internet matters.org

digital matters

Parent & Carer Companion Guide

PRIVACY AND SECURITY MODULE

Introduction to protecting personal information online

PSHE Association Quality Assured Resource

Introduction

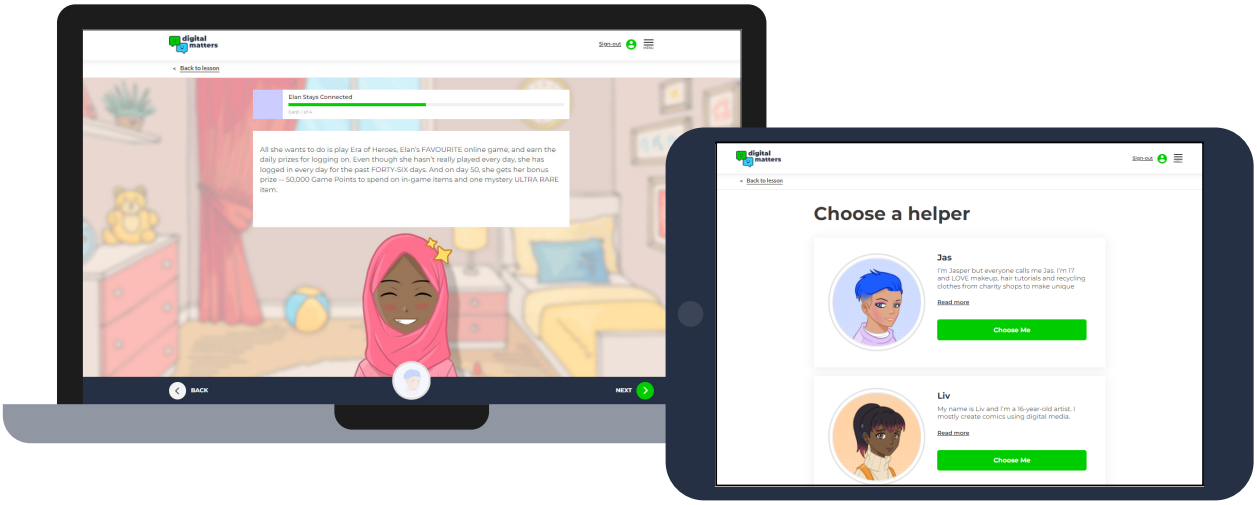
As the world becomes more reliant on technology, it's important for children to grow up understanding how the online world works and what positive interactions look like. The Digital Matters platform is designed to help children navigate online issues in a way that allows them to take risks and explore consequences without harm.

The platform is divided into two sections that help your child develop their understanding of each online safety topic.

The first is **Interactive Learning**, which is designed for use in the classroom. It features a range of quiz-based questions to encourage children to think about and discuss key points in the module. As a parent, you can also make use of this section to help introduce your child to the topics.

The second is **Once Upon Online**, a story-based activity where your child has to make choices to move the story forward. Users receive instant feedback on how their decisions impact the characters, helping children to understand that what they do online has real world consequences. The story allows them to make choices just to see where they go without putting themselves in harm's way.

Digital Matters is a great way to explore online safety in a realistic and engaging manner.



Take Home

As a part of the lesson, your child's teacher may assign take-home work to consolidate their learning. Teachers may choose from the following activities or may have their own activity for children to do.

Option 1: Your child might show you a printout of their Once Upon Online journey. With your help, they may be asked to consider what other choices the characters may have made and how those choices would have led to different results. Because the Once Upon Online story only allows children to select one of two choices, it's important to discuss other possibilities. It's unlikely that in real life children will only have two choices.

Option 2: Your child may share their Once Upon Online journey printout with you. There are also a selection of reflection questions for children to consider once they complete their journey. They can then discuss their journey and these questions with you. At home, you may want to do the journey on your own to see what ending you get and to compare the choices you each made. You may also wish to complete the journey a second time with your child and discuss the potential outcomes for each decision point.

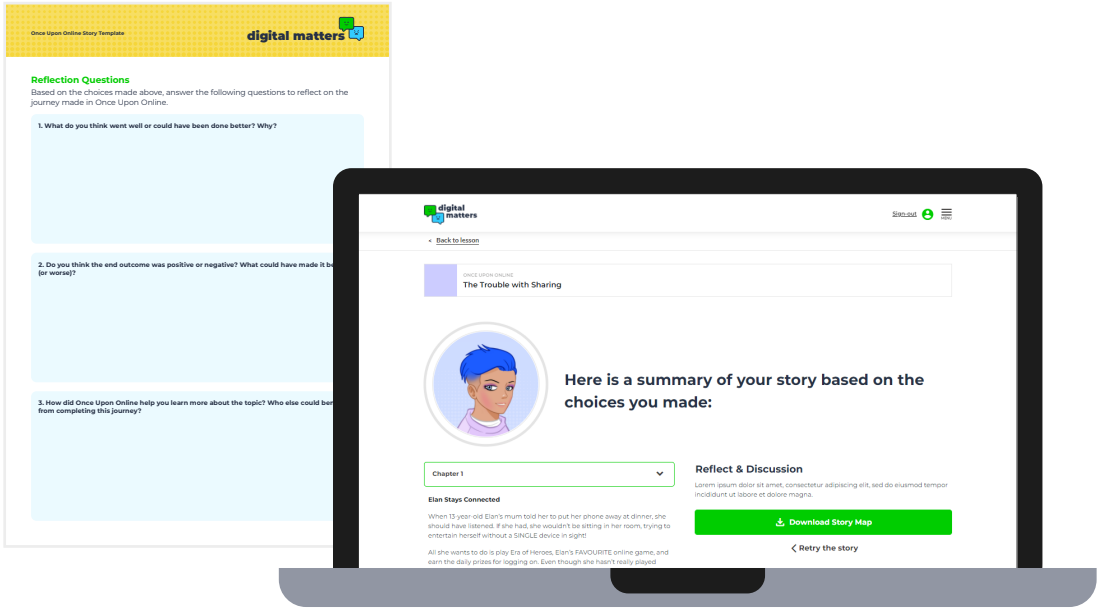
Privacy and Security

Fast facts you need to know

Use these facts to have informed conversations about the topic with your child:

- 66% of children aged 12-15 know how to block people when playing games
- only 41% of these children actually blocked anyone they didn't want to talk to
- 52% of parents of children aged 8-11 had rules in place about whom their child gamed with/ against
- 3/4 of 12-15s on social media know how to block someone from sending messages
- 1/3 of parents sat with or helped their children online
- only 32% of parents say they have used parental controls
- one of the biggest concerns of parents in the UK is companies collecting information about what their child is doing online

Source: Children and parents: media use and attitudes report 2020/21 (Ofcom)



Privacy and Security Quiz

How much do you know about privacy and security?

Keep your child's engagement with the module going by competing against each other on the quiz below. Who can score the highest?

Once finished, check out the answers at the end of the document to see how you did before learning a little more about each one.

1. Which of the following is an example of a STRONG password?
   a. p@22w0rd
   b. JanE1976
   c. v@sePlan3tree
   d. 19John90

2. Which of the following examples is NOT something that users should share publicly online?
   a. a photo of your child in front of their school on their first day
   b. a photo of your family in front of their new house
   c. a photo of you and your family abroad on holiday last year
   d. a photo of yourself out for a walk with friends

3. Discuss with your child: what are some ways you can keep yourself secure online?

4. If someone seems to be asking for personal information online such as login details, surname or bank information, what should you do?
   a. give them false information
   b. screenshot and post about them publicly to make others aware
   c. engage them in conversation and ask why they need it
   d. block and report them

5. What are the benefits of using parental controls on apps, devices and consoles?
   a. they're easy to set up and last forever
   b. they keep your child and family protected from inappropriate content and harm
   c. they limit who your child can talk to
   d. they help your child balance their online and offline lives

Recommended Resources

This list of resources will help you learn more about managing children's personal information online so that you can be prepared from privacy and security issues that might come up.

Internet Matters

Privacy and Identity Theft Advice Hub

It can be difficult to maintain a child's privacy as they may not understand what information is safe to share online, or what default privacy settings are on the sites and devices they're using. Explore the Internet Matters advice hub to learn more about what practical tools you can use to stay in control of your child's data online.

What is doxxing and how can you keep your child safe?

Doxxing is a scary problem that can put your child in danger. However, there are things you can do to ensure they are protected online. Colette Bernard from PixelPrivacy.com explains what you need to know.

Parental Controls

Give your child the power to create, connect and share safely online with step-by-step controls and privacy guides from Internet Matters.

E-Safety Checklist

Getting your children's devices set up safe will help you make sure that they get the best out of their device. This checklist gives you some simple tips to give you a head start.

ESET UK Newsroom

Get the latest information on security and privacy from Digital Matters' partner, ESET.

National Cybersecurity Alliance: Privacy Tips for Teens

Help your child take an active role in staying safe online with these tips.

SWGfL: What is Online Safety?

The first step to staying safe online is understanding the risks and harm that come with sharing private information. Be prepared by learning what online safety is.

Answers to the Privacy and Security Quiz

See how you did on the privacy and security quiz. Discussing the answers with your child will help them consolidate the information they learnt from the module. These conversations are vital to keeping your child safe online.

1. **The answer is C - v@sePlan3tree!** Stay away from passwords that use the word 'password', your name, or a date like a birth. These make your passwords easy to guess. Choosing three random words is a recommended format, and replacing letters with numbers can make it more secure. Generally, passwords should:
   - Use letters (upper and lowercase), numbers, and symbols
   - Be eight characters long or more
   - Not use obvious names or dates
   - Be something you will remember but others can't guess
   - Never be shared*

* Your child should understand that they may have to share their password with you for certain accounts. There may also be school passwords that are shared with teachers. However, they should not be sharing passwords with strangers or friends outside of these exceptions.

2. **The answer is A - a photo of your child in front of their school on their first day or B - a photo of your family in front of their new house.** However, there are risks with all types of publicly-posted photos. Photos that show identifying information such as the school your child goes to, where your family lives or where you currently are should not be shared publicly. If someone wants to find out where you are, these kinds of photos can make it easier for them. Check that privacy settings on photos are set up and that people are not sharing pictures without your permission.

3. Answers could include: setting up privacy settings/ securing your accounts, using a false name/ pseudonym instead of your real name, using an avatar instead of a profile image, sharing your country but not your city/not sharing your location at all, not sharing last names or names of other people, etc.

4. **The answer is D - block and report them.** While the other options may seem enticing, the only way to stop them from targeting others (and perhaps being successful) is to block and report them on the platform. They will then be investigated, which could likely result in their ban. It's best not to engage with them in any way.

5. Whatever you answered, you're right! Parental controls are an excellent way to monitor and limit who your child can speak with, what kinds of games they can play (appropriate to their age), what kind of content they see, how much/if they can spend on in-game purchases, the amount of time spent online, and more. They're really easy to set up and make a great long term solution for safety. Learn more here.