

DEVELOPING INFORMATION LITERACY SKILLS: UNDERSTANDING DIGITAL LITERACY

FACILITATOR'S GUIDE

This guide and the following lesson plan are designed to provide you with sample tools and preparation that you might consider using to deliver simple, introductory lessons to community members on the topic of digital literacy. IMLS has created these materials with the understanding that many organizations do not have the expertise or staff to deliver comprehensive trainings on information literacy topics. If you would rather seek the services of a subject matter expert, we have provided a sample guide for partnering locally with a trainer or offering online training resources to your **community**.

Thank you for all you do to promote information literacy every day.

Advance Preparation:

- While you prepare for this lesson on digital literacy, consider compiling a variety of examples to effectively convey the importance of the subject and engage participants.
- Examples can include digital-related articles, illustrations/infographics/other visual aids (make sure all sources are attributed), interactive websites, etc., that can help simplify complex information and make it more accessible.
- These resources can help you show participants the practical implications of digital literacy in their daily lives, empower them to make informed decisions about their online activity, and inspire them to become advocates for improving digital literacy in their community.

Setting Expectations:

The following section outlines some best practices that we have identified and encourage you to consider. You are welcome to revise as necessary to accurately reflect your training goals.

- Begin by welcoming participants to the training. Introduce yourself as the instructor and thank them for joining you today.
- Inform participants of your role and experience with digital literacy.
- Clearly communicate any expectations or guidelines for participation and behavior (e.g., avoid interruptions, put phones away). This helps set boundaries and creates a positive learning environment.
- Addressing confidentiality and privacy at the outset of the activity can encourage more active participation. For this lesson plan, we advise that participants' names and/or identities are not attributed to their commentary. Any reporting after the activity, whether internally or to the public, should be in the aggregate. Remind participants that they should not share any personal or confidential information.
- Give a brief outline of the format and agenda for the training. Let participants know how the training will be structured, including activities or exercises to come.

INFORMATION LITERACY LESSON PLAN

www.InformationLiteracy.gov

- Invite each participant to introduce themselves with their first name, if they are willing, in order to facilitate the conversation (not for attribution), and any relevant background information such as why they joined the training today. This helps create a sense of community and familiarity among participants.
- Emphasize the importance of everyone's participation and encourage all participants to share their thoughts and experiences openly. Assure them that all perspectives are welcome and valuable.
- Invite participants to ask any questions before the lesson starts.

LESSON PLAN

Objectives:

- By the end of the lesson, participants will be able to grasp why strong digital literacy improves individual/community wellbeing and know how to complete several key tasks related to digital literacy, including:
 - Using the internet safely;
 - Assessing the quality of online sources and their credibility to decipher what is real vs. fake;
 - Navigating mis- and disinformation on social media.

Materials Needed:

- Pen and paper, laptop, or mobile device

Duration:

- This digital literacy overview is designed to be delivered in 120 minutes, but it also can be broken into a series of trainings on the topic.

Lesson:

Introduction (10 minutes):

Greet participants and introduce the topic. Provide an overview of what will be covered during the lesson and why understanding digital literacy is important to individual/community wellbeing.

- The internet is an incredible resource for education. But before we can learn to use it safely and wisely, we need to understand how it works and how people can misuse it to mislead others.
- As technology evolves, we see more and more information every day — including mis- and disinformation. Digital literacy is the ability to use the internet and other digital tools to find correct information and apply that information to our own lives.
- This lesson will cover:
 - How to navigate the internet (basics, safety tips);
 - How to assess the quality of sources/source credibility (deciphering what is real vs. fake); and
 - How to navigate mis- and disinformation on social media.

Engagement (10 minutes):

INFORMATION LITERACY LESSON PLAN

www.InformationLiteracy.gov

Discuss participants' prior knowledge related to digital literacy and their experiences with the concepts being taught today.

- Ask the participants:
 - What does digital literacy mean to you?
 - How do you define it?
 - What are some examples of digital tools or technologies you use in your everyday life?
 - What are some potential risks or challenges associated with using digital technologies?
- Have them talk in pairs at first and then elicit several responses in the whole group.
- **Note:** Take care to promote an atmosphere of acceptance and respect. Before beginning, it may be beneficial to remind the participants once more to not disclose any personal or confidential information.

Instruction (40 minutes):

Present information, breaking down complex ideas into smaller, more digestible parts on:

- How to navigate the internet (basics, safety tips):
 - There are people all over the world who know how to exploit personal and business weaknesses on the internet. You can protect yourself and your business by being a responsible internet user.
 - **Use strong and unique passwords:** Use a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like your name or birthday.
 - **Enable two-factor authentication:** This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, in addition to your password.
 - **Keep software updated:** Regularly update your computer's operating system, web browsers, and security software to protect against vulnerabilities and abuse.
 - **Beware of phishing attempts:** Be cautious of emails, messages, or websites that ask for sensitive financial or personal information or urge you to click on a link. Before you respond or click on anything in an email, verify the legitimacy of requests by contacting the organization directly through official channels.
 - **Use secure websites:** Look for HTTPS in the URL and a padlock icon in the address bar when visiting websites, especially when entering sensitive information like passwords or payment details. This shows that the connection is encrypted and secure. Try going to a website on your laptop or mobile device to check it out!
 - **Use secure Wi-Fi networks:** Avoid using public Wi-Fi networks for sensitive activities like online banking or shopping. If you have to do something important online, like paying bills or checking your bank account, and you're using the library's Wi-Fi, you can use something called a VPN (Virtual Private Network) to make your connection more private and protect your information from being seen by other people on the Wi-Fi network. Also, always log out of your accounts when you're done and close the browser if you're using a public computer.
 - **Practice safe online shopping:** Only shop from reputable websites with secure payment methods. Search for reviews of the website and its products. Look for reviews on independent review sites or platforms like Trustpilot, Google Reviews, or the Better Business Bureau.

INFORMATION LITERACY LESSON PLAN

www.InformationLiteracy.gov

- **Be mindful of what you share:** Avoid oversharing personal information on social media and do not post that you are away from your house or on vacation. Adjust privacy settings to control who can see your posts and information. Use your laptop or mobile device to check your settings now.
- How to assess the quality of sources/source credibility (deciphering what is real vs. fake): With an increasing stream of contradictory information coming at us daily, it can be hard to decide what is real. vs fake.
 - **Evaluate the reputation of the source:** Consider whether the source is well-known, reputable, and recognized for its expertise in the field. Look for established news organizations, academic institutions, government agencies, and well-known websites.
 - **Check the author's credentials:** Look for author bios or profiles that provide information about their background and expertise. Be cautious of anonymous authors or those lacking verifiable credentials.
 - **Verify the accuracy of the information:** Cross-reference the information with other reliable sources to verify its accuracy. Be skeptical of information that lacks evidence or relies on anecdotal accounts.
 - **Assess objectivity and bias:** Look for signs of bias, such as one-sided arguments, inflammatory language, or ideological agendas. Be wary of sources that prioritize sensationalism or clickbait over factual accuracy.
 - **Check the publication date:** Information may become outdated or superseded by new developments over time.
- How to navigate mis- and disinformation on social media:
 - **Ask participants:** Why do you think some people share fake news stories? What is the potential problem with fake news and not being able to tell what is fake and what isn't?
 - **Misinformation:** Spreading false information (rumors, insults, and pranks).
 - **Disinformation:** The creation and distribution of intentionally false information, usually for political ends (scams, hoaxes, forgeries).
 - Report mis- and disinformation to the platform right away. You can usually do so right from the post. By taking this step, you can help prevent the spread of false information and promote a more informed online environment.
 - **Educate others:** Share information you learned today for finding and combating mis- and disinformation with your friends, family, and followers. Encourage critical thinking and skepticism when consuming information online.

Guided Practice (15 minutes):

Facilitate exercises where participants can practice applying new knowledge to real-life scenarios and may be faced with roadblocks.

- Put participants into small groups and give them copies of [the Sample Google Search handout](#) or other similar material. Ask participants to rank results from most to least reliable. As a group, define the term reliability on the board (the quality of being trustworthy).
- Have groups report out their ranking and explain why they ranked certain sources the way they did.
- Create a t-chart on the board with the headings "Reliable Source" and "Unreliable Source." Based on participants' rankings, place each source from the search examples into the relevant column. Document the reasons the participants provided for their rankings. Inform the participants that this

INFORMATION LITERACY LESSON PLAN

www.InformationLiteracy.gov

exercise is only for thinking about how to approach material and does not necessarily mean that any particular source is either “reliable” or “unreliable.”

- Reveal that the handout illustrates how search results actually appear — not in order of reliability but prioritized based on a variety of factors, including popularity, location, and search history.
- Ask participants to find a partner and together create a checklist for evaluating search results.
- Have them share out their checklist items and compile a list. Distinguish between checklist items that must be checked and checklist items that may be checked (for example, the website *may* end in .edu or the website *must* not state an opinion in its title).
- Checklists might include, but shouldn't be limited to, the following criteria:
 - What kind of website or page is this? (Personal blogs, discussion forums, and advice columns aren't typically reliable sources.)
 - Is the website connected to an educational institution or organization?
 - Is the website from a fact-checked news source you have heard of such as the Associated Press?
 - Does the website URL end in .edu, .com, .org, .net, or another extension? What does this tell you about the website?
 - Does the title of the website seem to be “clickbait” or include charged or sensational language?
 - Does the page or site have a credible author clearly listed?
 - Does the author cite sources?
 - Is an opinion shared in the title or heading?
 - When was the website or article published?
- Provide general guidance and support as needed.

Independent Practice (20 minutes):

After giving participants separate worksheets to complete, encourage them to apply what they have learned on their own.

Assessment (15 minutes):

Evaluate participants' understanding through formative assessment methods (e.g., questioning, observation, quizzes, etc.).

- Ask questions to discuss earlier activities:
 - Why is having a reliability checklist important?
 - How have these activities changed the way you will approach search results online?

Wrap Up (10 minutes):

Summarize the key points covered during the lesson.

- Internet Navigation Basics and Safety Tips:
 - Use strong and unique passwords to secure accounts.
 - Enable two-factor authentication for added security.
 - Keep software updated to protect against vulnerabilities.

INFORMATION LITERACY LESSON PLAN

www.InformationLiteracy.gov

- Beware of phishing attempts and verify requests.
- Look for HTTPS and padlock icons on secure websites.
- Avoid public Wi-Fi for sensitive activities.
- Practice safe online shopping using reputable websites.
- Be mindful of sharing personal information on social media and adjust privacy settings.
- **Assessing Source Credibility:**
 - Evaluate the reputation of the source and check author credentials.
 - Verify information accuracy by cross-referencing content with reliable sources.
 - Assess objectivity and bias, looking for signs of sensationalism.
 - Check the publication date for currency and relevancy.
- **Navigating Mis- and Disinformation on Social Media:**
 - Understand the difference between misinformation and disinformation.
 - Report mis- and disinformation to prevent its spread.
 - Educate others by sharing knowledge and promoting critical thinking.
- Ask participants to share one new thing they learned about digital literacy today.
- Summarize the importance of digital literacy for individual and community wellbeing.
 - Digital literacy enhances access to information, critical thinking, and communication skills, empowering individuals to navigate the digital world effectively.
 - It promotes employability, economic opportunities, and online safety, contributing to individual well-being and participation in the digital economy.
 - Digital literacy fosters community development, social inclusion, and civic engagement by enabling communities to use digital technologies for education, health care, and economic empowerment.
- Encourage participants to continue their progress with digital literacy.
 - Offer them digital literacy information websites that are accurate and trustworthy to check in the future:
 - **Real Fake: A Graphic Novel**
 - > https://www.cisa.gov/sites/default/files/publications/cfi_real-fake_graphic-novel_508.pdf
 - > Created by the Cybersecurity and Infrastructure Security Agency — Graphic novel for adults about online mis- and disinformation
 - **Tactics of Disinformation Fact Sheets**
 - > https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
 - > Created by the Cybersecurity and Infrastructure Security Agency — Fact sheets for organizations about online mis- and disinformation

Instructor Reflection:

- Reflect on the effectiveness of the lesson.
- Consider what worked well and areas for improvement.
- Adjust future lessons based on reflections.