SYLLABUS

ICDL Arabia

ICDL Module
Cyber Security for Educators and Teachers

Syllabus Version 1.0

Purpose

This document details the syllabus for the Cyber Security for Educators and Teachers module. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for the Cyber Security for Educators and teachers should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Disclaimer

Although every care has been taken by ICDL Foundation in the preparation of this publication, no warranty is given by ICDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ICDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ICDL Foundation at its own discretion and at any time without notice.

Cyber Security for Educators and Teachers in the K12- Environment

This module is designed to give a comprehensive overview of Cybersecurity for the educational realm. The outcome of this certification is to ensure that teachers and educational leadership teams have a solid understanding of the risks involved for students working online, and how they should identify and respond to such risks.

Module Goals

Successful candidates will be able to:

- Recognise the potential security risks and drawbacks of students engaging in various online activities.
- Develop and refresh teachers' awareness and understanding of student protection to help keep students safe online.
- Understand how to create effective plans to help protect students online, including supporting parents' concerns.
- Use various tools and techniques to secure and protect students with their online experiences.
- Recognise practical ways to keep students safe, like child-friendly search engines, privacy settings, and parental controls.
- Develop an awareness of online risks, like cyberbullying, inappropriate messages, sexual harassment, inappropriate websites, and online radicalisation, sharing (streaming) online and inappropriate use of social networking sites.
- Recognise how to help students manage Internet safety risks, including speaking with the students about online content and activities
- Understand the relevant legislation and ethical guidance for student safeguarding.
- Recognise the different types of online risks and signs of cyberbullying, to provide a suitable response for the students involved.
- Recognise the key elements of Cybersecurity policies and procedures.
- Track changes in children's online behaviour, updating them on new developments/risks.
- Understand a range of safety initiatives, such as awareness, strategies, and rules regulating online access and usage. Also, build children's digital resilience through safety and privacy.
- Understand how to use security policies and what resources are available.
- Understand and apply the concepts and principles of ethical thinking to problems relating to computers and digital technologies.
- Define the legal issues and be aware of what will happen when a student breaches cyber laws.

This module is based on the international practices and experiences of Cybersecurity for educators, specifically ages (K12-) from many leading countries in education, including:

- The UK Council for Child Internet Safety (UKCCIS)- Government of UK
- UK Safer Internet Centre

- Research Paper: children's use of the internet – London School of Economics and Political Science (LES)
- Organisation Stop it Now- UK and Ireland
- Australian Parenting Website
- Australian Parenting Website
- Office of the E-safety Commissioner- Government of Australia
- Federal Trade Commission – Protecting American's Consumer – US
- The Privacy Technical Assistance Center - U.S. Department of Education
- COSN Leading Education Innovation- Norway and Finland Built Innovative, Trusted Educational Environments.
- The K12 Cyber security Resource Center-Department of Education – Ohio - US
- Canada's Center for Digital and Media Literacy
- National Crime Agency – Child Line – UK
- US News Education
- The Security Awareness Company (SAC) –US
- Office of Education Technology (OET)
- Security Best Practices Guideline for Districts- Kentucky Department of Education
- City University of New York (CUNY) CUNY Academic Works- US
- United Nations Educational, Scientific and Cultural Organisation
- Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University
- Council of the Great City School – Baltimore City Public School – USA
- National Cybersecurity Centre- Government of UK

CATEGORY	SKILL SET	REF.	TASK ITEM
1: Use of the Internet and Social Networks in school	*1.1 The use of the Internet*	1.1.1	Recognise the benefits of using the Internet to support and enhance teaching and learning.
		1.1.2	Recognise the need to educate students that using the internet can result in risky activities, such as viewing inappropriate content or inappropriate communication.
	1.2 The use of Social Media	1.2.1	Outline the educational benefits gained with the use of digital technology and social media when used properly by teachers and by students.
		1.2.2	Outline the benefits of using social media platforms to support students in uploading and sharing classroom-led content.
		1.2.3	Recognise that social media can connect students to online global communities based on shared interests.

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.2.4	Outline the use of common social media networking platforms, such as Facebook, Instagram, Twitter, Snapchat and more.
2: Online Activity Risks	*2.1 Risks of harm to students online*	2.1.1	Recognise that students increasingly use portable devices to access the Internet, which can carry both benefits and risks.
		2.1.2	Outline what types of online content can be upsetting to students.
	2.2 Internet Safety Risks for students	2.2.1	Recognise the different types of risks students might face when they are online, including content, contact, and conduct.
		2.2.2	Be aware of the content risks students could accidentally access; including inappropriate websites.
		2.2.3	Be aware of the online risk Grooming.
		2.2.4	Understand conduct risks which include cyberbullying and improper messaging
		2.2.5	Outline the types of online risks students may encounter online, and recognise that risks vary depending on how the student interacts with the digital environment.
3. Social Networks	*3.1 Risks of Social Media*	3.1.1	Recognise the common Social Media sites that can pose risk, like cyberbullying and social engineering threats.
		3.1.2	Understand the term “digital footprint”
	3.2 Navigating the Risks of Social Media	3.2.1	Understand that communication with students provides an opportunity to protect them and ensure their online safety.
		3.2.2	Understand that social media platforms have age restrictions.
		3.2.3	Recognise that banning or blocking social media platforms is not an appropriate solution even for younger students.
	3.3 Social Media: E-Safety	3.3.1	Recognise that written guidelines on social media conduct can help students use social media responsibly, respectfully, and safely.
		3.3.2	Understand that proper guidance encourages good ethical behaviour, attitudes, and beliefs, including students’ technological use.

CATEGORY	SKILL SET	REF.	TASK ITEM
		3.3.3	Identify how to be a Responsible Digital Citizen and participant in online community life in an ethical and respectful manner.
		3.3.4	Outline best practises for youth when posting content and comments online.
		3.3.5	Recognise how to create student's privacy guidelines, settings and make shared decisions about the platforms to protect their privacy online.
		3.3.6	Be aware of safety essentials for students when they are using social media platforms.
		3.3.7	Understand how to create rules and guidelines, without prohibiting students from social sharing, like age-appropriate monitoring.
	3.4 Understand how different types of Social Media Apps may pose a risk	3.4.1	Understand the risks to students from using certain types of social media applications, for example, Calculators, Live.me, Yubo, and Blendr.
4: Online Risks & Harms	*4.1 Cyberbullying*	4.1.1	Define what is meant by cyberbullying.
		4.1.2	Identify the prominent issues associated with the growth of social networking websites and increasing technological sophistication amongst students; cyberbullying.
		4.1.3	Understand why cyberbullying happens
		4.1.4	Recognise the effects and risk factors of cyberbullying.
		4.1.5	Understand the different types of cyberbullying, and how and where it occurs.
		4.1.6	Understand how to spot cyberbullying signs, such as reduced academic performance, withdrawal, emotional and self-destructive behaviour.
		4.1.7	Recognise ways to help students avoid or reduce the risk of cyberbullying.
		4.1.8	Understand how to support victims of cyberbullying through the (G.E.T.R.I.D) steps of Go, Ensure, Tell, Report, Initiate and Delete.
		4.1.9	Recognise the role of parents to support students at home.
		4.1.10	Understand how to work with the student's school regarding bullying.
		4.1.11	Understand what can be done if a student requests non-involvement of the school.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.1.12	Understand how to promote a safe school environment if cyberbullying exists and continues.
		4.1.13	Understand what a student should know regarding Frenemies and toxic friendships.
	4.2 Online Advertising and Students	4.2.1	Understand where online advertising to students appears
		4.2.2	Understand how a student's age affects how online advertising is perceived.
		4.2.3	Understand how students can Identify fake and misleading advertisements
	4.3 Improper websites and videos	4.3.1	Understand what is meant by improper websites and videos
		4.3.2	Recognise the different attitudes students may have regarding improper websites and content.
		4.3.3	Identify where a student may come across improper content.
		4.3.4	Understand how to talk appropriately with students about improper content and how to safeguard against this on the Internet.
		4.3.5	Understand the guidelines to follow if a student has come across improper content online
		4.3.6	Understand what Educators can do when Students are found Surfing for Inappropriate Content Online
	4.4 Inappropriate messaging and sexual harassment	4.4.1	Understand what is meant by inappropriate messaging; sexting.
		4.4.2	Define the term Online Sexual Harassment.
		4.4.3	Define the term grooming.
		4.4.4	Understand how to recognise child sexual exploitation.
		4.4.5	Be aware of online behaviours that carry risks, such as images being shared without consent.
		4.4.6	Recognise the reasons why sending inappropriate messages can be a serious issue for students, and how this may lead to a digital footprint and cyberbullying.
		4.4.7	Identify the importance of talking with students about inappropriate messages
		4.4.8	Understand how to initiate a conversation about inappropriate messages to students

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.4.9	Understand how to respond if a student receives an unwanted/ explicit message.
		4.4.10	Recognise how to support a student that has sent an unwanted or explicit message
		4.4.11	Recognise what steps must be taken to support a student that has shared an inappropriate message.
		4.4.12	Recognise that students should build respectful online relationships with one another
		4.4.13	Recognise that inappropriate messaging involving a student under the age of 18 years is considered a criminal offense.
	4.5 Online Radicalisation	4.5.1	Identify what needs to be known about online radicalisation.
		4.5.2	Understand the role of the Internet and social media which can provide an opportunity for self-radicalisation.
		4.5.3	Recognise the characteristics of a vulnerable student and general indicators of vulnerability that are applicable to radicalisation.
		4.5.4	Understand how to prevent a student from being drawn into terrorism.
	4.6 Vulnerability and Victimhood	4.6.1	Define the terms Vulnerability and Victimhood and understand who is vulnerable online.
		4.6.2	Identify how to avoid being a victim of spam and phasing and how to be protected by using Stop, Think and Connect methodology.
		4.6.3	Recognise that students should not venture online without taking some basics precautions against Malware and Botnets.
		4.6.4	Understand what action to take in case a student is a victim of Identity Theft, Fraud, or Cybercrimes.
		4.6.5	Understand how students can protect their main resources, such as computers, tablets, iPads, etc.
	4.7 Respond to the Risks of "Live Streaming"	4.7.1	Understand what Live Streaming is over the Internet.
		4.7.2	Explain the opportunities and risks of live streaming when sharing content online.

CATEGORY	SKILL SET	REF.	TASK ITEM
5: Manage student's online safety	*5.1 Active Listening*	5.1.1	Recognise that active listening can be a powerful tool to improve communication and build a positive relationship with students.
		5.1.2	Outline the benefits of using active listening.
		5.1.3	Understand how to improve active listening skills.
		5.1.4	Recognise that problem-solving strategy is an important life skill to support solving students' problems.
	5.2 Confidence in Students	5.2.1	Understand why confidence helps students to surf safely online, make informed decisions and avoid dishonest people and risky situations.
		5.2.2	Understand how to build confidence and resilience in students by following special guidelines;
		5.2.3	Understand what action to take if a student suddenly lacks confidence or refuses to try new things.
	5.3 Student Moods: The ups and downs of Adolescence	5.3.1	Understand students' changing moods.
		5.3.2	Recognise students' motives such as physical and emotional.
		5.3.3	Understand the role of educators when dealing with students emotions. Learn new information to deal with student anxiety, and/or difficult emotions at school that can interfere with his/her
	5.4 Digital Citizenship	5.4.1	Recognise the importance of digital citizenship to keep students responsible and safe online.
		5.4.2	Outline the ways to be digitally responsible citizens, such as being respectful online and protecting other student's reputation. Be sceptical and not gullible.
	5.5 Digital Resilience in Students	5.5.1	Define the term Digital Resilience. Understand what being Digitally Resilience means.
		5.5.2	Identify the importance of digital resilience.
		5.5.3	Define the role of personal values and attitudes for building resilience.
		5.5.4	Understand that social skills are an important building block for resilience.
		5.5.5	Outline positive thinking habits for resilience to help students keep things in perspective by focusing on facts and reality.

CATEGORY	SKILL SET	REF.	TASK ITEM
		5.5.6	Recognise how to develop a student's digital resilience in order to support them in becoming active agents in their own protection and safety.
6: Initiatives to Safeguard Students Online	*6.1 Student Privacy, Monitoring & Trust*	6.1.1	Understand what constitutes a student's online privacy.
		6.1.2	Understand what a school's monitoring policy should include.
		6.1.3	Understand how monitoring online activity is important at school and at home
		6.1.4	Recognise that the use of surveillance apps may have negative effects on a student's trust
		6.1.5	Outline how to handle online breaches of trust or misuse of online privacy with students
	6.2 Keeping students safe online	6.2.1	Understand how to identify and manage Internet safety risks to protect students. Recognising the signs that a Student may be Abused Online.
		6.2.2	Understanding how to help students identify and manage internet safety risks.
		6.2.3	Understand the importance of open communication with students' regarding digital media, Internet usage and bad experiences online. Understand how to uncover online scams and hoaxes using Hoax-Slayer.
		6.2.4	Understand how to prevent students from becoming victims of cybercrime, downloading accidental viruses and how to ensure safe surfing.
	6.3 Teaching Safe & Responsible Online Behaviour	6.3.1	Outline how students can manage Internet safety risks by themselves.
		6.3.2	Recognise that apps and content can be reviewed for appropriateness by sharing online experiences with students
		6.3.3	Understand that an ongoing dialogue is required to keep communication channels open with your student
		6.3.4	Identify the risks for students regarding privacy and personal information.
		6.3.5	Understand how to converse appropriately when talking about online behaviour with students and the proper use of language.
		6.3.6	Recognise the role of parents regarding risks their children might face and help them to define proper strategies to protect their child at home.

CATEGORY	SKILL SET	REF.	TASK ITEM
	6.4 Discussing internet safety with students	6.4.1	Recognise signs that a student may be at risk of unwanted online behaviour
		6.4.2	Understand why Internet Parental Controls may also be used in school to protect students online.
		6.4.3	Understand what good Internet Tools & Habits can be adopted to protect students.
7: A Classroom Resource Guide for Engaging Students in Cybersecurity	*7.1 Classroom and Professional Development Resources*	7.1.1	Identify the stages of technology integration, which include substitution, augmentation, modification, and redefinition.
		7.1.2	Understand that students can be encouraged to practise Cybersecurity through school activities e.g. a boot camp or a competition.
		7.1.3	Recognise how to integrate Cybersecurity concepts into the classroom.
		7.1.4	Students practice safe strategies to C3 Framework
8: Cybersecurity Policy	*8.1 Writing Policy Guidelines*	8.1.1	Understand what policies should be covered to safeguard student's online activities.
		8.1.2	Understand what resources are required to implement and maintain an online school policy
		8.1.3	Understand which types of issues should be reported to the school
		8.1.4	Understand how to handle incident responses regarding student's digital devices.
9: Cyber Ethics	*9.1 What are the important ethical issues in cybersecurity?*	9.1.1	Understand the most popular ethical theories, like morality rules and ethics.
		9.1.2	Understand the importance of ethical issues when it comes to harming/benefiting students.
		9.1.3	Identify how educators should apply the code of ethics
		9.1.4	Understand how to monitor students effectively without breaching students' privacy.
		9.1.5	Understand how Educators should monitor student's activities.
	9.2 Ethics Perspectives: Networked Communications	9.2.1	Outline the ethics regarding sending messages.
		9.2.2	Recognise the ethics of important Internet Interactions.
		9.2.3	Recognise how to handle cyberbullying in an ethical way.
		9.2.4	Recognise signs of Internet Addiction and how to cope.

CATEGORY	SKILL SET	REF.	TASK ITEM
		9.2.5	Understand the ethics of inappropriate content when using digital technology including web filters and messaging.
10. Cyber Laws	*10.1 Awareness & Guidelines*	10.1.1	Understand how to distinguish between criminal offense and moral obligations. Understand the specific cyber laws that students may breach.
		10.1.2	Recognise how to protect intellectual property including trade secrets, trademarks, copyrights, and patents.
		10.1.3	Understand the privacy and confidentiality laws which are applied when posting photographs, and defamatory statements.
		10.1.4	Understand the legal implications of uploading and downloading media.
		10.1.5	Recognise that there are legal challenges with the use of social media.