

[Partner Logo]



ERF:

3. Digital Competence.

Project Partner Name

Jordan Youth Innovation Forum

Duration: 6.5



**Co-funded by
the European Union**

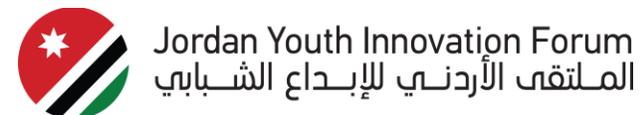
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project Consortium

Coordinator:



Partners:



Project Details

Title: “Joint Development, Piloting, and Validation of Entrepreneurial Mindset and Key Skills Curricula and Training Materials for Third Countries”

Acronym: EMSA (Entrepreneurial Mindset and Skills for All)

Agreement Number: 101092477 – EMSA – ERASMUS-EDU-2022-CB-VET

Programme: Erasmus+ Capacity Building in the Field of Vocational Education and Training (VET)

Call for Proposals: ERASMUS-EDU-2022-CB-VET

Start Date: 01.01.2023

End Date: 31.12.2025

General Principles, Mechanisms, and Logic Underlying Evolving Digital Technologies

Training Aim

To provide a comprehensive understanding of the key mechanisms and logic behind evolving digital technologies. This session will introduce participants to the fundamentals of digitalization, data protection, and GDPR, alongside data management skills essential in both personal and professional settings.



Engagement with Digital Technologies.

Learning Outcomes

All LOs of the Competence

In terms of **knowledge**:

- ✓ *Define digitalization and its core principles.*
- ✓ *Analyze reliable digital sources and retrieve relevant data.*
- ✓ *Describe GDPR compliance, data protection, and internet safety issues.*

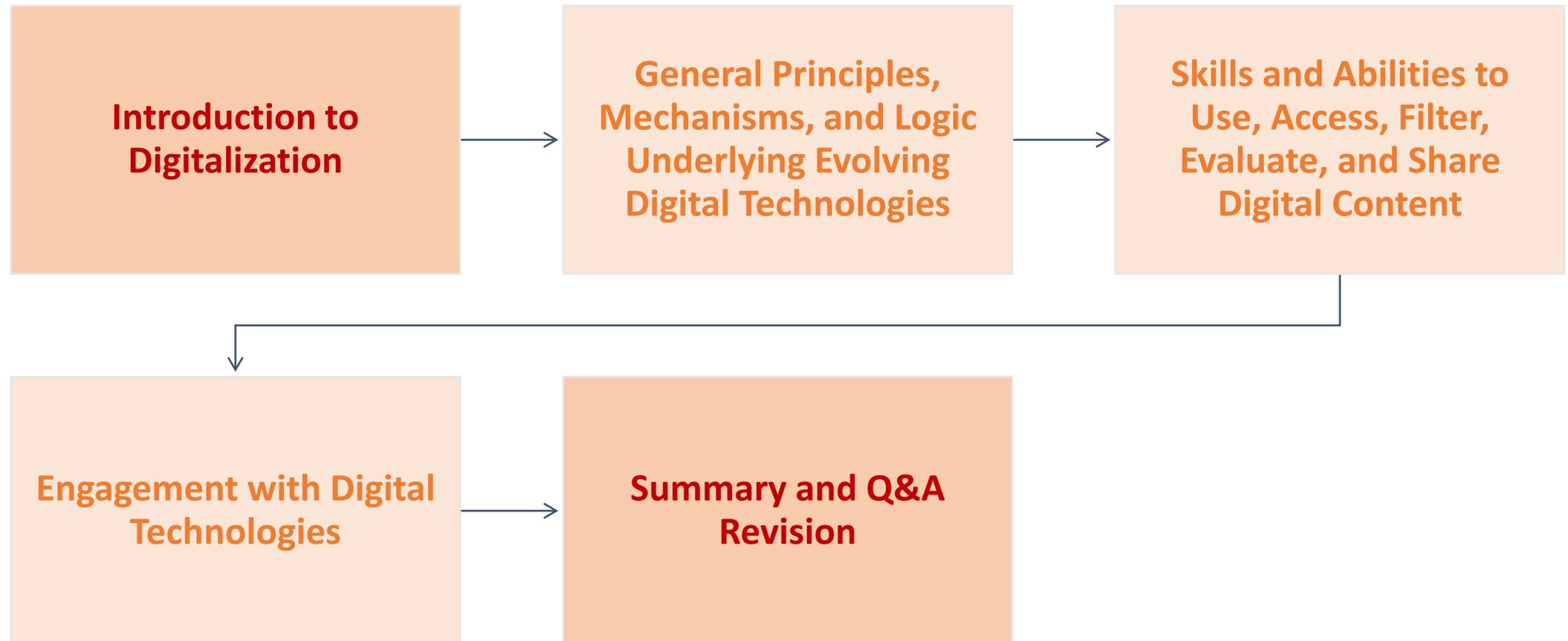
In terms of **skills**:

- ✓ *Demonstrate the ability to use cloud-based platforms for collaboration and digital content creation.*
- ✓ *Develop and share digital content using appropriate media platforms (text, images, audio, video).*
- ✓ *Apply tools like Google Analytics to evaluate the impact of digital content.*

In terms of **attitudes**:

- ✓ *Show respect for GDPR, data protection, and ethical standards while using digital technologies.*
- ✓ *Exhibit confidence in applying online etiquette and netiquette in various digital environments.*
- ✓ *Implement strategies to protect oneself and others from online dangers and risks.*

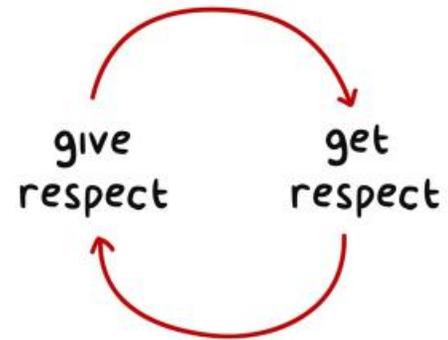
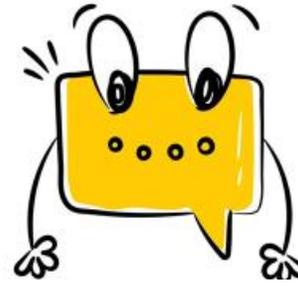
Training Route Map



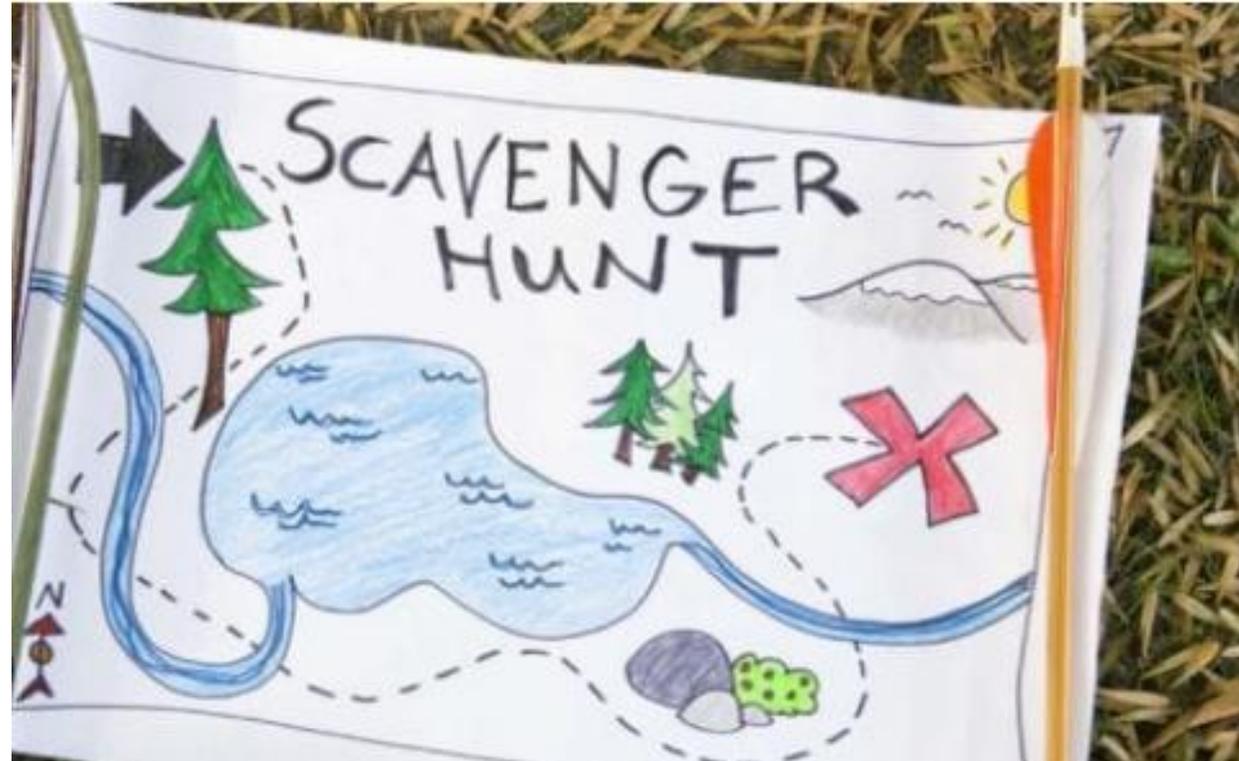
Digital Competence refers to the ability to confidently and responsibly use digital technologies in both personal and professional contexts. This course will focus on the mechanisms and principles behind digitalization, including data protection and GDPR compliance. Participants will explore the evolving landscape of digital technologies and learn how to apply digital management skills to ensure data safety, accuracy, and ethical use in today's interconnected world.

What ERF
competence
is our training about?

Training Rules



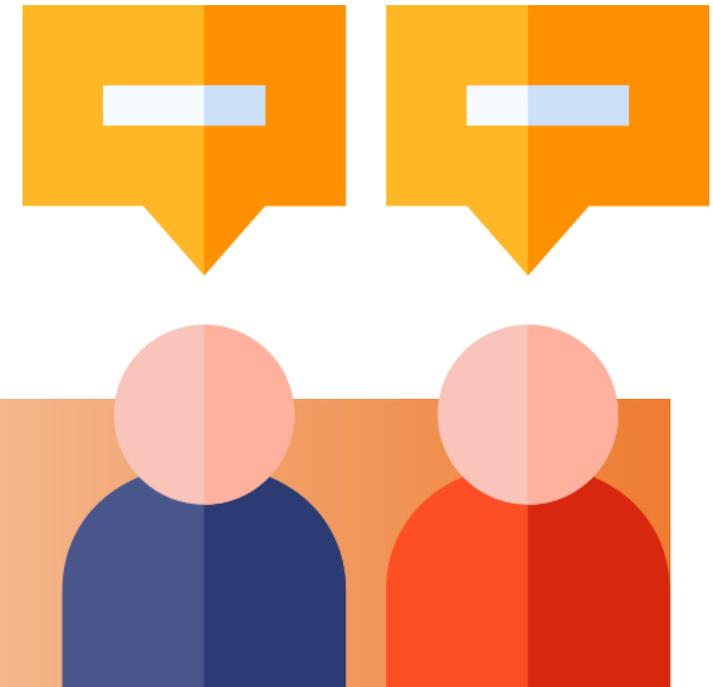
BREAK TIME



Icebreaker: "Virtual Scavenger Hunt"



MT3.1_6



Introductions

Let's get to know each other!

Quote on the Competence

*“Technology is best when it brings people together.”
Matt Mullenweg, Founder of WordPress*

Introduction to Digitalization

Introduction to Digitalization

- **Definition of Digitalization:**

Digitalization refers to the integration of digital technologies into everyday processes and activities, transforming how businesses, governments, and individuals operate. It involves converting information into a digital format, optimizing workflows, and enabling new ways of communication and service delivery. Digitalization extends beyond merely digitizing existing data—it reshapes entire business models, economic sectors, and societal functions by harnessing the power of digital technologies to create value, improve efficiency, and enhance experiences.





Aspects and Examples

- **Key Aspects:**

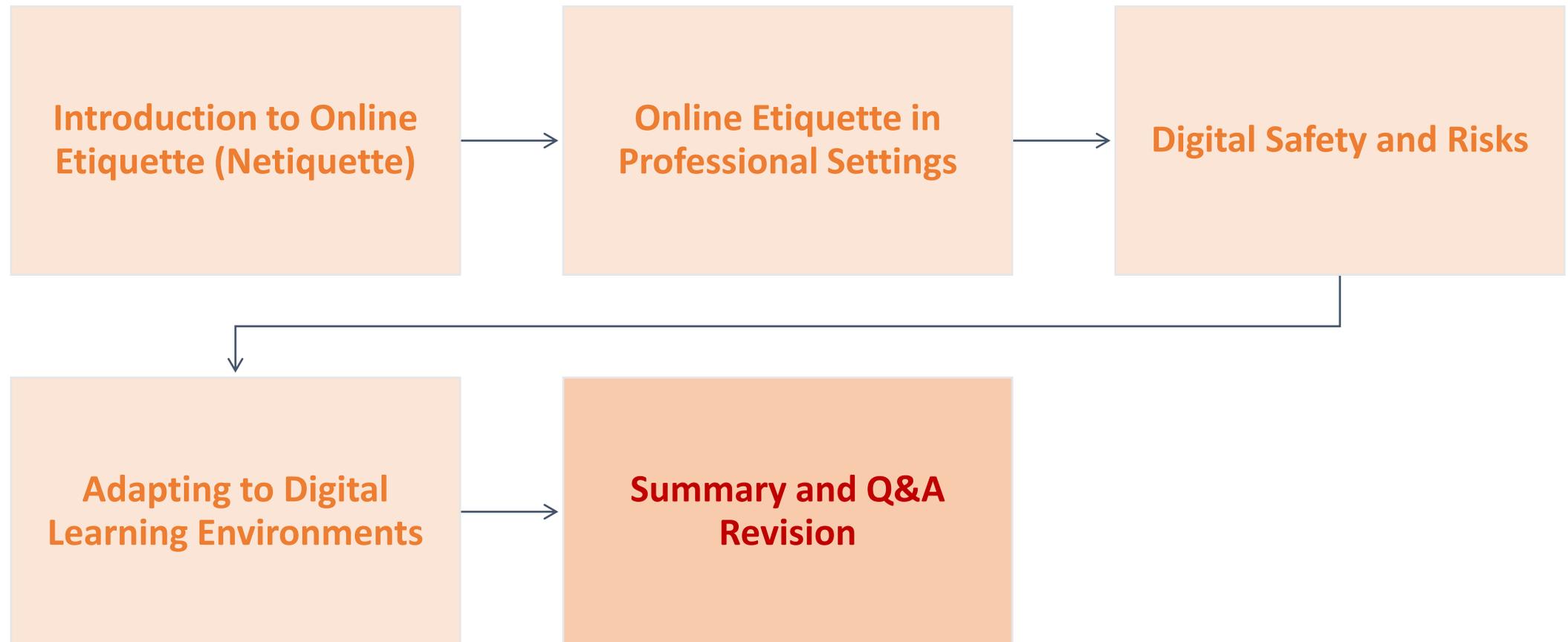
- **Automation:** Replacing manual tasks with automated digital processes, improving speed and reducing human error.
- **Data-Driven:** Leveraging digital data to make informed decisions, analyze trends, and predict future outcomes.
- **Connectivity:** Enhancing communication through networks and the internet, allowing real-time collaboration across geographic boundaries.
- **Innovation:** Digitalization enables the creation of new products, services, and even industries by utilizing technological advancements.

- **Examples:**

- **Healthcare:** Using digital patient records, telemedicine, and AI-driven diagnostics.
- **Retail:** E-commerce platforms transforming the way customers shop and interact with brands.
- **Education:** Online learning platforms providing access to education for students worldwide.

Topic 3. Engagement with Digital Technologies

Topic 3 Route Map



“The Internet is the first thing that humanity has built that humanity doesn’t understand, the largest experiment in anarchy that we have ever had.”

— Eric Schmidt, Former CEO of Google

Introduction to Online Etiquette (Netiquette)

Definition of Netiquette:

Netiquette: The expected set of rules and behaviors for **respectful communication** in the digital environment.

Why it's important: As digital communication grows, maintaining professional, respectful interactions is essential to building positive relationships and communities online.

Respectful Language and Tone:

- Always communicate in a way that respects others, avoiding offensive or inappropriate language.
- Remember that text lacks vocal tone—what might seem neutral to you could come off as rude to someone else.

Avoiding All-Caps (Shouting):

- ALL CAPS are perceived as shouting or aggression. Use standard capitalization to convey your point professionally.

Proper Acknowledgment of Others' Work:

- Always credit the original creator of content (ideas, quotes, resources) to avoid plagiarism and show respect for intellectual property.

Refraining from Personal Attacks or Flaming:

- Avoid hostile or aggressive comments, known as flaming. Engaging in personal attacks harms the online environment and disrupts productive communication.



Digital Etiquette Do's and Don'ts

- **Do:** Be polite, check your facts, and stay on topic.
- **Don't:** Post inflammatory content, spam, or monopolize discussions.
 - Use emojis and humor appropriately, remembering that tone can be misinterpreted.



Examples of Good and Bad Netiquette

Positive Examples (Good Netiquette)

1. Using Respectful Language

Example:

1. **“Thank you for your feedback. I will consider your suggestions for the next project!”**
2. **Explanation:** This response demonstrates politeness, open-mindedness, and encourages constructive feedback, fostering positive communication.

2. Acknowledging Others' Work

Example:

1. **“As mentioned by [Name] in their report, we should focus on...”**
2. **Explanation:** Giving credit where it's due shows respect for others' contributions and ensures intellectual property is recognized.

3. Using Proper Formatting (Avoiding ALL CAPS)

Example:

1. **“Please review the attached document and let me know your thoughts.”**
2. **Explanation:** Proper use of grammar, punctuation, and formatting (without caps lock) ensures the message is professional and clear.

Examples of Good and Bad Netiquette

Negative Examples (Poor Netiquette)

1. Using Aggressive Language

Example:

1. **“You’re WRONG! This makes NO sense, and you clearly didn’t think this through.”**
2. **Explanation:** This kind of response comes off as hostile and dismissive, which can escalate conflicts and damage relationships.

2. Failing to Credit Others

Example:

1. **“I think we should focus on... (idea taken from another person without acknowledgment).”**
2. **Explanation:** Failing to acknowledge someone else’s work or ideas may be perceived as plagiarism or disrespectful, especially in professional or academic settings.

3. Shouting (Using ALL CAPS)

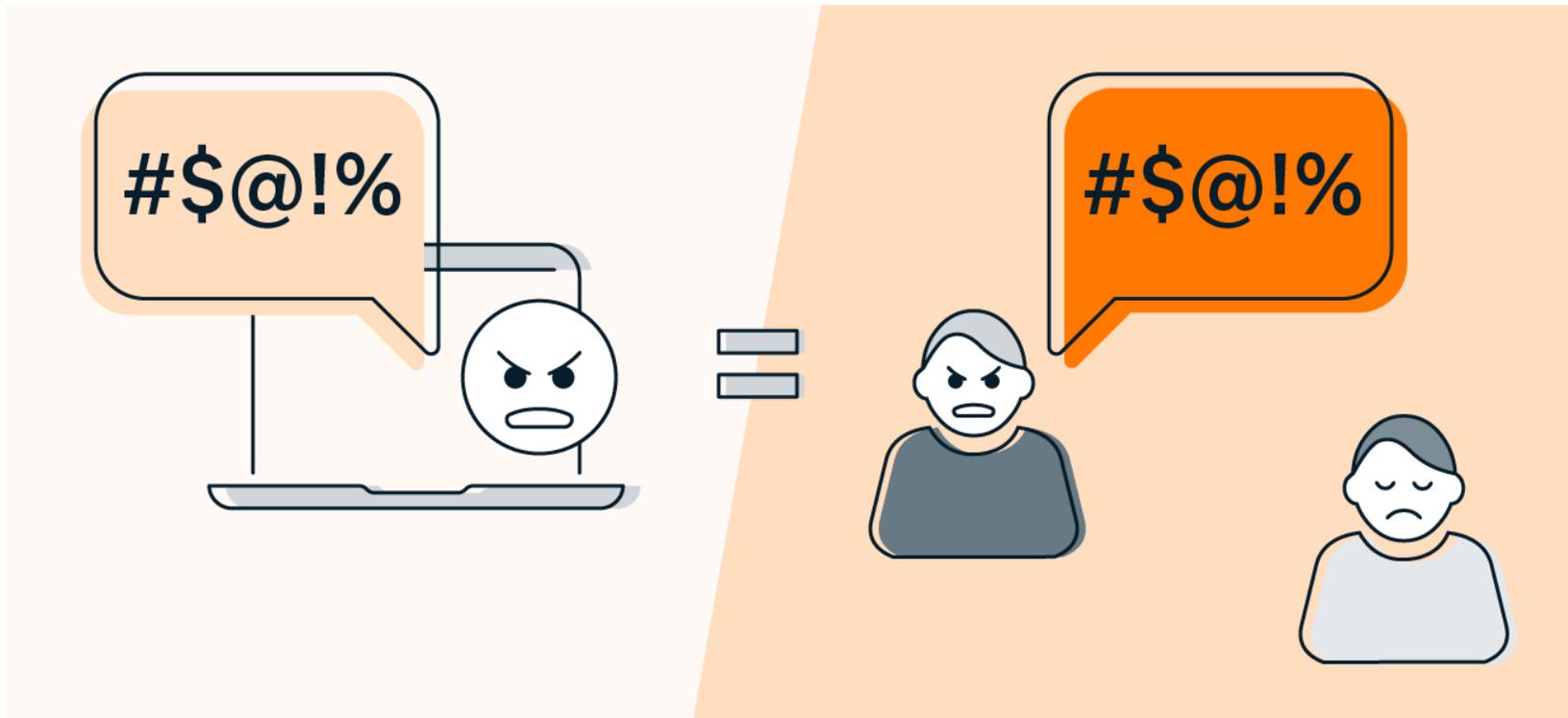
Example:

1. **“PLEASE SEND THE REPORT BY 5 PM TODAY!”**
2. **Explanation:** Using all caps in written communication is perceived as shouting and can come across as aggressive, leading to miscommunication or a negative tone.

Reflecting on Poor Netiquette Scenarios



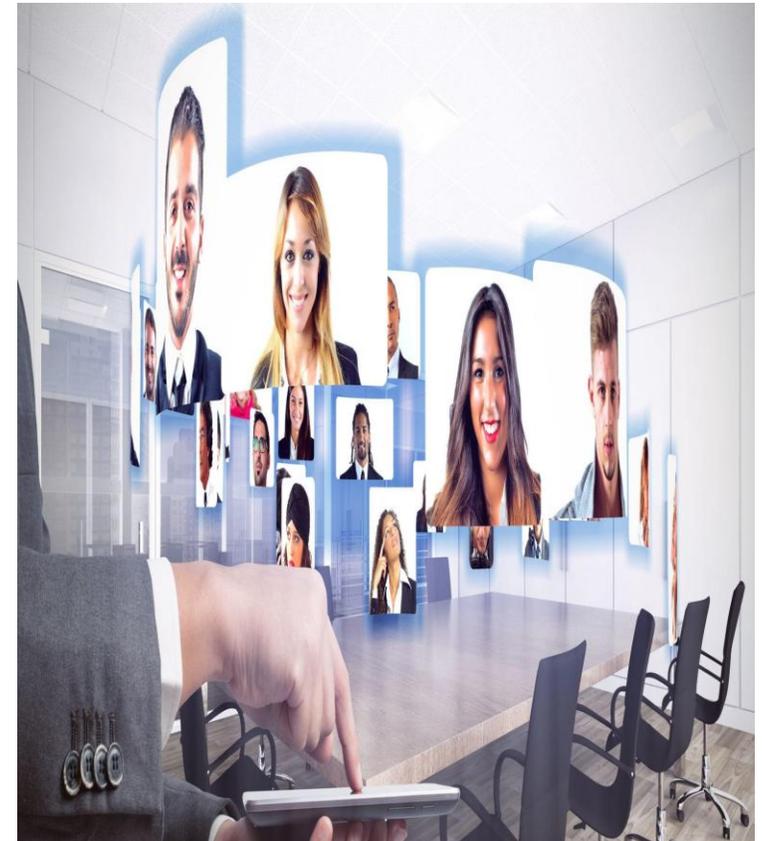
MT3.3_1



Topic 3.1 Online Etiquette in Professional Settings

What is Professionalism in Online Settings?

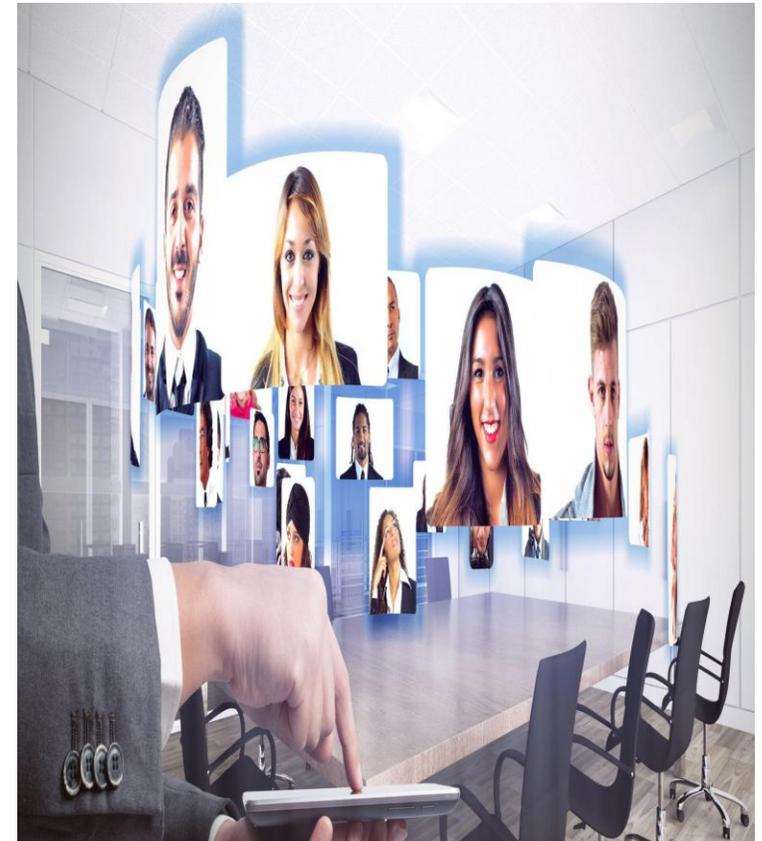
- **Professionalism:** The set of behaviors and communication techniques expected in a professional environment.
- **Online professionalism includes:**
 - Using formal language.
 - Following company policies.
 - Maintaining respectful and clear communication.



Topic 3.1 Online Etiquette in Professional Settings

Key Principles of Professional Online Communication

- **Use Proper Greetings and Closures:**
 - Start with formal greetings and end with a polite closure.
 - Example: "Dear Ms. Smith" or "Best regards, [Your Name]."
- **Be Concise and Clear:**
 - Communicate efficiently and avoid ambiguity.
 - Example: "Please complete the attached task by Friday."
- **Respect Time and Boundaries:**
 - Send emails or messages during appropriate working hours.
- **Handle Misunderstandings Professionally:**
 - Resolve conflicts with a calm and constructive approach.



Example of Poor Professional Communication

- "HEY TEAM! URGENT! NEED THIS NOW!"

- "Can you do this ASAP? I don't care how, just get it done."

Example of Proper Professional Communication

"Dear Team,

I hope this message finds you well. Could you please complete the attached task by the end of the day? Let me know if you need any assistance.

Best regards,
[Your Name]."

Improving Professional Emails



MT3.3_2



Challenges in Professional Digital Communication

Misinterpretation of Tone:

- **Challenge:** Text-based communication lacks vocal cues, making it difficult to convey tone. What seems like a neutral message may be interpreted as harsh or unfriendly.
- **Solution:** Use clear and concise language. Avoid sarcasm or overly informal expressions. Consider adding clarifying phrases, or where appropriate, emoticons to show intent.

Work-Life Boundaries:

- **Challenge:** With digital tools like emails and messaging apps, there's an expectation to always be available, blurring the lines between personal time and work.
- **Solution:** Set clear boundaries for when you are available. Communicate your working hours to your team and use tools like "Do Not Disturb" features to protect personal time.

Challenges in Professional Digital Communication

Lack of Visual or Vocal Cues:

- **Challenge:** In digital communication, body language, facial expressions, and tone of voice are absent, which can lead to misunderstandings or lack of clarity.
- **Solution:** Use video conferencing for more complex discussions, or use voice messages where appropriate. For written communication, be as specific as possible to avoid misinterpretation.

Overuse of Informal Language:

- **Challenge:** Digital communication, especially via instant messaging, can lead to over-casual communication that may not be appropriate for professional settings.
- **Solution:** Always assess the context and audience. Use professional language for clients or formal discussions. Tailor the level of formality depending on the setting.

Email Etiquette Tips



Topic 3.2: Digital Safety and Risks

What is Digital Safety?

Digital Safety refers to the practices that protect users from risks and harm when interacting in digital environments.

Key Areas of Focus:

- **Data privacy:** Safeguarding personal information from unauthorized access.
- **Cybersecurity:** Protecting systems and networks from attacks.
- **Digital identity protection:** Ensuring that personal online identities are not stolen or misused.



Topic 3.2: Digital Safety and Risks

Common Online Risks

- **Phishing:** Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.
- **Malware:** Malicious software designed to harm, exploit, or otherwise compromise digital devices.
- **Identity Theft:** The fraudulent acquisition and use of a person's private identifying information for financial gain.
- **Data Breaches:** Unauthorized access to personal or sensitive information that can result in misuse.



Protecting Digital Identity

Strong Passwords: Using complex, unique passwords for different platforms.

Two-Factor Authentication: Adding an extra layer of security by requiring a second form of identification.

Secure Browsing: Ensuring websites are secure before entering personal information (HTTPS).

Avoid Sharing Personal Information: Limiting the sharing of personal details on social media or unsecured websites.



Digital Threats and How to Deal with Them

Phishing Attacks

- **Definition:** Fraudulent attempts to obtain sensitive information (e.g., passwords, credit card numbers) by pretending to be a trustworthy entity via email, phone, or text.
- **How to Deal with Phishing:**
 - **Do not click on links** in unsolicited emails.
 - **Verify the sender's identity** by contacting the company directly through official communication channels.
 - **Report phishing attempts** to your email provider or IT department.

Malware (Viruses, Trojans, Ransomware)

- **Definition:** Malicious software designed to harm or exploit devices, networks, or data.
- **How to Deal with Malware:**
 - Install and regularly update **antivirus and anti-malware software**.
 - **Avoid downloading attachments** from unknown sources.
 - **Backup important data** regularly in case of ransomware or other data-compromising attacks.

Digital Threats and How to Deal with Them

3. Identity Theft

- **Definition:** The fraudulent use of another person's identity, typically for financial gain.
- **How to Deal with Identity Theft:**
 - Use **strong, unique passwords** and enable **two-factor authentication**.
 - Be cautious about sharing personal information online.
 - Monitor your **financial accounts** regularly for suspicious activity.

Digital Threats and How to Deal with Them

4. Data Breaches

- **Definition:** Unauthorized access to personal or sensitive information, often through hacking.
- **How to Deal with Data Breaches:**
 - **Change passwords** immediately after a breach is discovered.
 - **Monitor accounts** for any signs of misuse or fraud.
 - **Enable alerts** for unusual account activity and use **encryption** for sensitive data.

5. Social Engineering Attacks

- **Definition:** Manipulating people into divulging confidential information through deception (e.g., pretending to be a colleague).
- **How to Deal with Social Engineering:**
 - **Be cautious of unsolicited requests** for sensitive information, even from familiar individuals.
 - **Verify identities** through secondary communication channels (e.g., calling the person directly).
 - **Educate employees** about recognizing social engineering techniques.

Responding to a Digital Threat



MT3.3_4



Digital Identity Theft



Topic 3.3: Adapting to Digital Learning

- **What is Digital Learning?**
- Digital learning is the process of acquiring skills or knowledge using digital tools and platforms.
- **Examples:**
 - **Workplace Learning:** Using platforms like **LinkedIn Learning** or **Coursera** for job-related skills.
 - **Personal Development:** Apps like **Duolingo** for language learning or **Headspace** for well-being.
 - **Daily Problem-Solving:** **YouTube tutorials** or online forums to learn new skills or solve issues.



Topic 3.3: Adapting to Digital Learning

Why is Digital Learning Important?

1. **Flexibility:** Learn at your own pace, anytime, anywhere.
2. **Accessibility:** Digital tools make learning available to everyone, globally.
3. **Cost-Effective:** Many platforms offer free or affordable learning options.
4. **Self-Directed:** Tailor your learning to your needs and goals.
5. **Learning on the Go:** Access content on various devices, making it easy to fit into daily routines.
6. **Stay Competitive:** Adapt to technological advances and stay relevant in your field.

Key Takeaway:

- Digital learning is embedded in daily life—whether for career development, personal growth, or practical skills. Adapting to it ensures continued growth in an information-rich world.



Common Challenges in Digital Learning for Life

Information Overload:

- There's an overwhelming amount of online resources, making it difficult to know where to focus attention.

Digital Fatigue:

- Over-reliance on screens can lead to burnout and lack of motivation.

Self-Discipline:

- Digital learning requires high levels of self-motivation and time management, especially in non-formal settings (e.g., work projects or personal goals).

Technological Gaps:

- Difficulty in using certain platforms or lack of digital literacy.



Strategies for Effective Digital Learning in Work

Set Clear Goals:

- Define what you want to learn and create measurable objectives (e.g., learning a new skill for a work project or improving productivity habits).

Use the Right Tools:

- Choose the most relevant tools or platforms for your learning goals.

Examples:

- For project management, use [Trello](#) or [Monday.com](#).
- For personal development, use apps like [Headspace](#) or [Coursera](#).

Time Management:

- Block time in your schedule for self-learning and practice.

Seek Community:

- Join online forums, webinars, or peer groups to share your learning journey and get support.



Developing a Personal Digital Learning Plan



MT3.3_6



Digital Tools for Professional and Life Learning

For Work:

- **Project Management Tools:** Trello, Monday.com, Asana.
- **Video Conferencing:** Zoom, Microsoft Teams.
- **Training and Development:** LinkedIn Learning, Coursera.



For Personal Growth:

- **Personal Finance:** Mint, You Need A Budget (YNAB).
- **Health and Well-being:** Headspace, MyFitnessPal.
- **Skill Development:** Duolingo (language learning), Skillshare (creative skills).



For Life Management:

- **Time Management:** Google Calendar, Todoist.
- **Organizational Tools:** Evernote, Notion.



Adapting Digital Strategies to Workplace Scenarios



MT3.3_7



Case Study – Digital Upskilling for a Job

Scenario:

- A professional has been offered a promotion but needs to gain advanced project management skills within 3 months. They decide to use digital platforms, such as **LinkedIn Learning** for training and **Monday.com** for hands-on practice in project management.

Key Learning Points:

- **Balancing Learning with a Full-Time Job:**
- Learn how to manage time effectively by setting aside dedicated hours for upskilling each week.
- Use productivity tools (e.g., Google Calendar, Todoist) to prioritize learning without impacting job performance.

Using Structured Learning Platforms:

- Take advantage of well-organized online courses that break complex topics into manageable lessons.
- Platforms like LinkedIn Learning offer certifications and progress tracking, making learning more structured and measurable.

Overcoming Challenges:

- **Time Management:** Develop a schedule that balances work responsibilities and learning. Set realistic daily or weekly goals to track progress.
- **Lack of Motivation:** Stay motivated by rewarding progress, joining peer learning groups, or finding an accountability partner to stay on track.

Outcome:

- By the end of 3 months, the professional successfully gains the necessary skills, completes certifications, and feels confident in handling the new project management responsibilities. They demonstrate how digital upskilling can fast-track career growth while maintaining full-time job commitments.

Revision-Summary

Recap of Key Points

Introduction to Online Etiquette (Netiquette):

- **Defining Online Etiquette:** Digital communication requires using respectful language, acknowledging others, and avoiding behaviors like using all caps (shouting) or personal attacks.
- **Key Principles:** Maintain professionalism, give proper credit, and use tone appropriately.

Online Etiquette in Professional Settings:

- **Maintaining Professionalism:** Ensure clarity in emails and messages, use formal greetings and signatures, and avoid emotional or inappropriate language.
- **Group Exercise:** Participants learned how to improve communication by identifying and correcting poorly written professional emails.

Revision-Summary

Digital Safety and Risks:

- **Identifying Online Threats:** Key digital threats include phishing, malware, and identity theft. Awareness of these risks is crucial for protecting personal and organizational data.
- **Protecting Digital Identity:** Best practices include using strong passwords, enabling two-factor authentication, and being cautious with public Wi-Fi.

Adapting to Digital Learning Environments:

- **Personal Learning Strategies:** Participants created their own digital learning strategies, selecting tools like LinkedIn Learning or Coursera for skill development.
- **Practical Application:** Groups worked through real-life scenarios, identifying challenges and solutions for adapting to new digital tools in workplace environments.



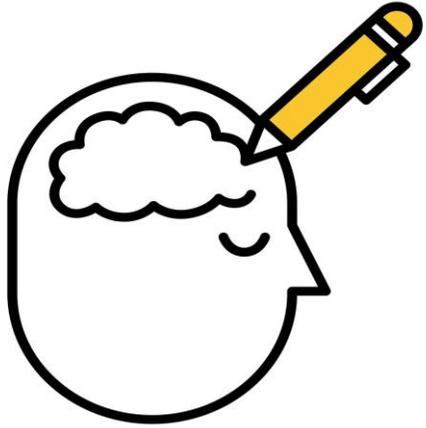
Revision-Summary and Q&A

✓ Digital Safety & Etiquette:

- ✓ Netiquette: Respectful and professional behavior in digital communications.
- ✓ Digital Risks: Protecting online identity, recognizing threats, and managing digital safety.
- ✓ Adapting to Digital Learning Environments: Strategies for efficiently learning and applying new digital tools in the workplace.



Do you have any questions?



What will you keep from
today's training?

Training Evaluation



List of References

Engagement with Digital Technologies

11. **Turkle, S.** (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.
Available at: [Amazon Link](#)
12. **Baym, N. K.** (2015). *Personal Connections in the Digital Age*. Polity Press.
Available at: [Amazon Link](#)
13. **Cialdini, R. B.** (2006). *Influence: The Psychology of Persuasion*. Harper Business.
Available at: [Amazon Link](#)
14. **Howard, P. N., & Hussain, M. M.** (2013). *Democracy's Fourth Wave? Digital Media and the Arab Spring*. Oxford University Press.
Available at: Oxford University Press
15. **Rheingold, H.** (2012). *Net Smart: How to Thrive Online*. MIT Press.
Available at: MIT Press

Digital Safety and GDPR Compliance

16. **Schneier, B.** (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
Available at: [Amazon Link](#)
17. **GDPR.eu** (2020). *General Data Protection Regulation: A Detailed Overview*.
Available at: [GDPR.eu](#)
18. **Cavoukian, A.** (2009). *Privacy by Design: The 7 Foundational Principles*.
Available at: Information and Privacy Commissioner of Ontario
19. **Singer, P. W., & Friedman, A.** (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
Available at: Oxford University Press
20. **Westby, J.** (2017). *Cybersecurity & Privacy Best Practices for Small to Medium Enterprises*. American Bar Association.
Available at: [Amazon Link](#)

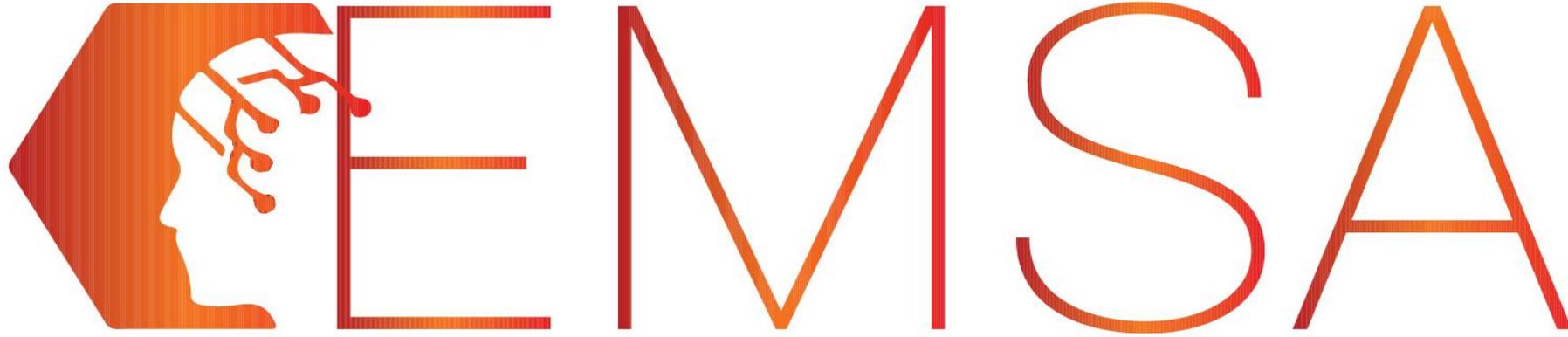
List of Suggested Resources for Self-Directed Learning

3. Engagement with Digital Technologies

- **"Digital Minimalism: Choosing a Focused Life in a Noisy World"** – Cal Newport
Available at: [Amazon Link](#)
- **"Netiquette"** – Virginia Shea
Available at: [Amazon Link](#)
- **Dropbox: Collaborating with Dropbox for Teams**
Available at: Dropbox
- **TED Talks: The Dark Side of Technology**
Available at: [TED.com](#)
- **LinkedIn Learning: Developing Digital Competence**
Available at: [LinkedIn Learning](#)

4. Digital Safety and GDPR

- **"Cybersecurity and Cyberwar: What Everyone Needs to Know"** – P.W. Singer
Available at: [Amazon Link](#)
- **"The GDPR Handbook"** – E. Corynne McSherry
Available at: [Amazon Link](#)
- **GDPR.eu: GDPR Training Materials**
Available at: [GDPR.eu](#)
- **"Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World"** – Bruce Schneier
Available at: [Amazon Link](#)
- **Cyber Awareness Learning Hub**
Available at: [Cyber Awareness](#)



Entrepreneurial Mindset and Key Skills for All

Thank you!



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.