digital technology and imposed a society similar to the typical society, so it was necessary to deal with it with regulations and laws that protects people's rights, privacy, and security. This made it imperative to teach cyber security to school students and make them aware of safety, citizenship and digital issues. There is no way to complete this except by formulating educational curricula that enhances awareness of digital safety and the concepts and foundations of cyber security.

As a result, the Cyber security Educational Curricula Project is sponsored by the National Agency for Cyber security in conjunction with the Ministry of Education and Higher Education. It targets students of all ages, from the first grade through the twelfth grade. This project is the first of its kind in the region as it aims to raise the awareness of children and adolescents in the State of Qatar of the various concepts and foundations related to digital safety and cyber security.

The increasing volume of losses incurred by various official and unofficial sectors as a result of cybercrimes that accompanied the technological boom that the world witnessed over the past two decades underscores the significance of introducing educational cyber security curricula, accordingly

cyber security curricula revolves around several main points



In accordance with the perceptions of children and adolescents, the curricula were given a great deal of leeway in order to accomplish the objectives outlined in them. Each age stage has its own curriculum and this allocation is thought to be an important starting point for achieving the curriculum's objectives. Throughout the various stages of education, the following examples demonstrate how the curriculum takes into account the psychological and age characteristics of students:

In the curricula directed to children in elementary school

The educational curriculum at this stage considers the demographic and psychological characteristics of children, such as being a very young age and their lack of experience. In line with children's cognitive abilities for this stage, the focus will be on engaging videos and visual products that captivate their interest in an entertaining and attractive fashion. 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 recognize these characters as their friends, from whom they derive valuable information and knowledge that they are looking for in the field of cyber security.

In the curricula directed to children in middle school

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 primary 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.

In the curricula directed to children in high school

In this stage, topics related to cloud computing, the basics of file protection, information about electronic attacks, threats, phishing and other relevant information are introduced in an age-appropriate way that considers the children's and adolescents' capability in analytical analysis and conclusion.

Parallel Education and Literacy Students

To ensure that the National Agency for Cyber security has the greatest possible impact on the targeted community, students in literacy programs and those in the parallel education track received the majority of the educational content so that the project reaches the entire intended audience. In this case, the same curriculum that was designed for all stages was used for students in parallel education and literacy programs.

The educational staff were also taken care of by the curriculum, whereas directing the training content for the educational staff in the State of Qatar's public and private schools is necessary to achieve the program's intended effect.

Because their training and rehabilitation contribute to the establishment of a teaching environment that is capable of delivering educational content to students effectively and with high efficiency, the educational staff is regarded as having a direct and close relationship with children and adolescents throughout the various educational stages. As a result, a guide for the various educational stages of the teaching staff was developed on the basis of this proposition.



The following points summarize several aspects of the significance of involving educational institutions in the digital preparation of students:

- Fostering a culture of conscious and rational use of digital technologies, enhancing associated behaviors, and increasing students' Internet proficiency and experience.
- Familiarizing students with the safe and legal use of digital technologies.
- Developing positive attitudes towards technology in a way that supports and enhances cooperation, learning and productivity.
- Encouraging lifelong learning as a personal obligation to acquire knowledge about anything that enhances one's well-being and raises the awareness of the subject.
- Educating students about the standards for sharing and dialogue in the virtual environment and fostering a culture of respect.
- Making the right decision when communicating through digital channels.
- Protecting personal information and data from hacking and theft.
- Reducing health, psychological and social risks resulting from digital addiction.
- Developing students' skills to prepare them for future work and providing them with special skills that are suitable for the rapid development of digital technology.



On the other hand, the curricula are aware that the project's efforts to build a digitally safe society are directly supported by qualifying and training parents on how to use modern technological tools and raising their awareness of cyber security and digital safety, as the presence of qualified parents on the safe use of technology is fully reflected positively on the children's environment and consequently, on Qatari society in all its facets.

During the three elementary school, middle school, and high school stages of the "Cyber Security Education Curricula" project, approved educational content is considered integrated, which applies to parallel literacy and education programs. Because each stage is a knowledge input for the subsequent stage, it is a single curriculum with integrated content. This integration is a major tool in achieving the project's objectives and the desired impact at the community level.

Vision

Creating a society that is technologically secure in order to achieve Qatar Vision 2030 on the social and digital levels. To do this, we must qualify and raise a generation that is aware of the dangers of digital technology, has control over electronic devices, and understands the relevant concepts in this regard.



What will the intended students be taught?

Networked computer systems and integrated communications systems make up cyberspace. One of the characteristics of modern societies is this space, which helps to facilitate rapid communication, distributed control systems, and the massive storage and transmission of data. These issues are now common knowledge in societies and are crucial to the successful operation of any kind of business.

Cyberspace is now everywhere, even in the military and intelligence fields, our reliance on it is growing. The connections between individuals, businesses, and governments have become more complicated as a result of this proliferation, making it challenging to manage or mitigate the challenges they pose.

With the daily news and reports about breaches of individuals and institutions worldwide, such as service disruptions, electronic fraud, privacy violations, and attacks on intellectual property, as well as what we can refer to as dangerous electronic and information warfare involves the disclosure of national security secrets. As such, one of the new issues brought on by the recent technological boom is what we now refer to as "cyber security," which has expanded the scope of the concept of national security.

This is something that state actors now look at with concern for national security. To deal with it and quickly respond to any emergency that threatens their security or the safety of their employees, they tend to form teams of trained individuals until we see entire departments specialized in cyber security whose responsibilities extend to all official and private state agencies.

Numerous nations have turned to students because of the rapid pace of cyber security challenges; to educate them about and introduce them to information and communication technology in order to raise their awareness. The State of Qatar was not immune to these difficulties, so it intends to develop an integrated curriculum that educated students of all ages to qualify them and raise their awareness, to face these difficulties and train them on how to deal with them effectively and professionally and to raise their cyber security awareness and prepare them for it.

The reference curriculum that has been provided is thought to be a good place to start and serves as an important exploratory method for raising cyber security awareness among young target audiences in schools, among parents and teachers. Given that technology has become a kind of luxury that nations strive to provide and make accessible to everyone, without exception, those with simple technical backgrounds on technology will find simplified illustrative responses to many issues related to cyber security practices that respond to their day-to-day needs.

In order to strike a balance between accessibility, usability, and cyberspace security, the cyber security educational curricula provide an in-depth, simplified reading of cyber security concepts.

As a result, the curricula include the social and educational aspects of students' interactions with electronic devices and various websites, as well as the study and processing of information related to information and communication technology, the examination of data security flaws and the search for technological solutions to them.

The curricula are designed to offer five main concepts:

- Informational life: utilizing information with self-assurance, independence and safety.
- Information tools: using digital tools creatively and choosing technology for a specific purpose and 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 manner.
- 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, to respect the privacy of others, be considerate of social aspects when dealing with social media and to use social media responsibly.



In summary, the following is what the students at the specified educational levels acquire,

- Instruction and training in how to secure email and browsers.
- Learn how to stay safe on social media.
- Educating children about cyber security.
- Learn about cyber security tools and how to use them to achieve the highest levels of protection.
- Learn about the most important hacking methods, means and approaches.



- Define and use key terms and concepts in the field of cyber security and understand what cyberspace means.
- Learn about the most important terms used in cyber security.
- Learn about antivirus and hacking software.
- Identify and define threat actors and their motives.
- Understand the preventive controls achieved by cyber security tools.

It is expected that the educational cyber security curricula will achieve several results for students,

- Properly, critically, creatively and responsibly explore, transfer, transform and manage information.
- Choosing and utilizing digital tools in everyday situations for their intended purposes.
- Use digital tools creatively, respond to communication, produce, process, analyze, share and display information depending on their level of knowledge.
- Recognize and determine the functions of digital devices and tools.
- Install computer tools that are appropriate for their age.
- Use digital tools in a safe and ethical manner.
- Acknowledging the difficulties of cyber security and the dangers of dealing with the Internet.
- Knowing how to deal with the problems and dangers they might encounter when using the internet and the various browsing sites.
- Enhancing their skills in dealing with electronic devices and their technological knowledge in a manner that does not compromise their social life or family values.



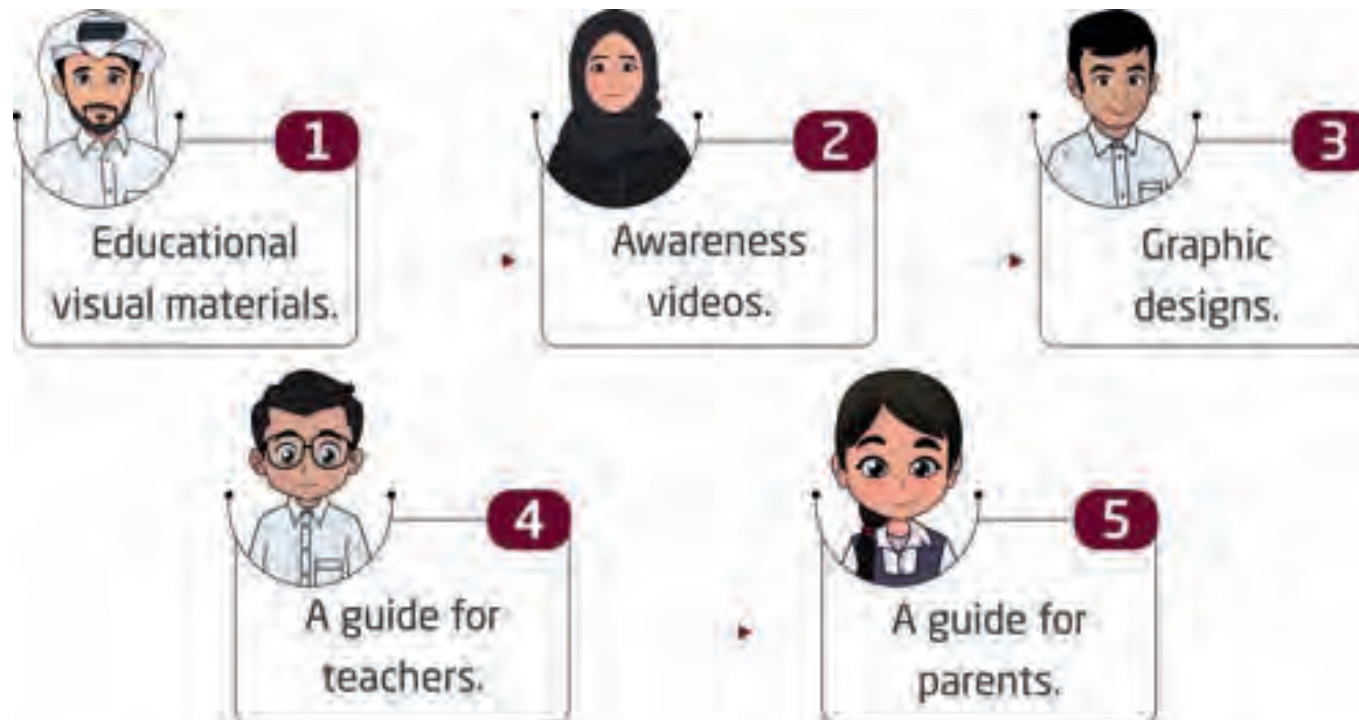
The importance of educational cyber security curricula

In collaboration with the Ministry of Education and Higher Education, the educational cyber security curriculum project aims to accomplish the following objective,

- Introducing the idea of digital citizenship—the responsible, ethical, and secure use of information and communication technology—to children and teenagers.
- Educating these younger generations about the risks posed by the Internet and the safe and responsible ways to use it.
- Rehabilitation of children and adolescents based on the protection of personal data and how to keep electronic devices safe from intrusion and hacking.
- Learn about general concepts related to cyber security and digital safety.
- Educating a young generation of Qataris who can effectively and professionally deal with digital technology to serve as the foundation for future cyber security specialists.

Cyber security educational curricula tools

The age range of the target groups in the educational stages necessitates the use of tools and techniques that are compatible with their level of awareness and enables them to comprehend the cyber security-related content for their benefit and for the Qatari government. Hence, several educational tools were used in an integrated manner that suits each age group and its own curricula, in order to teach cyber security curricula, which included the following,



Topics and characters of educational cyber security curricula」

Cyber security educational curricula tools

First grade	• Safe use of the Internet.
Second grade	• Guidelines for Safe Internet Use.
Third grade	• Safe use of email. • Trusted information on the Internet. • Copyright.
Fourth grade	• Your health and the computer. • Social isolation. • Protecting the computer. • Licensing software.
Fifth grade	• Intellectual property. • Digital piracy.
Sixth grade	• Online posting and social media. • Cyberbullying.

Seventh grade	• Malware. • Protecting networks from malware. • Social Media Networks. • The challenges of social networking. • Computer security measures. • Network communication protocols.
Eighth grade	• Data privacy. • Children's personal information
Ninth grade	• Backup and protecting databases. • Backup and protecting databases with passwords. • Online meetings. • Best practices for working online.
Tenth grade	• Evaluate information sources on the Internet. • Tracking and privacy. • Network security protocols.

	• Security and usability. • Surveillance systems. • Sensors. • Information security in commercial establishments.
Eleventh grade	• Research and verifying the quality of the information. • Data collection and verification. • Data encryption. • System Design - Security issues related to systems. • Cloud computing - information security. • Are my files safe on cloud storage? • Raspberry PI based projects - Security monitoring systems. • Research and verifying the quality of information (market study).
Twelfth grade	• Online payment methods. • Safe financial transactions over the Internet. • Internet scams. • Signs of trust and safe communication.

- Digital security.
- The importance of information security and the triangle of protection.
- Cybercrime.
- Personal security precautions.
- Malware detection and removal.
- Ransomware attack.
- Firewalls.
- File and folder permissions.
- Digital footprints.
- Digital tracking effects.
- Browsing social networks safely.
- Cyber security.

Characters of the educational cyber security curricula videos:

Male teacher

The importance of the characters in the curricula

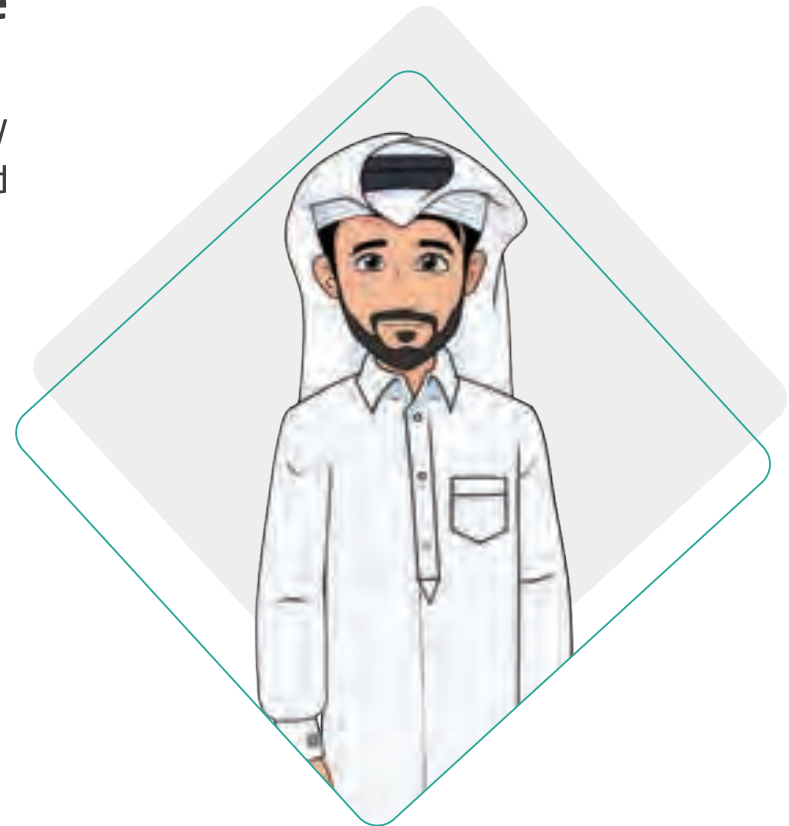
A main character who is well-versed in computer technology and conveys knowledge to his students with ease and amusement.

Character's appearance in the setting

School

Stage

Elementary school / Middle school / High School



Female teacher

The importance of the characters in the curricula

The female teacher sometimes deputizing for the male teacher. She is a kind young woman who loves her students and provides them with information in an easy and enjoyable manner.

Character's appearance in the setting

School

Stage

Elementary school/ High School



Nasser

The importance of the characters in the curricula

A main character, a diligent, polite and conscientious student, who always has rich information on the topics of the lessons, and is constantly participating.

Character's appearance in the setting

School/family home

Stage

Elementary school / Middle school / High School



Rashed

The importance of the characters in the curricula

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

Character's appearance in the setting

School

Stage

Elementary school / Middle school / High School



Jasim

The importance of the characters in the curricula

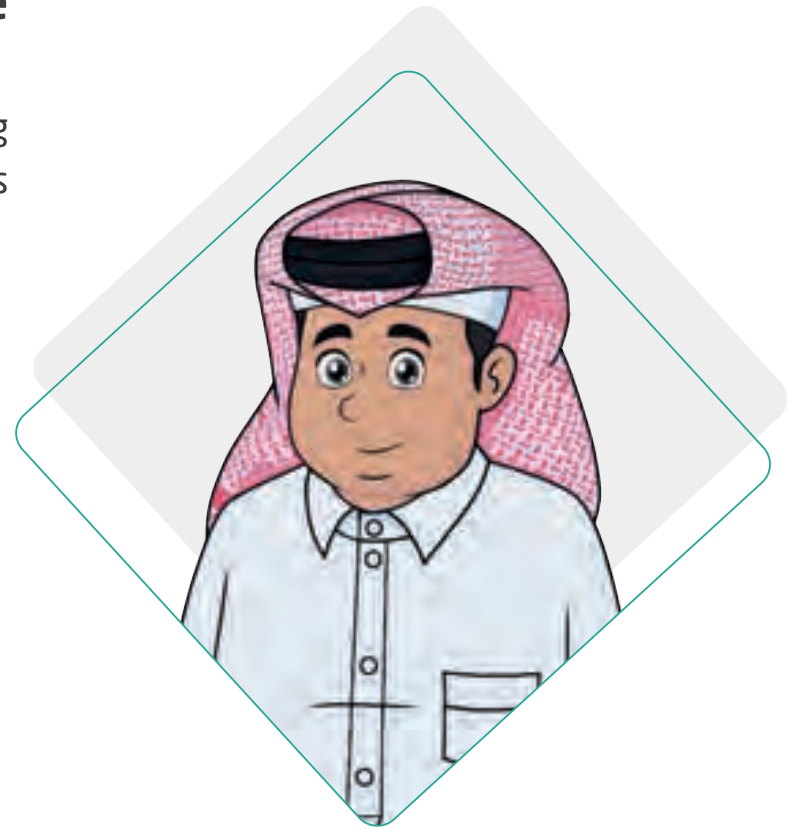
A cheerful student who enjoys making people laugh, making jokes with his classmates and teachers and making friends with everyone.

Character's appearance in the setting

School

Stage

Elementary school / Middle school / High School



Khaled

The importance of the characters in the curricula

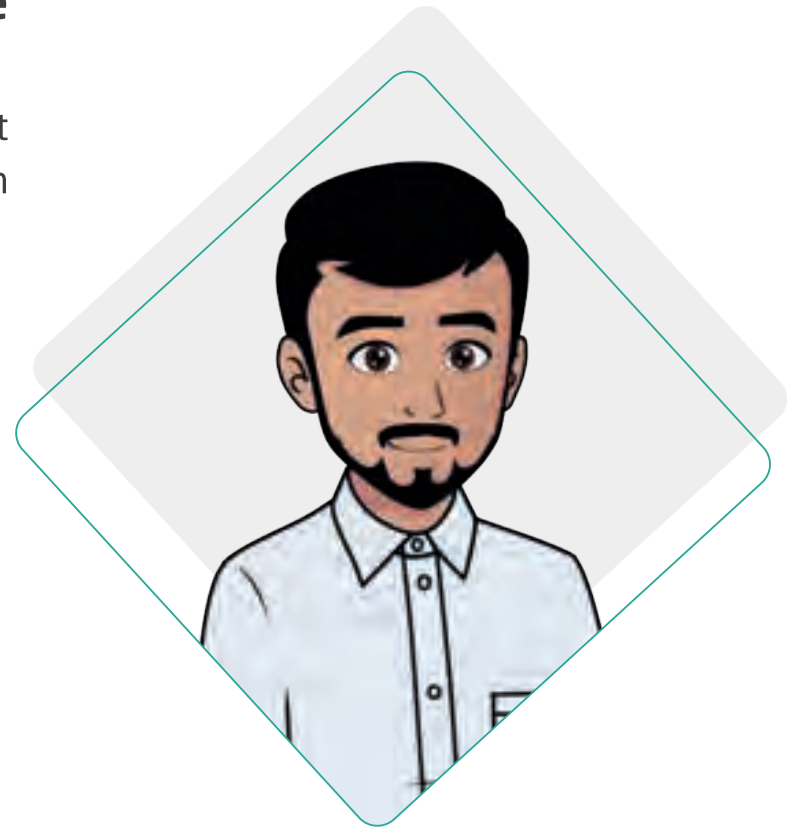
He is the mature older brother and he is a polite, elegant young man who has extensive knowledge of information technology.

Character's appearance in the setting

family home

Stage

Elementary school / Middle school / High School



Fatima

The importance of the characters in the curricula

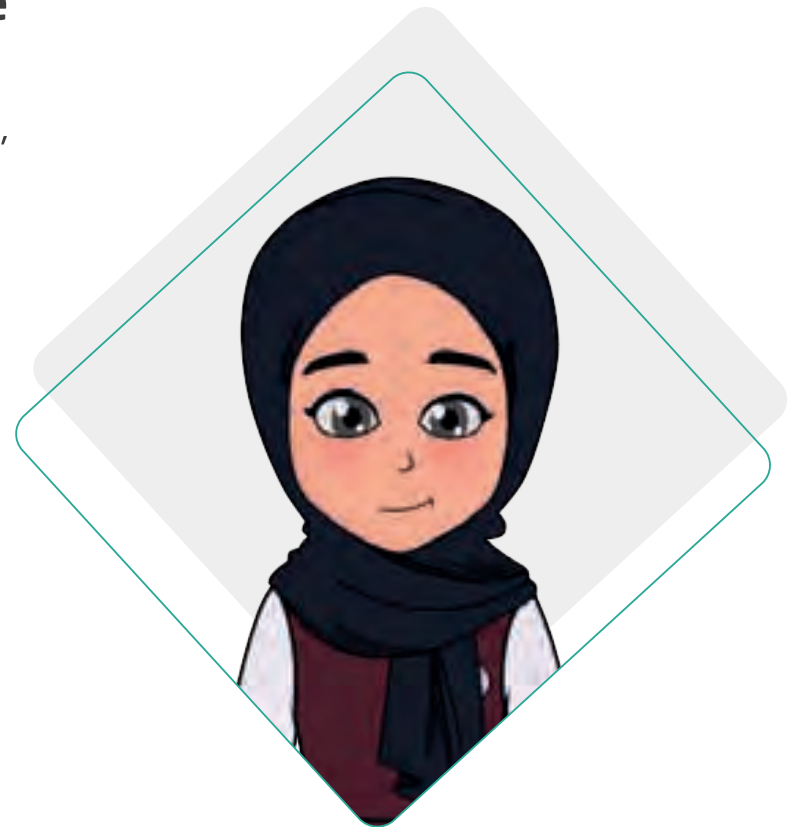
The main character, polite and kind and a diligent student, has a lot of information about data and network security.

Character's appearance in the setting

family home

Stage

Elementary school / Middle school / High School



Mohamed

The importance of the characters in the curricula

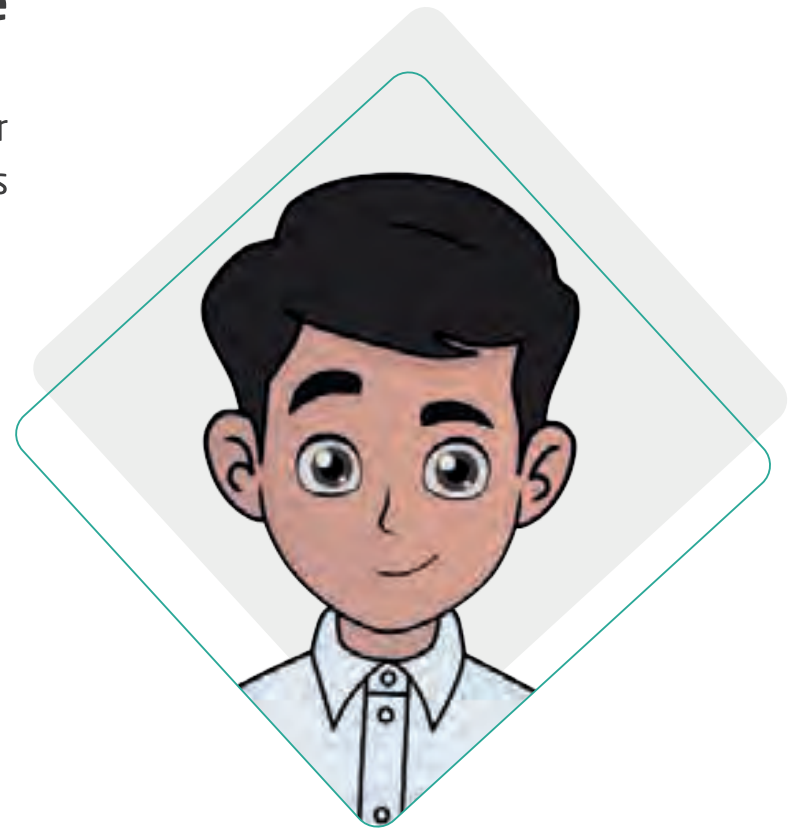
A cheerful child who asks many questions and is looking for knowledge. He gets into trouble sometimes and his siblings always guide him and fix his mistakes.

Character's appearance in the setting

family home

Stage

Middle school / High School



Mariam

The importance of the characters in the curricula

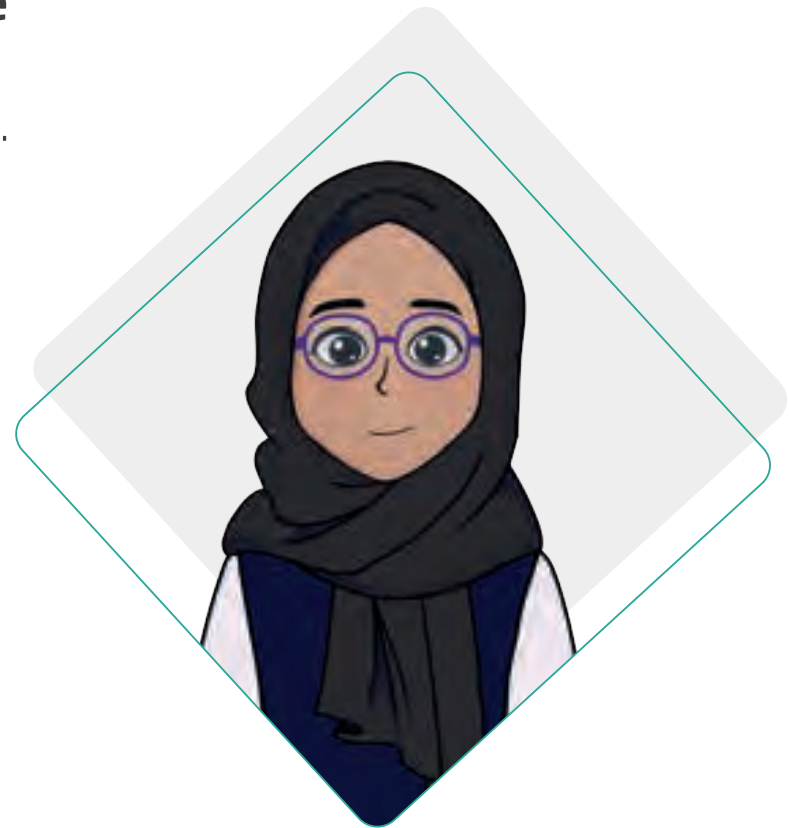
Enjoyable and friendly person, diligent in school and serious.

Character's appearance in the setting

Girls school

Stage

High School



Aisha

The importance of the characters in the curricula

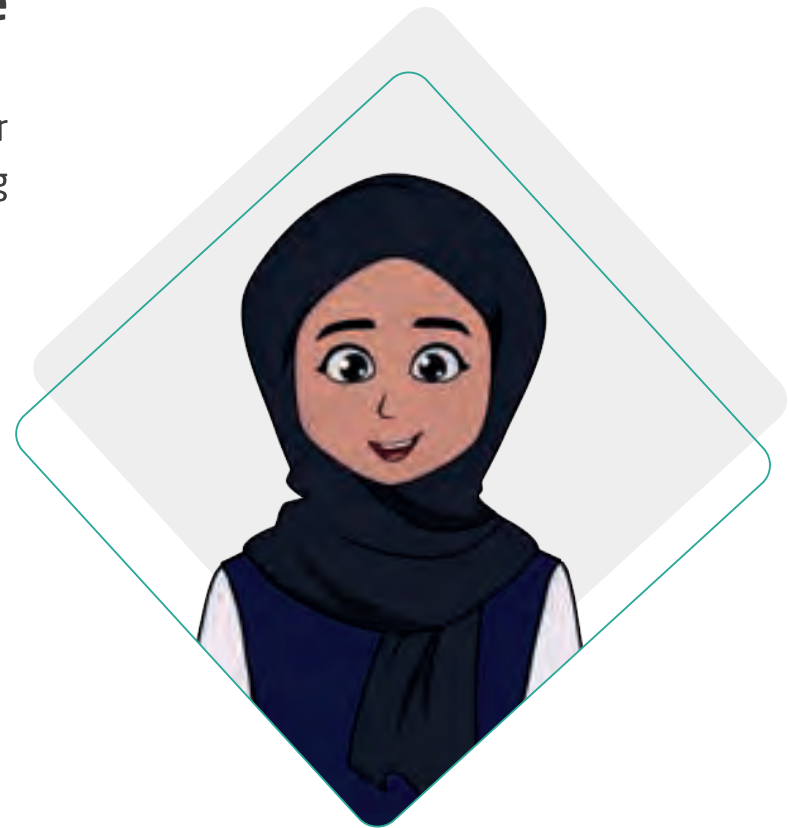
A cheerful and rambunctious student, less diligent than her two friends, but always asking questions and seeking knowledge.

Character's appearance in the setting

Girls school

Stage

High School



Saleh the Robot

The importance of the characters in the curricula

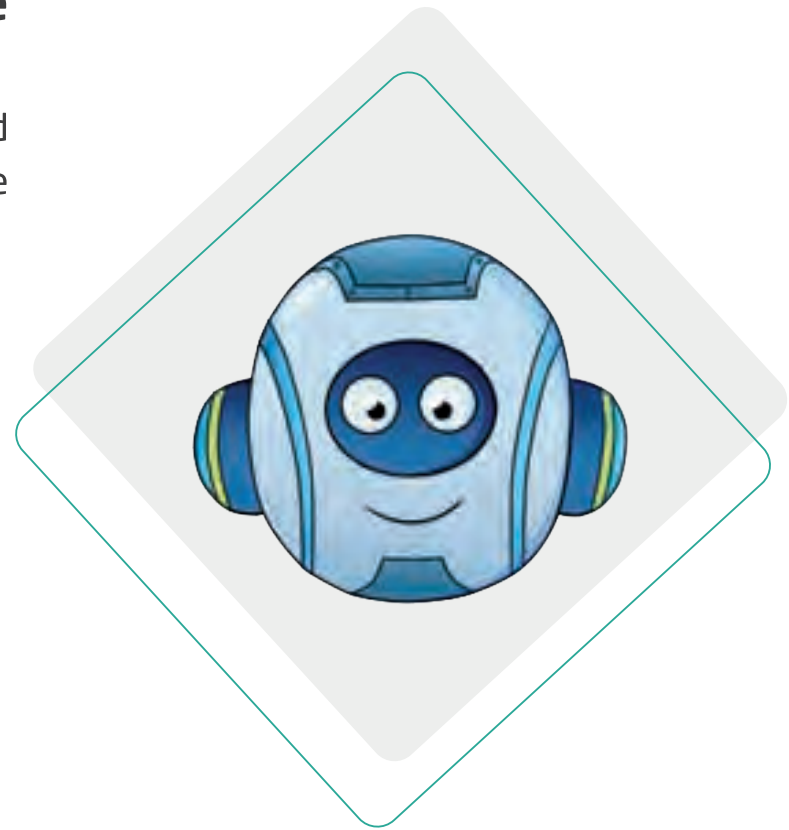
A main character in all stages, his look does not change and he appears at the end of each video to summarize the lesson.

Character's appearance in the setting

School/family home

Stage

Elementary school / Middle school / High School



Interactive content design

It goes without saying that the materials offered need to be varied in order to cater to the various age groups that cyber security curricula target. In order to achieve educational objectives from the content that is provided in a timely manner and with high efficiency, interactive content is one of the necessary explanation tools.

Therefore, in order to teach students about the significance of cyber security and how to use the Internet safely, the National Agency for Cyber security has partnered with the Ministry to design and implement innovative and varied interactive content. This content includes videos and short animations featuring beloved characters and is inspired by the Qatari environment and its social and intellectual values.

In addition, the interactive content consists of banner posters and infographic designs that concentrate on scientific content specialized in cyber security aspects. These will be first published on the electronic platform of the National Agency for Cyber security and will be accessible to all adults and children

within and outside of the State of Qatar. Through the electronic platform of the Ministry of Education in the LMS system, an additional copy of the content will also be made available to the specific audience of the curriculum project—students, teachers and parents—in the State of Qatar for their exclusive use.

The interactive content assists the instructor in developing a comprehensive picture of the taught curriculum and extracting the most significant lessons learned from it to present to the students in concise points in accordance with the grade-specific curricula.

When creating interactive materials for cyber security curricula, individual student differences were taken into consideration. The materials focused on a single concept at a time to keep students from being distracted and presented illustrative examples that made information easier for them to understand.



Evaluating comprehension capacities of students

The education process involves more than just giving the students the prescribed educational materials. It also involves assessing their level to see what has been accomplished in terms of the goals that the interactive materials try to present so that corrective actions can be taken based on a clear vision for any deficiencies in the curriculum.

The assessment method is based on a number of standards related to fundamental concepts and skills acquired through interactive content, real-world problems encountered by students every day and their use of technology to improve their perceptions, broaden their horizons and inspire them to keep learning.

The process of evaluating student performance is divided into several type,



Diagnostic evaluation

at the beginning of each lesson, students are evaluated with their knowledge gained and determine how much new information they are prepared to absorb.



Formative evaluation

It is a methodical, organized process that occurs during the teaching of interactive content. The goal is to improve the interactive content teaching and learning process, determine how far along students are in the curriculum and adjust the teaching and learning process accordingly.



Summative evaluation (Final):

It is the final assessment that the instructor conducts at the conclusion of the lesson, unit, or educational curriculum to ascertain the extent to which students comprehend the material and have achieved their objectives. Where the entire lesson, unit, or curriculum has been completed by the students.

In order to carry out the evaluation, a number of methods are used,

Tests:

these are done every week, every month, or every quarter to see how well students are doing with interactive content and how much they benefit from the information and skills they learn.

Evaluation of performance:

In order to evaluate the extent to which the student benefits from the interactive materials that are taught, the student is placed in a situation that resembles a life experience that he encounters when interacting on the Internet.

Observation:

this kind of test relies on the teacher's ability to accurately and efficiently observe how students respond to active situations involving interactive content in order to gauge their level of comprehension.

Meetings:

the teacher and the students meet to talk about the interactive content, its applicability to real-world situations and how they can benefit from it. The instructor can thus evaluate each student's level individually.

Portfolio:

this indicates that each student's scores on tests related to the lesson, unit, or curriculum are recorded in a file of his accomplishments over a predetermined time period, subject to the teacher reviewing them in light of predetermined rubric to determine whether or not his performance has met the desired standards and learning outcomes that are required.

Concept maps:

by creating a concept map and making clear connections between the concepts, the teacher helps the students identify the most important ideas in the interactive material.

Mutual evaluation:

where the teacher sets the rubric by which each student or group of students evaluates a classmate or another group of students.

Self-assessment:

using a set of questions the teacher has already developed, each student evaluates his or her level of comprehension of the interactive content, the lessons he learned from it, the strengths and weaknesses of the content, his or her own performance and their understanding of the curriculum and related content.

Real assessment:

It is the assessment of the learner's performance while they are completing real-world tasks and assignments that look like learning activities rather than typical test situations. In it, the teacher aims to involve the students in the application of their knowledge and skills through meaningful and realistic assignments. Where he engages in real-world activities that, in proportion to the level of what he has learned from the interactive content, require him to solve problems and make decisions, he exercises his mental operations as well as his discovery and investigation skills.

Following the stage in which the students' performance is evaluated, the stage in which they are informed of the assessment result occurs to direct them to the most effective and appropriate methods for collecting and utilizing the curriculum. This stage is referred to as feedback, which provides students with ongoing information on their performance in the interactive content, assists them in developing this performance positively and modifies it if necessary to ensure the achievement of the desired goals and objectives of those contents. This informs students of the outcome of their learning of the interactive content.

Feedback has several types, which are explained in the following points.



Corrective feedback

in which students are given feedback on how well they did with the interactive content and directed to additional learning resources that help them improve their knowledge and become more knowledgeable in the subject.



Explanatory feedback

students are given additional information to explain the reasons for the mistakes as well as the information that is confusing to them. They also talk about their weaknesses, which helps to reduce the likelihood of making the same theoretical or practical error again in the future, or they talk about their strengths and emphasize the correct information and experiments, which reinforces these points and enhances students' comprehension.



Rewarding feedback

students are provided with verbal or moral motivational phrases, or both, as well as information regarding the accuracy of their responses to questions pertaining to the interactive content, as well as discussing the reasons for the mistakes and correcting their incorrect responses and skills.



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

قناة قطر للتعليم



عزيزي ولي الامر / الطالب ، في حال رغبتك في معرفة الحساب الرسمي، إستعادة أو تغيير كلمة المرور، يمكنك الضغط على الرابط أدناه وإتباع الخطوات

الدخول على الحساب الرسمي / إغير كلمة المرور



حل التقييمات - حساب الطالب



تصفح الدروس - حساب الطالب



التعرف بالواجهة - حساب الطالب



تسجيل الدخول - حساب الطالب

The online platform of the Ministry of Education and Higher Education (LMS)

After being revised, reviewed, and officially approved by the National Agency for Cyber security, the produced interactive content will be uploaded to the Agency's electronic platform for public use within and outside the State of Qatar to maximize benefit and awareness among adults and children. A copy of it will be uploaded to the Ministry of Education's (LMS) platform in accordance with an agreement between the Agency and the Ministry of Education and Higher Education. This will make it permanently accessible to the project's intended audience, who can only access the platform (students, teachers and parents).

Platform features,

- 1/ A new system that has been applied since the academic year 2021-2022.
- 2/ This system relies on artificial intelligence and many advanced systems.
- 3/ Each student's academic level, behavior and class participation can all be examined with the assistance of the system.
- 4/ Teachers' performance can be analyzed and evaluated using the system.
- 5/ The system allows easy communication between parents and the school.

The team

The project's success is dependent on the availability of a qualified and experienced educational content work team with knowledge of educational content design, cyber security, digital safety, and e-learning principles. Therefore, the project relied on a group of consultants and experts in the field of cyber security at the National Agency for Cyber security.

A group of educational experts from the Ministry of Education and Higher Education's departments with expertise in this area were brought in to help achieve this objective and they were represented in,

1

E-learning and digital solutions management.

2

Educational Guidance Department, Information Technology Department.

3

Managing curricula and learning resources.

4

School Affairs Department, Programs and Activities department.

5

The Department of Special Education and Gifted Care.

The project team's philosophy is based on precise specialization. In order to ensure that the foundations of the task intersect with the work team's area of expertise, each task within the project framework has been assigned to a team of experts. There is a team that specializes in creating digital educational content based on cyber security and digital safety concepts, another team that specializes in delivering educational content to the intended audience and a design team that is highly skilled and specialized. The primary objective of the project, which is to design educational curricula that can increase awareness of digital safety and cyber security among the target society segments, is accomplished by integrating the expertise and competencies of the work team.

	National Agency for Cyber security	Ministry of Education and Higher Education
Work Teams	National Cyber Excellence. Management Team and Experts.	E-learning and digital solutions management.
		Educational Guidance Department- Department of Information Technology.
		Managing curricula and learning resources.
		School Affairs Department - Programs and Activities Department.
		The Department of Special Education and Gifted Care.

The teacher's guide

The teacher's guide is a set of steps, tips and instructions that the teacher is given to understand the strategy's nature and the roles it has been given in order to successfully implement it and get the best results for their students. By providing support to the teaching staff and expanding their knowledge, it aims to assist teachers in achieving the program's intended impact.

The educator can fulfill his educational responsibilities in accordance with the Ministry of Education's plan and in accordance with this guide. As the teacher's guide places the student at the center of the educational process, the guide is an important source of specialized and educational knowledge and information. It is designed to provide the teacher with strategies and cognitive and educational information to help him plan and implement lessons in a unique and effective way.



Parent's guide

The project's "Guidelines for Parents" are a set of procedural steps, tips and instructions for parents of students in the educational stages targeted by the project to help them understand the strategy's nature and the roles it plays in the success of its implementation and ensure the highest level of performance and results for their children.

By assisting parents and enriching their knowledge, this guide helps them achieve the program's intended impact. It assists them in monitoring students' comprehension and progress in the course; where it explains how to teach and the goals that the student should accomplish at the end of each lesson.

The parents can carry out their educational responsibilities in accordance with the Ministry of Education's plan and in accordance with this guide.



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

By proactively responding to and recovering from cyber attacks, the State of Qatar is intensifying its cyber security efforts and strengthening its cooperation with other nations to ensure an open and secure digital space. These efforts include protecting the country's essential information infrastructure and proactively responding to cyber-attacks. In addition to the legislation and legal framework that regulate the digital space, strengthening national cyber security capabilities, preparing a generation of talented professionals in this field and cultivating a culture of cyber security among citizens by educating them on how to use technology safely.

One of the first nations to make efforts to improve its national security was Qatar, which has recognized the significance of cyber security. As a result, it established the National Committee for Cyber security in 2013 to serve the Qatar National Vision 2030 and address the complex new global challenges.

The country's actions and measures reflect the rapid growth of its economy. Where the adoption of information and communication

technology serves as a foundation for innovation and prosperity in its numerous vital sectors, including health, electricity and energy and others, which led to the development of Qatari cyberspace to the point where it became an integral part of everyday life, posing national challenges and security threats.

Hence, the state frequently enacted legislation to regulate transactions in cyberspace, prevent cyber risks and punish cybercriminals. The inclusion of cyber security and safety on the Internet as one of the three main programs in the "National Strategy for Communications and Information Technology 2015," digital agenda for the State of Qatar. Because it is known as one of the major energy producers, the headquarters of international businesses and one of the early adopters of digital technologies in the region, it is susceptible to hacking and cyber attacks.

Qatar is one of the world's top 10 countries that has adopted information and communication technology and has made significant technological investments to become a regional pioneer. As Qatar, like the rest of the region, has a shortage of

professional workers in this field as well as dependable local cyber security service providers, putting Qatar's ability to protect the digital infrastructure in jeopardy, these investments have presented challenges, the most prominent of which is the provision of qualified and trained human cadres.

The nation faces the following additional difficulties: the global supply chain, which is made up of a number of interconnected systems all over the world, makes it harder to figure out how safe the components of the final products of information and communication technology are. This leaves gaps that some people can use to launch cyber attacks against government and private interests.

The availability of trained teams to intervene and take proactive measures is necessitated because connecting many productions and industries to internet networks increases the likelihood that control systems will be exposed to cyber threats. Examples of these industries include oil production, electricity generation, and water purification.

By directing the supply of qualified human resources for the labor market, the State of Qatar has recognized these obstacles and

worked to overcome them. In order to raise a generation that is aware of and competent in dealing with cyber challenges professionally and to attract distinguished skills in this field to work at the national level, cyber security curricula are a necessary entry point for the success of this approach for all businesses and government agencies.

In accordance with the Qatar National Vision 2030, which serves as a roadmap for transforming Qatar into a sophisticated society capable of sustainable development and aiming to provide a high standard of living for all citizens by 2030.

The "Educational Cyber security Curricula" project proves to be a useful and effective way for educators who are in charge of the next generation to show them how important cyber security is and educate them about it in a fun and useful manner and through this it is possible to impart knowledge to this generation that will safeguard them, ensure that they comprehend the difficulties posed by technology and teach them how to make the most of it without putting themselves in danger.

Given the significance it entails in the field of information technology and digital transformation, which is linked to every aspect of life, cyber security is an essential component of the

State of Qatar's national project. Given the digital transformation that the State of Qatar is experiencing within the framework of its national vision and aspirations for the future, cyber security is one of the most important requirements for the future.

It is necessary to use all resources in a thoughtful and rational manner in order to accomplish this, ensuring that people are built and educated, focusing on the younger generation and providing it with the necessary knowledge tools that contribute to enhancing its awareness and culture and preparing it to be able to respond to the requirements of the future and keep up with the development and progress that the world is experiencing, while at the same time preserving the Qatari people's national identity's core values and principles.

Where might a cyber security strategy reach?

As one of the first Arab and regional nations to recognize the significance of cyber security, Qatar has incorporated it into its strategic plans to safeguard its institutions and citizens from cyber attacks and information piracy.

The National Agency for Cyber security's strategy represented a significant shift in the state's approach to enhancing cyber security, safeguarding vital interests, national security, and sensitive infrastructure, raising a digitally aware generation of children and adolescents, and spreading societal awareness of digital culture.

In order to achieve a higher level of data protection and important capabilities in the information technology infrastructure, as well as to construct a tight line of defense from the competencies and national scientific knowledge to benefit from them, this significant progress in the strategy must include all sectors of the state, whether governmental or private. Finding and establishing partnerships with public and private research, academic, and industrial bodies, encouraging innovation, and encouraging local and foreign investment in the field of cyber security led to an unprecedented technical renaissance that serves society in all its segments, as well as qualifying and empowering more young cyber security professionals.



Conclusion

The educational cyber security curricula set a precedent for the State of Qatar in this crucial field and represents an exceptional experience in the region. These curricula are the result of a collaboration between the National Agency for Cyber security and the Ministry of Education and Higher Education. They serve as the foundation for raising a generation that is aware of cyber risks and has control over its affairs that enables it to deal with them effectively and with unique scientific and practical experience. Taking into account the cyber security curriculums that are available to students of all ages, from the first grade through the twelfth grade. In order to advance all segments of society at various levels of their education and experience in the field of technology, the curricula also paid attention to students of parallel education and literacy programs. They also prepared a guide for the teacher and prepared another guide that was suitable for the families of students.

A strong digital structure with technical tools and human cadres was necessary for this exceptional experience that brought together two important bodies in the State of Qatar to lay the groundwork for a national project that contributes to the realization of the country's 2030 vision, which targets sustainable development and the introduction of technology in all aspects of life. Because of this, it is able to repel and confront any cyber threats, as well as deal wisely and effectively with actual crimes and breaches that pose a threat to the security of Qatari citizens, public institutions, and the private sector.

This is based on the belief that, despite its distinction, the global digital boom carries extremely dangerous negatives that pose a threat to people's and nations' futures and calls for raising awareness and establishing concepts like digital citizenship.

Based on the significance of science in achieving sustainable development and raising people's awareness of the risks and requirements of the digital age, the educational cyber security curricula were Qatar's entry point to achieving these objectives. In order to achieve these objectives, the state is working to make the teacher one of the system's active components, alongside interactive content and curricula.

- main partner

وزارة التربية والتعليم العالي
Ministry of Education and Higher Education
Riyadh, Saudi Arabia



initiatives of



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency