

Mobile Information Literacy – Kenya Curriculum

Module 3: Making mobile phones and the mobile internet work for you

Stacey Wedlake

Lauren Holstein

March 2018

# TASCHA_logo_stacked_black

ABSTRACT (100–150 WORDS)

As millions of people come online across the globe through mobile devices, mobile information literacy is vital for those who have leapfrogged from traditional media to digital devices that provide instant access to information. Mobile information literacy is necessary to help people learn how to find and evaluate the quality and credibility of information obtained online, understand how to create and share online information effectively, and participate safely and securely. Mobile information literacy is critical to help people better consume, generate, and disseminate trustworthy information through both digital and traditional media. Most information and digital literacy curricula were designed for a PC age, and public and private organizations around the world have used these curricula to help newcomers use computers and the internet effectively and safely. The central question for this project is: what are the relevant skills, concepts, and attitudes for people using mobiles, not PCs, to access the internet?

140-CHARACTER SUMMARY

What are the relevant skills, concepts, and attitudes for people using mobile devices, not PCs, to access the internet & information?

KEYWORDS

mobile information literacy, information literacy, digital information literacy, digital literacy, mobile-centric, mobile-first, mobile phones, smart phones, Kenya, ICTs, libraries, curriculum, training, training of trainers

RECOMMENDED CITATION

Wedlake, S & Holstein, L. (2018). Mobile Information Literacy – Kenya Curriculum. Seattle: Technology & Social Change Group, University of Washington Information School.

ABOUT THE AUTHOR

**Stacey Wedlake** is a Research Coordinator at the Technology and Social Change Group.

**Lauren Holstein** is a graduate of the University of Washington Evans School of Public Policy & Governance.

ACKNOWLEDGEMENTS

First, the authors would like to acknowledge the work of the original Mobile Information Literacy Curriculum developed for Myanmar. Our work builds upon your research and curriculum. The development of this curriculum also received valuable input and direction from Ramune Petuchovaite, Ugne Lipeikaite, and Susan Schnuer of EIFL. Raymond Chepkwony and Juliana Muchai from the Kenya National Library Service (KNLS) helped with development and adaptation to the Kenya Public Library Context. Many thanks to the inspiring KNLS public librarians and library staff TASCHA researchers met on both of our trips to Kenya. Last but not least, thank you to the TASCHA Researchers and staff that provided important behind-the-scenes work to make this possible: Melody Clark, Maria Garrido, and Chris Rothschild.

COPYRIGHT, LICENCING, DISCLAIMER

Copyright 2018, University of Washington. This content is distributed under a Creative Commons Attribution Share-Alike license. The views, opinions, and findings expressed by the authors of this document do not necessarily state or reflect those of TASCHA, the University of Washington, or the research sponsors.

TECHNOLOGY & SOCIAL CHANGE GROUP (TASCHA)

The Technology & Social Change Group (TASCHA) at the University of Washington Information School explores the design, use, and effects of information and communication technologies in communities facing social and economic challenges. With experience in 50 countries, TASCHA brings together a multidisciplinary network of social scientists, engineers, and development practitioners to conduct research, advance knowledge, create public resources, and improve policy and program design. Our purpose? To spark innovation and opportunities for those who need it most.

CONTACT

Technology & Social Change Group
University of Washington Information School
Box 354985
Seattle, WA 98195

Telephone: +1.206.616.9101
Email: tascha@uw.edu
Web: *tascha.uw.edu*

Table of Contents

[Module 3 Overview 4](#_Toc521938242)

[Objectives 4](#_Toc521938243)

[Materials 4](#_Toc521938244)

[Module Guide 4](#_Toc521938245)

[Learning Objectives 4](#_Toc521938246)

[Take some time to review content from the previous module. Does anyone have any questions from the day before? 5](#_Toc521938247)

[Icebreaker 5](#_Toc521938248)

[App privacy basics 5](#_Toc521938249)

[Activity 3.1: Evaluating an app for credibility and security 5](#_Toc521938250)

[10 minute break 7](#_Toc521938251)

[App security basics 7](#_Toc521938252)

[Activity 3.2: Exploring local apps 8](#_Toc521938253)

[Smartphone exploration 9](#_Toc521938254)

[Debrief 9](#_Toc521938255)

# Module 3: Making mobile phones and the mobile internet work for you

## Module 3 Overview

Estimated total time: 3 hours

### Objectives

* Understand how to evaluate applications for trustworthiness, quality, etc.
* Learn about privacy and security settings on applications
* Learn how the mobile internet and smartphones can help in everyday lives to solve problems and improve livelihoods
* Learn how to download and use mobile apps locally available

### Materials

* Projector
* Blackboard/whiteboard (ideally)
* Paper
* Pencils

## Module Guide

### Learning Objectives

(10 minutes)

Outline the structure of the day: Before lunch, class will last approximately 3 hours including 10 minute break in between. Provide time to address any other administrative issues that need to be brought up before class begins.

Introduce to the class that at the end of module, the class will have a better understanding of the different ways they can use their smartphones to support their livelihoods and improve their lives. Explain to the participants that this module will be very hands-on and that for the majority of the lecture the participants will be working in groups or by themselves to apply what they have learned about what their smartphone can do and how their smartphone can work for them.

Pause to answer any questions.

### Take some time to review content from the previous module. Does anyone have any questions from the day before?

### Icebreaker

(10 minutes)

Explain that today we will do 2 rounds of introductions.

Round 1: Each person introduces him- or herself to the group by name and shares a safe, simple detail like a favorite app or favorite thing to do using their phone.

Round 2: Each person has to introduce someone else in the group by sharing that person’s name and, if they can remember, whatever else the other person shared. The facilitator should pick someone to go first. Whoever gets introduced goes next and picks someone new to introduce. Once someone has been introduced, they can’t be introduced again. If someone gets stuck, the group can help them finish their introduction.

(Mozilla, Digital Skills Observatory | [What’s possible online?](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-four.html#step-1))

### App privacy basics

(30 minutes)

Before we explore apps further, we’re going to review some safety and privacy steps you should take before downloading and using apps.

Earlier, we talked about when you create an account, you agree to share information with the apps. Can someone review what we talked about and what you should do?

When you create an account, you agree to share certain information. However, just by downloading app, you agree to share information with the app - even if you don’t create an account.

Before you download an app, in the Play store, you can view “the permissions” you agree to give the app. Here’s the permissions for “WhatsApp.” (Instructor’s note: Go here, scroll down to “view permissions.”) Does anything surprise you? Is there anything you don’t understand? (An alternative or an addition - look at the permissions from the app downloaded in the previous activity).

These permissions can be really confusing. There’s some things to watch for:

* Location/GPS
* Accessing contacts

Ask yourself why the app would need access to these parts of your phone.

Let’s look at Words with Friends permissions. This app asks access to your identity, contacts, and location - why?

### Activity 3.1: Evaluating an app for credibility and security

(30 minutes)

*Adapted from Mozilla,* [*What is Possible Online?*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-four.html#step-4)

**Objectives**:

* Understand how to evaluate applications for trustworthiness, quality, and content

**Materials Needed**:

* Computer
* Projector
* Smartphones for participants

**Introduction: (Use the following information to introduce and explain the activity to the class)**

Explain to the participants that this activity is designed to help them understand how to download and use apps, and how determine if the app is of high quality and safe for use.

Say to the participants that this next scenario is hypothetical, and a way that participants should consult applications to help them solve a problem. In this scenario, the students will think of ways they can use a phone to help in running a business.

Provide this scenario for the class:

One respondent sells jerrycans of water. She has a ledger that she would use to keep daily records of sales. However, she has heard that she can use an app to keep the ledger if she downloads it from the Google Play Store. This would help ensures that her records are always available since the app backs up to the cloud where she can always get at her information.

To help this business-owner problem-solve and find an app that works for her, ask participants (in pairs) to:

Search for a ledger app on the Play store (use the search bar and categories for discovery).

Emphasize that you’ll want to look at several options - just because a certain app appears first, doesn’t mean it’s the best fit.

* Check the description.
* Check the comments and ratings to help in decision.
* Look for any safety or privacy concerns.
* Check the app size.
* Choose the app that they think is the best based on its description, features, ratings, and size.
* Download the app.
* Install the app.
* Test the app with data that participants make up and put into the app.

While the pairs search, go around the room and check-in on the pairs and provide guidance as needed.

Before moving on, use the last 10 minutes of the activity to ask each pair to share the following:

* How did they choose their app?
* Did it work the way they expected from its description and ratings, or was it better or worse than they expected?
* Was the app difficult or easy to install and use?
* Could the participants use an app like this in their own lives or work? If so, how would they use it?

### 10 minute break

### App security basics

(20 minutes)

Now that you know what permissions you should watch for, you also need to keep safe from bad apps. Some apps are created to trick you into downloading them and can lead to malware and viruses on your devices that can cause problems in your device and compromise your information and security.

Show this article on the screen: [Why your vital mobile data is at increased risk](https://www.standardmedia.co.ke/business/article/2001255416/why-your-vital-mobile-data-is-at-increased-risk)

Explain that some apps are created to trick you into downloading them, and that you could inadvertently download malware that steals information from your phone including your PIN and bank information. Earlier, we talked about SPAM and Phishing. Ask is anyone familiar with the term malware?

Malware is a type of computer virus that intentionally damages a computer or smartphone.

As mentioned earlier, you should only download apps from the Google Play Store. All apps in the Google Play Store are checked for security issues. Now, this isn’t perfect, but it helps. Android has has a feature called “Google Play Protect” that will check all of the apps on your phone for security issues. To make sure Google Play Protect is on your phone, go to Settings > Google > Security > Google Play Protect.

Take time for participants to check their phone for Google Play Protect.

It’s also important that you keep apps up-to-date. Apps will routinely get updated to protect against new viruses and malware. Show everyone how to update their apps -

* Open the Google Play Store app
* Tap Menu   **Settings**.
* Tap **Auto-update apps**.
* Select an option:
	+ **Auto-update apps over Wi-Fi only** to update apps only when connected to Wi-Fi.

Explain that setting the apps to auto-update only over Wi-Fi will save data costs.

The best protection is for you not to download bad apps. Some apps are created to trick you. For example, if you want to download Facebook Messenger in the Google Play store, you’ll see several apps that are designed to look like Facebook Messenger. If you took a closer look and looked at the description, you would see that it’s not the app you’re looking for.

Using the steps we used earlier, looking at description, reviews, etc will help prevent you from downloading bad apps. To protect yourself, only download apps from the Google Play Store and read carefully before you download. And if you no longer use an app, delete from your phone.

Show the additional settings to protect privacy [from Mobile Security Toolkit from Library Freedom Project](https://libraryfreedomproject.org/mobileprivacytoolkit/)

* Settings and general stuff:
	+ iOS settings:
		- Settings → Touch ID & Passcode
		- Settings → Spotlight Search (off)
		- Settings → Keyboard → Predictive Text (off)
		- Settings → Keyboard → Enable Dictation (off)
		- Settings → Privacy → Location Services
			* Only give access where necessary
				+ Settings → Privacy → application data requests (review)
				+ Settings → Privacy → Diagnostics & Usage (don’t send)
				+ Settings → Privacy → Advertising → Limit Ad Tracking
	+ Android settings:
		- Settings → Connections → turn off all
		- Settings → location (off)
		- Settings→ more → Security
			* Password
			* Encrypt device
			* Device administrators
			* Unknown sources (uncheck)
			* Verify apps (check)

### Activity 3.2: Exploring local apps

(40 minutes)

*Mozilla |* [*How to solve problems with your phone*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-six.html#step-3)

**Objectives**:

* Learn how to download and use mobile apps locally available

**Materials Needed:**

* Smartphones for participants
* Paper
* Pencils
* Small pieces of paper with local apps
* Large pieces of paper
* Tape

**Introduction: (Use the following information to introduce and explain the activity to the class)**

This activity is designed to give participants a chance to learn about Kenyan apps.

Show the list of pre-made Kenyan apps. Ask if the list is missing any apps that participants have heard about. If so, add the app to small piece of paper.

Go around the room and have everyone take a piece of paper with an app name. Pair people up. As a pair, pick one app and go to the Google Play store and look up that app on their phone.

* Check the description. What does this app do?
* Check the comments and ratings. What do people think of the app?
* Look for any safety or privacy concerns. Do the permissions make sense for what the app does?
* Check the app size. How much space is needed on your phone?
* (If they think it’s safe to do so) Download the app.
* Install the app.
* Test the app. How well does it work?

On a large sheet of paper, have the pair write the name of the app and take notes on what they discover. After they finish analyzing one app, they can move onto the next app. Tape the paper with the notes about the app on the wall of the room. If they finish with both apps before everyone else is done, have the pair choose another app.

With 10 minutes left, ask participants to share any thoughts or discoveries they had while doing the exercise. Ask for the volunteers to present an app to the rest of the class. Encourage the participants to check out all of the findings on the apps during the rest of the day.

### Smartphone exploration

 (30 minutes)

Ask the class what respondents are interested in accomplishing using their phones. Write down their ideas and suggestions on a large piece of paper in the front of the room. Then, working in pairs, have participants work on accomplishing one of their goals. As the instructor, move around the room helping people as needed. Remind the class -

* Check the description.
* Check the ratings (check how many rated it).
* Check the reviews.
* Check the phone storage (check app size).
* Check privacy permissions
* Download and install app.
* Check for existing updates.

*Adapted from Mozilla |* [*What’s Possible Online?*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-four.html#step-5)

### Debrief

(5 minutes)

Briefly review key concepts identified, pause to answer any questions, and dismiss the workshop.