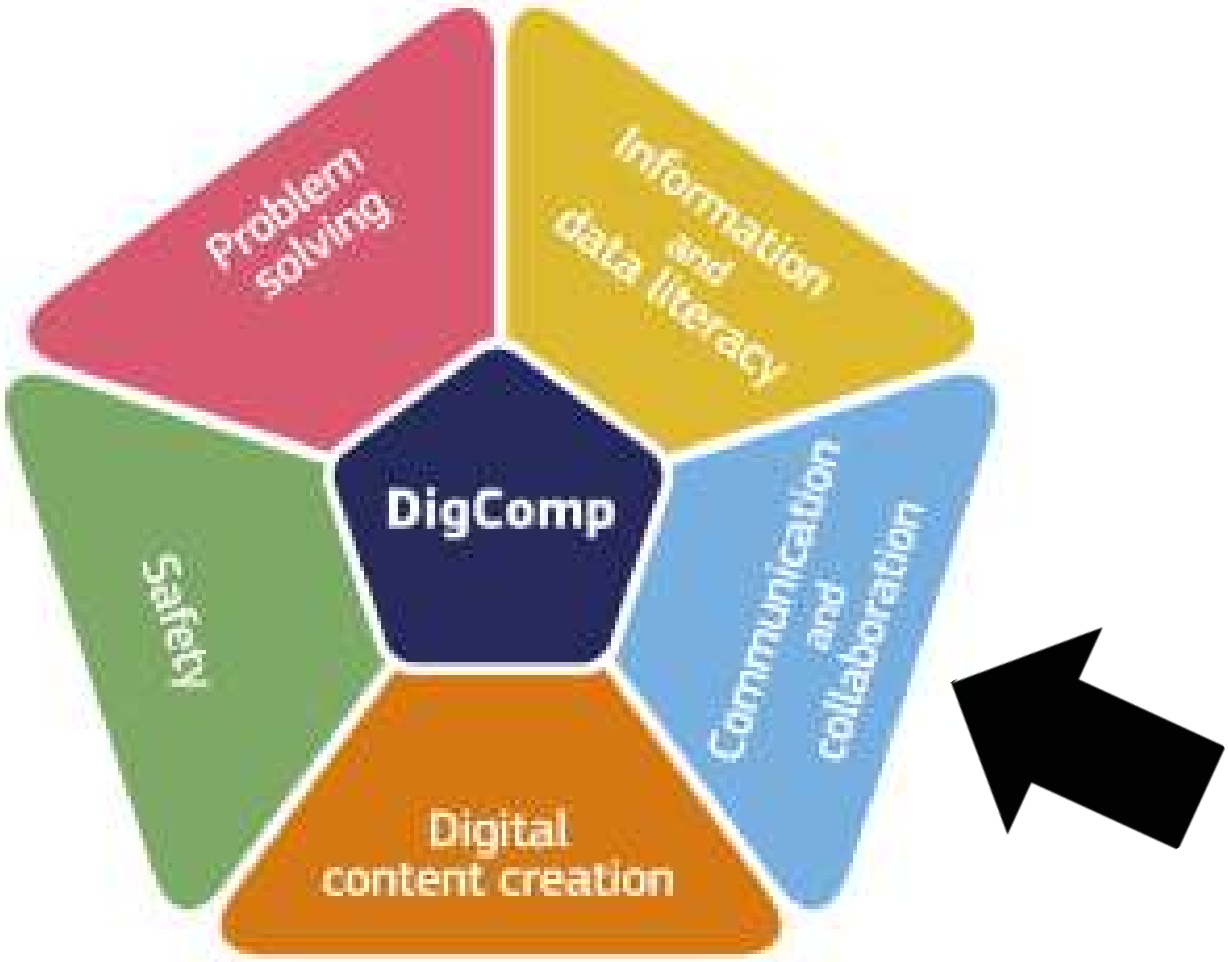
MICROCREDENTIALS FOR COMMUNICATION AND COLLABORATION
Competence 2.6: MANAGING DIGITAL IDENTITY

DSW
DIGITAL SKILLS WALLET

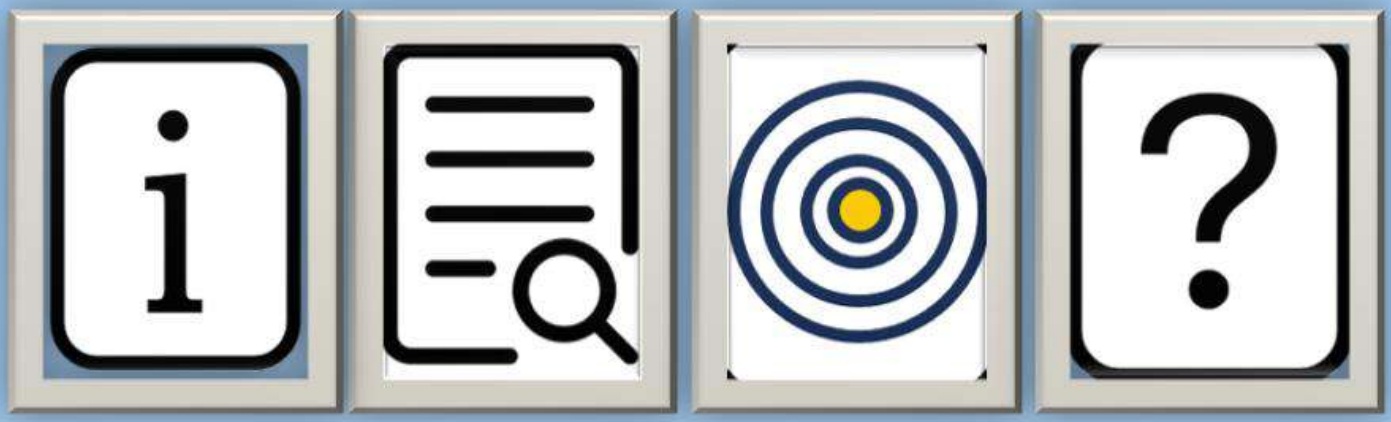
Co-funded by
the European Union

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.


Problem solving
Information and data literacy
DigComp
Communication and collaboration
Safety
Digital content creation

Contents

FOUNDATION LEVEL
(Level 1 and Level 2)



Defining Digital Identity (MC 2.6.A.1)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Defining Digital Identity **Code: MC 2.6.A.1**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	FOUNDATION
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 1 LOs 1.1, 1.2 and 1.3)

- Define digital identity.
- Describe the key characteristics of digital identity.
- Provide examples of different digital identities.

Description

The achievement of the micro credential **"Digital Identity"** proves that the learner is able to understand that digital identity refers to the electronic representation of an individual or an organization, as well as the ability of the learner to recognise that a digital identity refers to a set of data identifying a user by means of tracing their digital activities, actions and contributions on the internet.

Additionally, this micro-credential demonstrates the ability of the learner to describe the key characteristics of digital identity such as identification information, authentication credentials, authorization data, attributes and characteristics, digital certificates and biometric data.

Finally, this micro-credential confirms the ability of the learner to recognise that digital identities can take various forms across online platforms and services, for example a digital identity can be an email account, a social media profile, an online banking credential, an e-government ID, a gaming profile, a smart home device credential, a subscription services account and much more.

Questions

1. What is a digital identity?
2. What are the key characteristics of a digital identity?
3. What is biometric data?
4. What are some examples of different digital identities?
5. Is a subscription services account a form of digital identity? Explain why.
6. Is a gaming profile a form of digital identity? Explain why.

Digital Identity: Benefits and Risks (MC 2.6.A.2)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Digital Identity: Benefits and Risks Code: MC 2.6.A.2
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: 101087628
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	FOUNDATION
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 2 LOs 2.4 and 2.5)

- Describe the benefits of digital identify
- Describe the risks of digital identity

Description

"Digital Identity: Benefits and Risks" micro-credential demonstrates the ability of the learners to describe the benefits of digital identity such as security and authentication, convenience, privacy protection, efficiency and accessibility and technological innovation.

Additionally, this micro-credential also demonstrates the ability of the learners to describe the risks of digital identity such as security concerns, privacy issues, lack of standardization, regulatory and legal challenges and technological innovation.

Questions

1. What are the benefits of digital identity?
2. How does digital identity provide convenience for users?
3. What are the risks of digital identity?
4. Why is lack of standardization a risk of digital identity?
5. What are some security concerns related to a digital identity?
6. Technological innovation is considered both a benefit and a risk of digital identity. Explain the reasons why.

Online Reputation (MC 2.6.A.3)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Online Reputation **Code: MC 2.6.A.3**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	FOUNDATION
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 1 LOs 1.6 and Level 2 LOs 2.7 and 2.8)

- Identify simple ways to protect one's own reputation online.
- Request guidance when needed, to protect one's own reputation online.
- Emphasize on the importance of protecting one's own reputation online.

Description

"Online Reputation" micro-credential demonstrates the broad knowledge of the learners to name the simple ways an individual can follow to protect his/her own reputation online, such as to review and update privacy settings on social media platforms, to establish professional profiles on platforms that are not associated with their personal accounts on other social media platforms, to avoid sharing personal details online, to maintain strong and unique passwords and to enable two-factor authentication whenever possible, to be cautious about the content they post on social media platforms and to be cautious about the groups and forums they join online.

Additionally, this micro-credential demonstrates the ability of the learners to request guidance on ways to protect one's own reputation online such as to maintain strong and unique passwords and to enable two-factor authentication whenever possible, to be cautious about the content they post on social media platforms and to be cautious about the groups and forums they join online.

Finally, the achievement of this micro-credential demonstrates the ability of the learners to sensitize on the importance of protecting one's own reputation online. The learner should be able to recognise that protecting your reputation online its crucial for your professional opportunities, your personal branding, and safeguarding your personal information. As well as the ability of the learners to recognise that, businesses should also protect their own reputation online, because their online reputation impacts customer trust and loyalty, for example positive reviews, testimonials and a strong digital presence can lead to success and growth of a business.

Questions

1. What do we mean by the term online reputation?
2. Can you name simple ways in which you can protect your online reputation?
3. How does avoiding sharing personal details about myself, help to protect my online reputation?
4. What do we mean when we talk about personal branding?
5. Protecting your online reputation refers to both individuals and businesses. Explain why.
6. Explain the importance of protecting your online reputation.

Producing Data Online (MC 2.6.A.4)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Producing Data Online **Code: MC 2.6.A.4**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	2-4 Hours
Level of the learning experience leading to the micro-credential	FOUNDATION
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 1 LOs 1.9)

- Recognise simple data you produce through digital tools, environments and services.

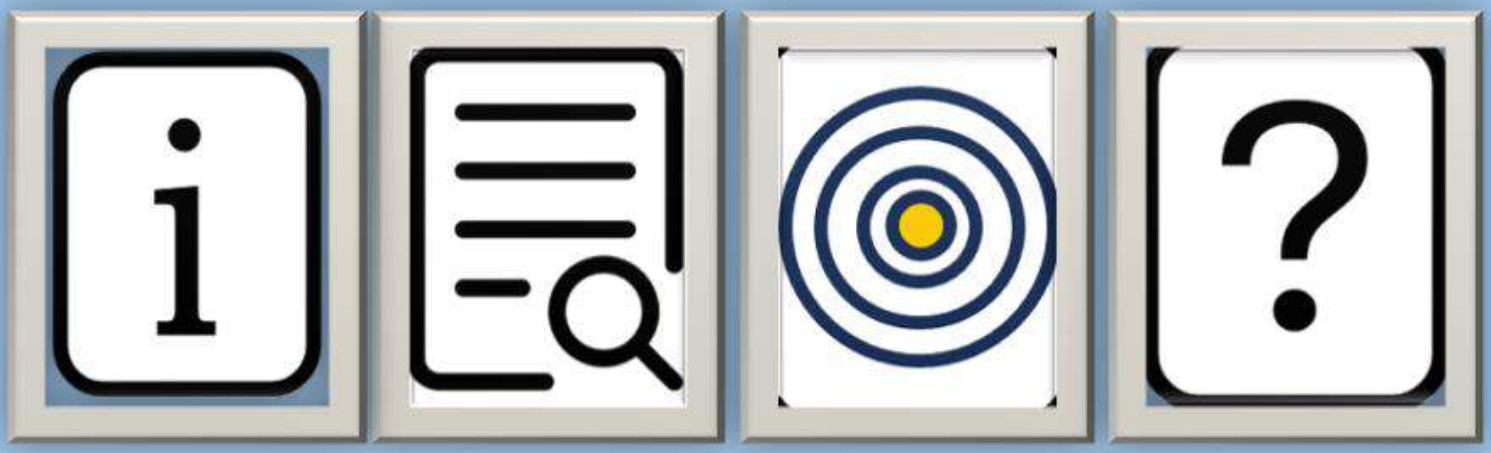
Description

"Producing Data Online" micro-credential demonstrates the ability of the learners to recognise simple data they produce through digital tools, environments and services such as personal information, online activity data , communication data, location data , transaction and financial data (purchase history, financial transactions, payment information), preference and settings , authentication data, device information, biometric data , search queries and cookies and tracking data.

Questions

1. What types of data does one produce online?
2. What is browsing history?
3. What types of data do you produce when you search online?
4. What are some examples of personal information data?
5. What are some examples of online activity data?
6. What are some examples of communication data?
7. What are some examples of biometric data?
8. What are some examples of authentication data?

INTERMEDIATE LEVEL
(Level 3 and Level 4)



Routine Digital Identities (MC 2.6.B.1)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Routine Digital Identities **Code: MC 2.6.B.1**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.10 and 3.11):

- Discriminate a range of well-defined and routine digital identities.
- Differentiate between a personal social media identity and a professional identity.

Description

The achievement of the micro credential **"Routine Digital Identities"** demonstrates the ability of the learners to discriminate a range of well-defined and routine digital identities such as personal or professional social media identity, gaming identity, ecommerce user identity, educational platform identity, job search platform identity, subscription service identity etc.

Additionally, this micro-credential demonstrates the ability of the learners to recognise that a personal social media identity is primarily used for socializing, connecting with friends and family and sharing personal experiences. The learner should also be able to recognise the content being shared on a personal social media identity such as personal photos and videos, casual updates, information about hobbies and interests and the interaction style being informal.

Finally, this micro-credential demonstrates the ability of the learners to recognise that a professional identity is primarily used for networking, career development and showcasing skills and achievements related to a specific professional field. The learner should also be able to recognise the content being shared on a professional identity such as details about work experience, professional achievements, skills, education and endorsements related to a specific career and the interaction style being formal and focuses on professional topics.

Questions

1. What are the types of routine digital identity?
2. What is a personal social media identity?
3. What is a professional social media identity?
4. What is the main purpose of having a personal social media identity? Can you describe some of its uses?
5. What is the main purpose of having a professional social media identity? Can you describe some of its uses?

Building a positive online identity (MC 2.6.B.2)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Building a positive online identity **Code: MC 2.6.B.2**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.12 and 3.13):

- Recognize information and communication practices that help an individual to build a positive online identity.
- Recognize information and communication practices that might cause a negative online identity.

Description

"Building a positive online identity" micro-credential demonstrates the ability of the learners to recognise information and communication practices that can help an individual to build a positive online identity such as, to create and post content that reflects your values and interests positively, selective sharing, promote constructive dialogue and avoid getting involved in negative interactions, maintain a professional demeanour in professional platforms like LinkedIn and stay informed about digital trends and best practices.

Additionally, this micro-credential demonstrates the ability of the learners to recognise information and communication practises that might cause a negative online identity such as, to use offensive or inflammatory language when engaging in online interactions, to engage in online harassment, to share content that spreads misinformation and rumours, to behave inappropriate or unprofessional in professional platforms like LinkedIn and to have to ignore digital trends and best practices.

Questions

1. What do we mean by positive online identity?
2. What do we mean by negative online identity?
3. Can you name some information and communication practices that help to build a positive online identity?
4. Can you name some information and communication practices that might cause a negative online identity?
5. What is your position related to constructive dialogue and spreading misinformation and rumors as far as the branding of online identity is concerned.
6. Why is promoting constructive dialogue a practice that helps to build a positive online identity?
7. Why is spreading misinformation and rumours a practise that might cause a negative online identity?

Understanding and manipulating the data you produce online (MC 2.6.B.3)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Understanding and manipulating the data you produce online **Code: MC 2.6.B.3**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.14 and Level 4 LOs 4.15, 4.16):

- Describe what kind of data one produces through digital tools, environment and services.
- Manipulate the data one produces through digital tools, environment and services.
- Sensitize on which data one should produce on digital identity.

Description

"Understanding and manipulating the data you produce online" micro-credential demonstrates the broad knowledge of the learners on the data they produce online, such as data related to their personal information, digital signatures, contact information, biometrics, browser history and cookies, transaction history, preferences and interests, communication metadata, authentication and authorization data and records of consent given.

Additionally, this micro-credential demonstrates the ability of the learners to manipulate the data one produces through digital tools, environment and services. For example regarding their personal information, the learner should be able to recognise when it is necessary to add information such as their home address or telephone number.

Finally, this micro-credential demonstrates the ability of the learner to sensitize on which data one should produce on digital identity, for example data related to their personal information should be avoided unless absolutely necessary (for example, home address, phone numbers), data related to financial information should be shared with cautious (for example, bank account numbers, credit card details, card PINs), data related to location should also be avoided unless necessary in order to protects one's own physical security and privacy.

Questions

1. Name some type of data you produce online.
2. Can you manipulate data related to personal information? Explain how.
3. Can you manipulate data related to contact information? Explain how.
4. Can you manipulate data related to location? Explain how.
5. Why is it important to manipulate data you produce online?

Creating and managing profiles for personal or professional purposes (MC 2.6.B.4)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Creating and managing profiles for personal or professional purposes **Code: MC 2.6.B.4**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.17 and 3.18):

- Creates profiles in digital environments for personal or professional purposes.
- Manages profiles in digital environments for personal or professional purposes.

Description

"Creating and managing profiles for personal or professional purposes" micro-credential demonstrates the ability of the learners to create a profile through filling out profile details comprehensively, including a bio, contact information, education, work experience, and any other relevant details.

Additionally, this micro-credential demonstrates the ability of the learners to manage their profile in digital environment for personal or professional purposes through regular updates, setting privacy settings, showcasing skills, seeking endorsement, review and cleanup digital profiles etc

Questions

1. What information will you include in your digital profile
2. Describe that activities you will undertake to ensure that your profile remains updated and attractive
3. How can you clean up your digital profile?
4. Differentiate between a digital profile to be used for personal and professional use.

Strategies to protect one's reputation online (MC 2.6.B.5)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Strategies to protects one's reputation online **Code: MC 2.6. B.5**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.19)

- Present different strategies to protect one's reputation online.

Description

"Strategies to protects one's reputation online" micro-credential demonstrates the ability of the learner to present different strategies to protect one's reputation online such as to monitor their online presence by searching on a regular basis their name, to set up the alerts on their browser, to adjust privacy settings on social media platforms, to be cautious about the information being shared online, to use strong passwords and to be cautious about the content you post online.

Questions

1. Name some strategies to protect one's reputation online.
2. How can you monitor your online presence? Give some examples.
3. Why is adjusting privacy setting on social media platforms a strategy to protect one's reputation online?
4. Describe information that one can share online and information that one should not share online.
5. Can you name some privacy settings that can be adjusted?

Metadata in shared pictures (MC 2.6.B.6)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Metadata in shared pictures **Code: MC 2.6. B.6**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 3 LOs 3.20 and Level 4 LOs 4.21)

- Describe what type of metadata is included in pictures being shared.
- Describe the ways you can modify the metadata of a picture being shared.

Description

"Metadata in shared pictures" micro-credential demonstrates the ability of the learners to describe what type of metadata is included in pictures being shared, such as EXIF data (Exchangeable Image File Format), IPTC data (International Press Telecommunications Council), XMP data (Extensible metadata platform), file information data, as well as the ability of the learners to recognise the metadata that can be modified.

Finally, this micro-credential demonstrates the ability of the learners to describe the ways you can modify the metadata of a picture being shared, such as using online tools and websites (Metapicz), using specialised software (Exif Pilot, Adobe Lightroom), on Windows and MacOS and using image editing software (Photoshop, GIMP).

Questions

1. What type of metadata are included in pictures being shared?
2. What does EXIF data include?
3. What does IPTC data include?
4. What type of metadata can be modifies?
5. Which digital tools will you use to modify these metadata?
6. Describe the process you will take in order to modify metadata using a digital tool.
7. Describe the process you will take in order to modify metadata on Windows.

Managing multiple digital identities: Benefits and Risks (MC 2.6.B.7)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Managing multiple digital identities: Benefits and Risks **Code: MC 2.6. B.7**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	4-6 Hours
Level of the learning experience leading to the micro-credential	INTERMEDIATE
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 4 LOs 4.22 and 4.23)

- Identify the benefits when managing one or multiple digital identities across digital systems, applications and services.
- Identify the risks when managing one or multiple digital identities across digital systems, applications and services.

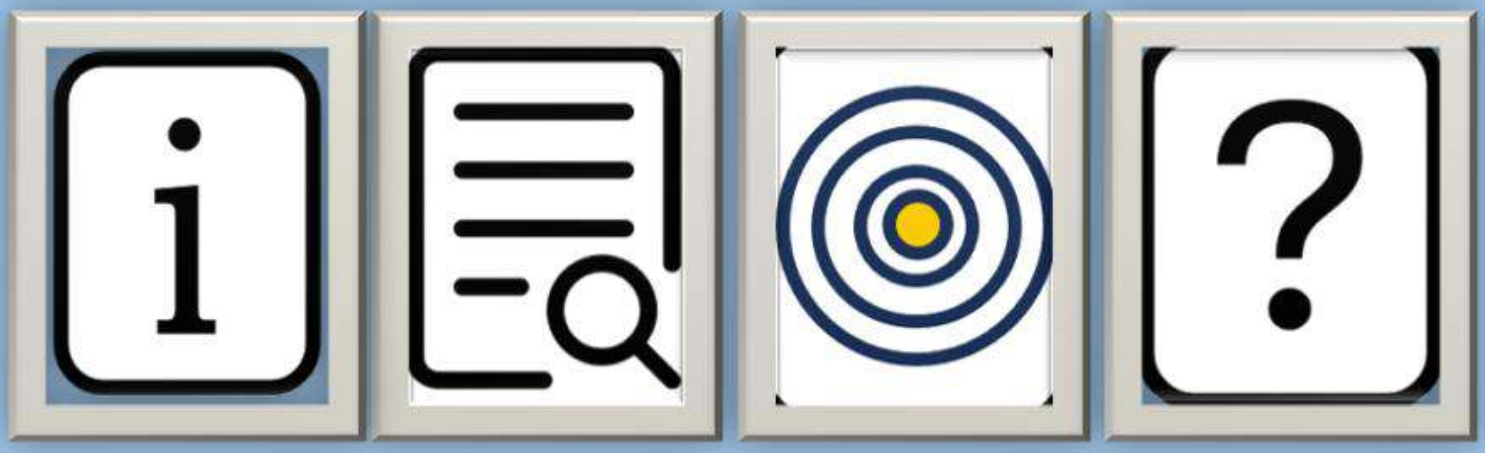
Description

"Managing multiple digital identities: Benefits and Risks" micro-credential demonstrates the ability of the learners to identify the benefits when managing one or multiple digital identities such as access and convenience, personalization, efficient authentication, customized services and professional networking, as well as the ability of the learners to identify the risks when managing one or multiple digital identities such as security threats, privacy concerns, identity fragmentation, data breaches, reputation damage, authentication challenges and lack of control.

Questions

1. What are the benefits of managing one or multiple digital identities across digital systems, applications and services?
2. What are the risks of managing one or multiple digital identities across digital systems, applications and services.?
3. Why is access and convenience a benefit when managing one or multiple digital identities across digital systems, applications and services?
4. Why is lack of control a risk when managing one or multiple digital identities across digital systems, applications and services?
5. Why is reputation damage a risk when managing one or multiple digital identities across digital systems, applications and services?

ADVNACED LEVEL
(Level 5 and Level 6)



Consistent digital identity (MC 2.6.C.1)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Consistent digital identity **Code: MC 2.6.C.1**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	ADVANCED
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 6 LOs 6.24, 6.25 and 6.26):

- Explain the phrase "*consistent digital identity in all social media*".
- Justify why one should have consistent digital identity in all social media.
- Create a consistent digital identify in all social media.

Description

"Consistent digital identity" proves the ability of the learners to explain the phrase "consistent digital identity in all social media" as referring to maintaining a uniform online presence across different platforms. This includes using the same or similar usernames, profile pictures, and a standardized personal or professional branding strategy, as well as the ability of the learners to justify why one should have a consistent digital identity in all social media in order to create a recognizable personal brand that represents the person on different online channels.

Additionally, this micro-credential demonstrates the ability of the learners to create a consistent digital identity.

Questions

1. What does consistent digital identity in all social media mean?
2. What are the main characteristics of a consistent digital identity?
3. What are the main reasons why one should have a consistent digital identity?
4. Describe the strategies through which one can achieve consistency in their digital identity.
5. What branding elements can one use to achieve consistency in their digital identity.

Modifying metadata (MC 2.6.C.2)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Modifying metadata **Code: MC 2.6.C.2**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	4-6 Hours
Level of the learning experience leading to the micro-credential	ADVANCED
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 6 LOs 6.27 and 6.28):

- Select a picture you would like to upload on a specific social media platform and modify its metadata using a specific software.
- Emphasize the importance of modifying metadata in order to protect one's privacy.

Description

"Modifying metadata" micro-credential demonstrates the ability of the learners select a picture they would like to upload on a specific social media platform and to modify its metadata using a specific digital tool or software. This micro-credential also demonstrates the ability of the learners to emphasize on the importance of modifying metadata in order to protect one's privacy, for example by modifying or removing information regarding the location, time and date of where and when the photo was taken, the individual can prevent to disclose their whereabouts and information about their activities.

Questions

1. Name two software that can be used to modify a picture's metadata.
2. Select one software and describe the process of modifying a picture's metadata.
3. What type of metadata can be modified?
4. How can an individual maintain their anonymity by modifying metadata?
5. How can an individual minimize the risk of being tracked by modifying metadata?
6. Explain the importance of modifying a picture's metadata.

Managing multiple digital identities (MC 2.6.C.3)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Managing multiple digital identities **Code: MC 2.6.C.3**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	4-6 Hours
Level of the learning experience leading to the micro-credential	ADVANCED
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 5 LOs 5.29 and 5.30):

- Manage one or multiple digital identities across digital systems
- Consider the benefits and risks when managing one or multiple digital identities across digital systems, apps and services

Description

"Managing multiple digital identities" micro-credential demonstrates the ability of the learners to manage one or multiple digital identities across digital systems. This micro-credential demonstrates also the ability of the learners to list the benefits of managing one or multiple digital identities across digital systems, apps and service such as establishing a personal branding and a professional reputation, maintaining network opportunities, improving efficient communication, adapting to change more easily, increasing visibility and more.

Questions

1. What does manage one or multiple digital identities across digital systems means?
2. Give us an example of managing one or multiple digital identities across digital systems.
3. Which digital systems, apps and services will you use in order to manage multiple digital identities?
4. What are the benefits of managing one or multiple digital identities?
5. How can you achieve efficient communication when managing multiple digital identities?

Control, manage or delete data collected by online systems (MC 2.6.C.4)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Control, manage or delete data collected by online systems **Code: MC 2.6.C.4**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	ADVANCED
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 6 LOs 6.31):

- Uses strategies in order to control, manage or delete data that is collected by online systems.

Description

"Control, manage or delete data collected by online systems" micro-credential demonstrates the ability of the learners to use effectively strategies in order to control, manage or delete data that is collected by online systems such as regularly clear cookies and cache, exercise right to request the deletion of one's data from online platforms, use strong passwords and two factor authentication, regularly audit connected apps and educate oneself.

Questions

1. Present strategies through which one can control, manage or delete data collected by online systems.
2. Explain the term cookies and cache.How will you clear your cookies and cache?
3. Can one request deletion of data from an online platform? What it the procedure to follow?
4. Why is using two-factor authentication a good strategy to follow?
5. How can you educate yourself in order to be efficient in controlling, managing and deleting data collected by online systems?

Applying different strategies to protect one's reputation online (MC 2.6.C.5)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Applying different strategies to protect one's reputation online **Code: MC 2.6.C.5**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	ADVANCED
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 5 LOs 5.32 and 6.33):

- Apply different strategies to protect one's reputation online.
- Explain the most appropriate strategies to protect one's reputation online.

Description

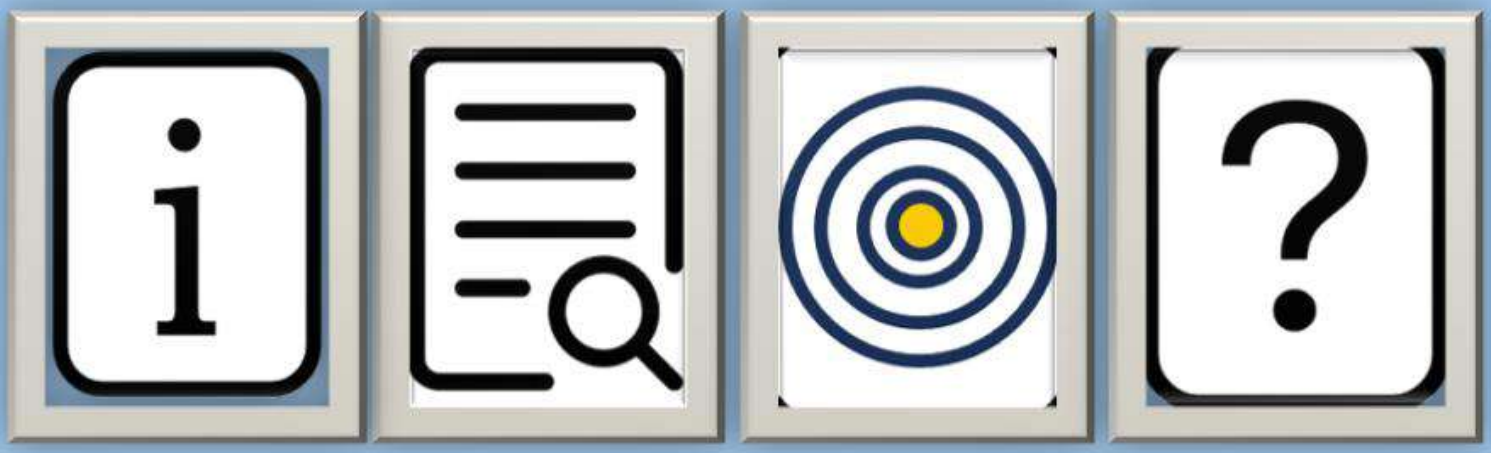
"Applying different strategies to protect one's reputation online" micro-credential demonstrates the ability of the learners to apply different strategies to protect one's reputation online such as to search their name and variations on search engines, to set up alerts in their browser in order to receive notifications about mentions or updates related to your online presence, to adjust privacy setting on social media platforms to control who can see your personal information, to use unique and strong password to various online accounts, to enable two-factor authentication whenever possible, to consider what type of content you share online to avoid posting controversial or offensive content.

This micro-credential also demonstrates the ability of the learners to explain the most appropriate strategies to protect one's reputation online, such as privacy settings, regular online monitoring, secure online accounts, content sharing and online etiquette.

Questions

1. Present strategies for protecting one's reputation online.
2. Describe the steps you will follow to set up alerts in two browsers in order to receive notifications about mentions or updates related to your online presence.
3. What do we mean when we talk about regular online monitoring?
4. How do we secure online accounts? Describe content that one can share online and content that one should not share online.
5.

EXPERT LEVEL
(Level 7 and Level 8)



Addressing complex problems related to digital identity and protecting one's own reputation online (MC 2.6.D.1)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Addressing complex problems related to digital identity and protecting one's own reputation online **Code: MC 2.6.D.1**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	EXPERT
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 7 LOs 7.34 and 7.35):

- Explain why creating solutions to complex problems related to digital identity requires a strategic approach.
- Explain why creating solutions to complex problems related to protecting one's own reputation online requires a strategic approach.

Description

"Addressing complex problems related to digital identity and protecting one's own reputation online" micro-credential demonstrates the ability of the learners to explain why addressing complex problems related to digital identity requires a strategic approach emphasizing on reasons such as the interconnected systems, the diversity of stakeholders, regulatory compliance, security and privacy concerns, the rapidly evolving technology, global considerations, ecosystem complexity and ethical considerations.

Additionally, this micro-credential demonstrates the ability of the learners to explain why addressing complex problems related to protecting one's own reputation online requires a strategic approach emphasizing on reasons such as the diversity of platforms and channels, continuous monitoring, the diversity of stakeholders, legal considerations, technology integration, the need for a proactive reputation building, the need for adaptability to change.

Questions

1. For which reasons addressing complex problems related to digital identity requires a strategic approach?
2. Name some key stakeholders whom we need to take into consideration when addressing complex problems related to digital identity. How are stakeholders related to the complexity of the problems related to digital identity?
3. Fow which reasons addressing complex problems related to protecting one's own reputation online requires a strategic approach?
4. How may legal considerations be related to protecting one's own reputation online?
5. Elaborate on the need for a proactive reputation building.

Guiding others in managing one or multiple identities and protecting one's own reputation online (MC 2.6.D.2)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Guiding others in managing one or multiple identities and protecting one's own reputation online **Code: MC 2.6.D.2**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	5-8 Hours
Level of the learning experience leading to the micro-credential	EXPERT
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 7 LOs 7.36 and 7.37):

- Guide others in managing one or multiple digital identities.
- Guide others in protecting one's own reputation online.

Description

"Guiding others in managing one or multiple identities and protecting one's own reputation online" micro-credential demonstrates the ability of the learners to conduct workshops on how to manage one or multiple identities, including sessions on how to set up privacy settings, how to review and cleanup, how to regularly update and how to showcase skills.

Additionally, this micro-credential demonstrates the ability of the learners to conduct workshops on how to protect one's own reputation online, including sessions on privacy settings, regular online monitoring, secure online accounts, content sharing and online etiquette.

Questions

1. Elaborate on the importance of guiding others in managing one or multiple digital identities.
2. Describe the main learning outcomes of a workshop you would organise on privacy settings.
3. Describe the main learning outcomes of a workshop you would organise on how to review and cleanup your digital identity.
4. Describe the main learning outcomes of a workshop you would organise on regular updates and showcasing skills on digital identities.
5. Elaborate on the importance of guiding others in protecting one's own reputation online.
6. Describe the main learning outcomes of a workshop you would organise on online etiquette.

Searching a name in online environments and modifying user configurations (MC 2.6.D.3)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Searching a name in online environments and modifying user configurations **Code: MC 2.6.D.3**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	3-5 Hours
Level of the learning experience leading to the micro-credential	EXPERT
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 7 LOs 7.38 and Level 8 LOs 8.39):

- Conduct an individual or family name search in online environments.
- Modify user configurations to enable, prevent or moderate the AI system tracking, collection or analysing data.

Description

"Searching a name in online environments and modifying user configurations" micro-credential demonstrates the ability of the learners to conduct an individual or family name search in online environments in order to inspect one's own digital footprint in online environments. Additionally, this micro-credential demonstrates the ability of the learners to modify user configurations through the use of apps, software and digital platforms in order to enable, prevent or moderate the AI system tracking, collection or analysing data.

Questions

1. What is the digital footprint?
2. Elaborate on the importance of conducting an individual search in online environments in order to inspect one's own digital footprint?
3. Describe the steps one should follow when conducting an individual search in online environments in order to inspect one's own digital footprint?
4. Can you elaborate on the importance of modifying user configurations to enable, prevent or moderate the AI system tracking, collection or analysing data?
5. Describe the steps one needs to follow to modify user configurations in order to enable, prevent or moderate the AI system tracking, collection or analysing data.
6. What is the opt-out option? Give examples.

Propose new ideas related to managing a digital identity and protecting one's reputation online (MC 2.6.D.4)

Basic Information

Identification of the learner	Any Citizen
Title and code of the micro-credential	Propose new ideas related to managing a digital identity and protecting one's reputation online **Code: MC 2.6.D.4**
Country(ies)/Region(s) of the issuer	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Awarding body(ies)	DSW Consortium Project Number: **101087628**
Date of issuing	Dec 2023
Notional workload needed to achieve the learning outcomes	1-3 Hours
Level of the learning experience leading to the micro-credential	EXPERT
Type of assessment	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Form of participation in the learning activity	Online Asynchronous
Type of quality assurance used to underpin the micro-credential	Peer Review

Learning Outcomes

Learning Outcomes (ref. Level 8 LOs 8.40 and 8.41):

- Propose new ideas in the field of managing digital identities.
- Propose new ideas in the field of protecting one's own online reputation.

Description

"Propose new ideas related to managing a digital identity and protecting one's reputation online" micro-credential demonstrates the ability of the learners to propose different ideas related to managing digital identities such as decentralized identity platforms, biometric authentication, AI driven identity verification, privacy preserving technologies and collaborative identity platforms.

Additionally, this micro-credential demonstrates the ability of the learners to propose different ideas related to protecting one's own online reputation such as blockchain based system for identity verification, personalized privacy and security apps and AI crisis management tools.

Questions

1. How could one leverage artificial intelligence to predict identity-related risks?
2. How could one leverage AI to proactively implement security measures to prevent potential threats?
3. Elaborate on ideas such as Consent-Based Identity Sharing that is allowing individuals to grant permissions for a specific and limited amount of time, thus having control over their personal information.
4. How could combination of biometrics contribute to accurate identity verification systems?
5. Elaborate on the idea of anonymous yet secure authentication, that will enable users to access services without revealing their full identity.

APPENDIX 1: LEARNING OUTCOMES FOR COMPETENCE AREA: MANAGING DIGITAL IDENTITY

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

COMPETENCE: COMMUNICATION AND COLLABORATION (2)		
COMPETENCE AREA 2.6: MANAGING DIGITAL EDENTITY		
To create, and manage one or multiple digital identities, to be able to protect one's own reputation, to deal with the data that one produces through several digital tools, environments and services.		
1	At basic level and with guidance, I can:	• Identify a digital identity • describe simple ways to protect my reputation online • recognize simple data I produce through digital tools, environments or services
2	At basic level and with autonomy and appropriate guidance where needed, I can:	• Identify a digital identity • describe simple ways to protect my reputation online • recognise simple data I produce through digital tools, environments or services
3	On my own and solving straightforward problems, I can:	• discriminate a range of well-defined and routine digital identities • explain well-defined and routine ways to protect my reputation online • describe well-defined data I routinely produce through digital tools, environments or services
4	Independently, according to my own needs, and solving well-defined and non-routine problems, I can:	• display a variety of specific digital identities • discuss specific ways to protect my reputation online, • manipulate data I produce through digital tools, environments or services
5	As well as guiding others, I can:	• use a variety of digital identities • apply different ways to protect my reputation online • use data I produce through digital tools, environments or services
6	At advanced level, according to my own needs and those of others, and in complex contexts, I can:	• discriminate multiple digital identities • explain the most appropriate ways to protect one's own reputation • change the data I produce through digital tools, environments or services
7	At highly specialised level, I can:	• create solutions to complex problems with limited definition that are related to managing digital identities and protection of people's online reputation • integrate my knowledge to contribute to professional practices and knowledge and guide others in managing digital identity

8	At the most advanced and specialised level, I can:	• create solutions to solve complex problems with many interacting factors that are related to managing digital identities and protection of people's online reputation • propose new ideas and processes to the field.

INTRODUCTION:

Communication and collaboration refer to the skills and competences required to effectively communicate and collaborate in the digital environment.

It involves the ability to use communication and collaboration with specific audiences and in specific context or to express opinions in public.

Communication and collaboration is achieved through identifying what a digital identity is and being able to create and manage one or multiple identities across digital systems, applications and services and by identifying and applying various strategies to protect one's own reputation such as reviewing and updating privacy settings, establishing professional profiles that are not associated with a personal profile, avoiding sharing personal details online, maintaining strong an unique passwords and being cautious about the content they post on social media platforms and to be cautious about the groups and forums they join online.

Last but not least, communication and collaboration through managing digital identity and protecting one's own reputation online serve as a powerful tool to create solution to complex problems, to guide others in managing digital identity and to propose new ideas and processes to the field.

PREREQUISITES:

To develop communication and collaboration skills, several knowledge areas and skills serve as prerequisites. These include:

1. **Basic Computer Literacy:** Individuals should have a fundamental understanding of computer operations, file management, and software usage to navigate digital platforms effectively.
2. **Internet Literacy:** Proficiency in using internet browsers, search engines, and an understanding of online security principles is essential for safe and effective digital communication.
3. **Adaptability to New Technologies:** Readiness and willingness to learn and adapt to new digital tools and technologies as they emerge in the rapidly evolving digital landscape.

FOUNDATION (LEVEL 1 and LEVEL 2)

COMPETENCE AREA 2.6: MANAGING DIGITAL EDENTITY			
COMPETENCE: TO CREATE, AND MANAGE ONE OR MULTIPLE DIGITAL IDENTITIES, TO BE ABLE TO PROTECT ONE'S OWN REPUTATION, TO DEAL WITH THE DATA THAT ONE PRODUCES THROUGH SEVERAL DIGITAL TOOLS, ENVIRONMENTS AND SERVICES.			
LEVEL: 1 - FOUNDATION At a basic level and with guidance I can: • Identify a digital identity • describe simple ways to protect my reputation online • recognise simple data I produce through digital tools, environments or services **LEVEL: 2 - FOUNDATION** At basic level and with autonomy and appropriate guidance where needed, I can: • Identify a digital identity • describe simple ways to protect my reputation online • recognise simple data I produce through digital tools, environments or services			
Learning Outcome	Level	K – S - A	Description
1. Define digital identity.	L1	K	Recognise that digital identity refers to the electronic representation of an individual or an organization. A digital identity is a set of information, attributes and credentials associated with an individual or organization that can be recognised and verified in the online environment. Recognise also, that a digital identity refers to a set of data identifying a user by means of tracing their digital activities, actions and contributions on the

			internet or digital services (for example, pages viewed, purchase history, personal data, geographical location and more).
2. Describe the key characteristics of digital identity.	L1	K	List some characteristics of digital identity such as **identification information** (for example, personal details such as name, surname, date of birth, address etc), **authentication credentials** (for example, username and password combinations, PINs, biometrics or any other authentications factors), **authorization data** (for example, determining what actions or resources the entity is allowed to access), **attributes and characteristics** (for example, additional information that describe the interests, affiliations or preferences of the entity), **digital certificates** (for example, digital signatures or certificates issued by trusted authorities to validate and verify the authenticity of the digital identity) and **biometric data (**for example, unique biological or behavioural characteristics, like fingerprints and facial recognition, used to verify an identity).
3. Provide examples of different digital identities	L1	K	The learner should be able to recognise that digital identities can take various forms across online platforms and services and that they serve a different purpose. A digital identity can be **an email account**, **a social media profile** on various social media platforms (Facebook, Instagram, X (former twitter)), containing personal information, posts and connections, **an online banking credential** containing a combination of username, password and additional security measures, **an e-government ID** for accessing government services, **a gaming profile** where the users can create digital identities associated with their gaming accounts, showcasing achievements, rankings and their in-game personas. A digital identity can also be**, a smart home device credential**, associated with smart home devices, enabling users to control and monitor devices with the use of digital tools and **a subscription services account**, for

			accessing subscription-based services such as streaming platforms, containing viewing history, preferences and account settings.
4. Describe the benefits of digital identify	L2	K	Describe the benefits of digital identity such as **security and authentication** (digital identity platforms enhance security through the use of multi-factor authentication, biometrics etc.), **convenience** (a digital identity allows for a more efficient online transactions and interactions across various digital platforms such as e-banking, e-commerce, etc.), **privacy protection** (individuals have the control over what information to share and who their audience is), **efficiency and accessibility** (individuals can easily access their digital identity from any place, at any time) and **technological innovation** (digital identity is serves as a foundational element for emerging technologies such as blockchain and AI).
5. Describe the risks of digital identity	L2	K	Describe the risks of digital identity such as **security concerns** (a digital identity is most likely to receive cyber threats, phishing attacks and malware), **privacy issues** (individuals share online content that may be collected and used against their own will), **lack of standardization** (there is a lack of standardized protocols and policies across various digital platforms and environments), regulatory and legal challenges (non-compliance with data protections and privacy regulations can lead to legal consequences and financial penalties) and technological innovation (outdated systems can become vulnerable to security threats when trying to meet new technological needs).
6. Identify simple ways to protect one's own reputation online.	L1	K	List the simple ways an individual can protect their own reputation online, such as **to review and update privacy settings** on social media platforms**, to establish professional profiles** on platforms that are not associated with their personal accounts on other social media platforms, **to avoid sharing personal details online** (for example, addresses or phone numbers), **to maintain strong and unique passwords** and to enable two-factor authentication whenever

			possible, **to be cautious about the content they post on social medi**a platforms and to be cautious about the groups and forums they join online.
7. Request guidance when needed to protect one's own reputation online.	L2	K	Request guidance on ways to protect one's own reputation online such as to **maintain strong and unique passwords** and to enable two-factor authentication whenever possible, **to be cautious** about the content they post on social media platforms and to be cautious about the groups and forums they join online.
8. Emphasize on the importance of protecting one's own reputation online.	L2	A	Sensitize on the importance of protecting one's own reputation online. The learner should be able to recognise that protecting your reputation online its crucial for your **professional opportunities**, for example, employers often conduct background checks in potential candidates, therefore a clean and professional digital presence can increase your chances of securing a job. Your online presence also contributes to your **personal branding,** for example managing carefully your online social media profile allows you to shape how other perceive you and it also allows you to build a network and strong connections. **Cybersecurity and privacy**, protecting your online reputation, involves safeguarding your personal information. Recognise that, businesses should also protect their own reputation online, because their online reputation impacts customer trust and loyalty, for example positive reviews, testimonials and a strong digital presence can lead to success and growth of a business.
9. Recognise simple data you produce through digital tools, environments and services.	L1	K	List simple data you produce through digital tools, environments and services such as **personal information** (name, date of birth, address, phone number), **online activity data** (browsing history, search queries, interactions with websites), **communication data** (emails, messages, call logs), **location data** (GPS data, check-in, location history), **transaction and financial data** (purchase history, financial transactions, payment information), **preference**

			and settings (customized settings, preferences, configurations), **authentication data** (usernames, passwords, authentication tokens), **device information** (device type, operating system, browser details), **biometric data** (fingerprints, facial recognition), **search queries** (terms and keywords entered into search engines) and **cookies and tracking data.**

INTERMEDIATE (LEVEL 3 and LEVEL 4)

COMPETENCE AREA 2.6: MANAGING DIGITAL EDENTITY			
COMPETENCE: TO CREATE, AND MANAGE ONE OR MULTIPLE DIGITAL IDENTITIES, TO BE ABLE TO PROTECT ONE'S OWN REPUTATION, TO DEAL WITH THE DATA THAT ONE PRODUCES THROUGH SEVERAL DIGITAL TOOLS, ENVIRONMENTS AND SERVICES.			
LEVEL: 3 – INTERMEDIATE On my own and solving straightforward problems, I can: • discriminate a range of well-defined and routine digital identities • explain well-defined and routine ways to protect my reputation online • describe well-defined data I routinely produce through digital tools, environments or services **LEVEL: 4 – INTERMEDIATE** Independently, according to my own needs, and solving well-defined and non-routine problems, I can: • display a variety of specific digital identities • discuss specific ways to protect my reputation online, • manipulate data I produce through digital tools, environments or services			
Learning Outcome	Level	K – S - A	Description
10. Discriminate a range of well-defined and routine digital identities	L3	K	Discriminate a range of well-defined and routine digital identities such as personal or professional social media identity, gaming identity, ecommerce user identity, educational platform identity, job search platform identity, subscription service identity etc.
11. Differentiate between a personal social media identity and a professional identity.	L3	K	Recognise that a personal social media identity is primarily used for socializing, connecting with friends and family and sharing personal experience. The learner should also be able to recognise the content being shared on a personal

			social media identity such as personal photos and videos, casual updates, information about hobbies and interests and the interaction style being informal. Recognise that a professional identity is primarily used for networking, career development and showcasing skills and achievements related to a specific professional field. The learner should also be able to recognise the content being shared on a professional identity such as details about work experience, professional achievements, skills, education and endorsements related to a specific career and the interaction style being formal and focuses on professional topics.
12. Recognize information and communication practices that help an individual to build a positive online identity.	L3	K	Recognise information and communication practices that can help an individual to build a positive online identity such as, to create and post content that reflects your values and interests positively, selective sharing, promote constructive dialogue and avoid getting involved in negative interactions, maintain a professional demeanour in professional platforms like LinkedIn and stay informed about digital trends and best practices.
13. Recognize information and communication practices that might cause a negative online identity.	L3	K	Recognise information and communication practises that might cause a negative online identity such as, to use offensive or inflammatory language when engaging in online interactions, to engage in online harassment, to share content that spreads misinformation and rumours, to behave inappropriate or unprofessional in professional platforms like LinkedIn and to have to ignore digital trends and best practises.
14. Describe what kind of data one produces through digital tools, environment and services	L3	K	The learner should be able to understand that through digital tools, environment and services, they produce data related to their personal information, digital signatures, contact information, biometrics, browser history and cookies, transaction history, preferences and interests, communication metadata, authentication and authorization data and records

			of consent given.
15. Manipulate the data one produces through digital tools, environment and services	L4	S	The learner should be able to manipulate the data one produces through digital tools, environment and services, for example in regard to their personal information, the learner should be able to recognise when it is necessary to add information such as their home address or telephone number and when it not necessary, on the cases when it is not necessary, the learner should be able to manipulate the data, either by not including them or by including a different set of data.
16. Sensitize on which data one should produce on digital identity.	L4	S	Sensitize on which data one should produce on digital identity, for example data related to their personal information should be avoided unless absolutely necessary (for example, home address, phone numbers), data related to financial information should be shared with cautious (for example, bank account numbers, credit card details, card PINs), data related to location should also be avoided unless necessary in order to protects one's own physical security and privacy. Data related to content, the learner should be cautious about expressing sensitive opinions or beliefs, in platforms where there is interaction with other people.
17. Create profiles in digital environments for personal or professional purposes	L3	S	The learner can create a profile through filling out profile details comprehensively, including a bio, contact information, education, work experience, and any other relevant details.
18. Manage profiles in digital environments for personal or professional purposes	L3	S	The learner can manage his/her profile in digital environment for personal or professional purposes through regular updates, setting privacy settings, showcasing skills, seeking endorsement, review and cleanup digital profiles etc
19. Present different strategies to protect one's reputation online.	L3	K	The learner should be able to present different strategies to protects one's reputation online such as, to monitor their online presence by searching on a regular basis their name and variations on search engines to see what information is available, to set up the alerts on their browser in order to receive notifications when their name is mentioned online. To adjust privacy settings on social media platforms, to be cautious about the information being shared

			online, to use strong passwords and to be cautious about the content you post online.
20. Describe what type of metadata is included in pictures being shared.	L3	K	Describe what type of metadata is included in pictures being shared, such as: • **EXIF data (Exchangeable Image File Format),** these include camera settings, information when the photo was taken for example shutter, speed, aperture, ISO and focal length. The date and the time the photo was captured and the geographic location of the photo. • **IPTC data (International Press Telecommunications Council),** these include a brief description of the photo, keywords or tags associated with the image and details about the copyright owner and usage rights. • **XMP data (Extensible metadata platform),** this includes additional information beyond EXIF and IPTC data. • **File information data**, these include the name and size of the file and the format in which the image is saved (JPEG, PNG).
21. Describe the ways you can modify the metadata of a picture being shared.	L4	S	Recognise the metadata that can be modified, for example: • **EXIF data (Exchangeable Image File Format),** you can change information like date, time and camera settings. • **IPTC data (International Press Telecommunications Council),** you can change information like edit captions, keywords and copyright information. • **XMP data (Extensible metadata platform),** you can modify extended metadata. Describe the ways you can modify the metadata of a picture being shared, such as using online tools and websites (Metapicz), using specialised software (Exif Pilot, Adobe Lightroom), on Windows and MacOS and using image editing software (Photoshop, GIMP).

22. Identify the **benefits** when managing one or multiple digital identities across digital systems, applications and services.	L4	K	Identify the **benefits** when managing one or multiple digital identities such as access and convenience, personalization, efficient authentication, customized services and professional networking.
23. Identify the **risks** when managing one or multiple digital identities across digital systems, applications and services.	L4	K	Identify the **risks** when managing one or multiple digital identities such as security threats, privacy concerns, identity fragmentation, data breaches, reputation damage, authentication challenges and lack of control.

ADVANCED (LEVEL 5 and LEVEL 6)

COMPETENCE AREA 2.6: MANAGING DIGITAL EDENTITY			
COMPETENCE: TO CREATE, AND MANAGE ONE OR MULTIPLE DIGITAL IDENTITIES, TO BE ABLE TO PROTECT ONE'S OWN REPUTATION, TO DEAL WITH THE DATA THAT ONE PRODUCES THROUGH SEVERAL DIGITAL TOOLS, ENVIRONMENTS AND SERVICES.			
LEVEL: 5 – ADVANCED As well as guiding others, I can: • use a variety of digital identities • apply different ways to protect my reputation online • use data I produce through digital tools, environments or services **LEVEL: 6 – ADVANCED** At advanced level, according to my own needs and those of others, and in complex contexts, I can: • discriminate multiple digital identities • explain the most appropriate ways to protect one's own reputation • change the data I produce through digital tools, environments or services			
Learning Outcome	Level	K – S - A	Description
24. Explain the phrase "consistent digital identity in all social media"	L6	K	Explain the phrase "consistent digital identity in all social media" as referring to maintaining a uniform online presence across different platforms. This includes using the same or similar usernames, profile pictures, and a standardized personal or professional branding strategy.
25. Justify why one should have consistent digital identity in	L6	S	Justify why one should have a consistent digital identity in all social media in order to create a recognizable personal brand that represents the person on

all social media			different online channels. Consistency portrays professionalism, trust and credibility, ease in finding the person, across platform engagement
26. Create a consistent digital identify in all social media	L6	S	Create a consistent digital identity in all social media through using same or similar username, designing a unified profile picture, composing a unified bio, maintaining consistent branding elements such as s colors, fonts, and logos across all social media profiles, linking to other profiles, maintaining a consistent style and tone on the posts but adapting the content to suit the unique characteristics of each platform while keeping the core messaging consistent, updating changes to all platforms.
27. Select a picture you would like to upload on a specific social media platform and modify its metadata using a specific software.	L6	S	Select a picture you would like to upload on a specific social media platform and modify its metadata using a specific software. The learner should be able to download and install Exif Pilot, open the image in the software, locate the metadata fields and make modifications. The learner should also be able to use Adobe Lightroom, select and open the image in the library module and enter the metadata panel. If using Windows, the learner should be able to right-click on the image, select properties, go to details and click on remove properties and personal information.
28. Emphasize the importance of modifying metadata in order to protect one's privacy.	L6	A	Emphasize on the importance of modifying metadata in order to protect one's privacy, for example by modifying or removing information regarding the location, time and date of where and when the photo was taken, the individual can prevent to disclose their whereabouts and information about their activities. By modifying metadata, the individual can control what information is shared and can minimize the risk of being tracked without their consent. By modifying metadata, the individual can maintain their anonymity.

29. Can manage one or multiple digital identities across digital systems	L5	S	Can manage one or multiple digital identities across digital systems for example Signing in through Facebook, or any other third-party authentication provider, means using your existing credentials from a social media or external service to access a website, application, or digital service. This method of authentication simplifies the sign-in process for users and offers a convenient alternative to creating and remembering a new set of credentials for each platform.
30. Considers the benefits and risks when managing one or multiple digital identities across digital systems, apps and services	L5	K	Can list the benefits of managing one or multiple digital identities across digital systems, apps and service such as establishing a personal branding and a professional reputation, maintaining network opportunities, improving efficient communication, adapting to change more easily, increasing visibility and more.
31. Uses strategies in order to control, manage or delete data that is collected by online systems	L6	S	Uses strategies in order to control, manage or delete data that is collected by online systems such as regularly clear cookies and cache, exercise right to request the deletion of one's data from online platforms, use strong passwords and two factor authentication, regularly audit connected apps and educate oneself.
32. Apply different strategies to protect one's reputation online.	L5	S	The learner should be able to apply different strategies to protect one's reputation online such as to search their name and variations on search engines, to set up alerts in their browser in order to receive notifications about mentions or updates related to your online presence, to adjust privacy setting on social media platforms to control who can see your personal information, to use unique and strong password to various online accounts, to enable two-factor authentication whenever possible, to consider what type of content you share online to avoid posting controversial or offensive content.
33. Explain the most appropriate strategies to protect one's	L6	K	The learner should be able to explain the most appropriate strategies to protect one's reputation online, such as:

reputation online.			• Privacy Settings: To adjust privacy settings on social media platforms, websites and other online accounts to control who can view personal information. • Regular online monitoring: To regularly monitor online presence by searching your own name online. • Secure Online Accounts: To strengthen security measures for online accounts by using strong and unique passwords and two-factor authentication. To change your password once every few months. • Content sharing: To be cautious of the content you share online, including text, emails, photos, and videos. • Online etiquette: To practice good online etiquette by treating others with respect and avoid making offensive or inflammatory comments.

EXPERT (LEVEL 7 and LEVEL 8)

COMPETENCE AREA 2.3: ENGAGING CITIZENSHIP THROUGH DIGITAL TECHNOLOGIES			
COMPETENCE: TO CREATE, AND MANAGE ONE OR MULTIPLE DIGITAL IDENTITIES, TO BE ABLE TO PROTECT ONE'S OWN REPUTATION, TO DEAL WITH THE DATA THAT ONE PRODUCES THROUGH SEVERAL DIGITAL TOOLS, ENVIRONMENTS AND SERVICES.			
LEVEL: 7 – HIGLHY SPECIALISED At highly specialised level, I can: • create solutions to complex problems with limited definition that are related to managing digital identities and protection of people's online reputation • integrate my knowledge to contribute to professional practices and knowledge and guide others in managing digital identity **LEVEL: 8 – HIGLHY SPECIALISED** At the most advanced and specialised level, I can: • create solutions to solve complex problems with many interacting factors that are related to managing digital identities and protection of people's online reputation • propose new ideas and processes to the field.			
Learning Outcome	Level	K – S - A	Description
34. Explain why creating solutions to complex problems *related to digital identity* requires a strategic approach	L7	K	Creating solutions to complex problems related to digital identify requires a strategic approach. This is due to several reasons such as **the interconnected systems** (digital identity management often involved multiple interconnected systems), **the diversity of stakeholders** (including individuals, businesses, government entities and service providers), **regulatory compliance** (the collection, storage and use of digital data comes with legal and regulatory frameworks), **security and privacy concerns** (managing multiple digital

			identities involves sensitive information and security and privacy are often required), the **rapidly evolving technology, global considerations** (digital identities often transcend national borders), ecosystem complexity (digital identities may include public and private entities) and ethical considerations (solutions must reflect to specific ethical standards).
35. Explain why creating solutions to complex problems *related to protecting one's own reputation online* requires a strategic approach	L7	K	Creating solutions to complex problems related to protecting one's own reputation online requires a strategic approach. This is due to several reasons such as the **diversity of platforms and channels** (online reputation spans across various social media platforms, websites and more), **continuous monitoring, the diversity of stakeholders** (including customers, employees, competitors and the public), **legal considerations** (dealing with one's own reputation online may involve legal aspects such as defamation, intellectual property etc.), technology integration (being able to use and manage digital tools for monitoring and modifying), the need for a proactive reputation building, the need for adaptability to change.
36. Guide others in managing one or multiple digital identities	L7	S	Conduct workshops on how to manage one or multiple identities, including sessions on how to set up privacy settings, how to review and cleanup, how to regularly update and how to showcase skills.
37. Guide others in protecting one's own reputation online	L7	S	Conduct workshops on how to protect one's own reputation online, including sessions on privacy settings, regular online monitoring, secure online accounts, content sharing and online etiquette.

38. Conduct an individual or family name search in online environments	L7	S	Conduct an individual or family name search in online environments in order to inspect one's own digital footprint in online environments. • The learner should be able to follow the following steps: • Search the family's full name of the individual or any other relevant information to different search engines (Google, Yahoo, Bing). • Search the name in various social media platforms (Facebook, Instagram, X (former twitter), LinkedIn). • Access online public records databases. • Access online court records or legal databases.
39. Modify user configurations to enable, prevent or moderate the AI system tracking, collection or analysing data.	L8	S	The learner should be able to modify user configurations through the use of apps, software and digital platforms in order to enable, prevent or moderate the AI system tracking, collection or analysing data. The learner should be able to follow the following steps: • Check account settings, more specifically settings related to privacy, data collection and other configurations. • Explore sections related to privacy, security and data usage on different platforms. • Review the terms of service and privacy policies. • Opt-Out of any data collection or analysis features. The learners should be able to access the settings of his/her phone device and opt-out of the tracking location option.
40. Propose new ideas in the field of managing digital identities.	L8	S	Propose different ideas related to managing digital identities such as decentralized identity platforms, biometric authentication, AI driven identity

			verification, privacy preserving technologies and collaborative identity platforms.
41. Propose new ideas in the field of protecting one's own online reputation.	L8	S	Propose different ideas related to protecting one's own online reputation such as blockchain based system for identity verification, personalized privacy and security apps and AI crisis management tools.

Project Coordinator:

EdiTC EDUCATION & INFORMATION TECHNOLOGY CENTRE

Partners:

DIMITRA educational organization

UNIVERSITAS GALATIENSIS

UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO

CYPRUS COMPUTER SOCIETY

MMC Mediterranean Management Centre

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

DSW DIGITAL SKILLS WALLET

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.