

MARCH 2019

PRIVACY ONLINE

A human rights education resource on privacy online, covering social media, terms and conditions, VPNs and web tracking.

For use with young people aged 11-18

TEACHING GUIDE

About this resource

We are a group of 3 students from Warwick Law School undertaking a human rights education project on privacy online. Our project's aim is to teach young people between the ages of 11-18 the privacy violations that take place online and how to reduce these risks. This resource covers the following topics: Social Media, Privacy Settings, Virtual Private Networks (VPNs), Terms & Conditions and Web Tracking. We have tested out this resource ourselves with a group of Year 7s and 8s with success.

Learning objectives

To give students:

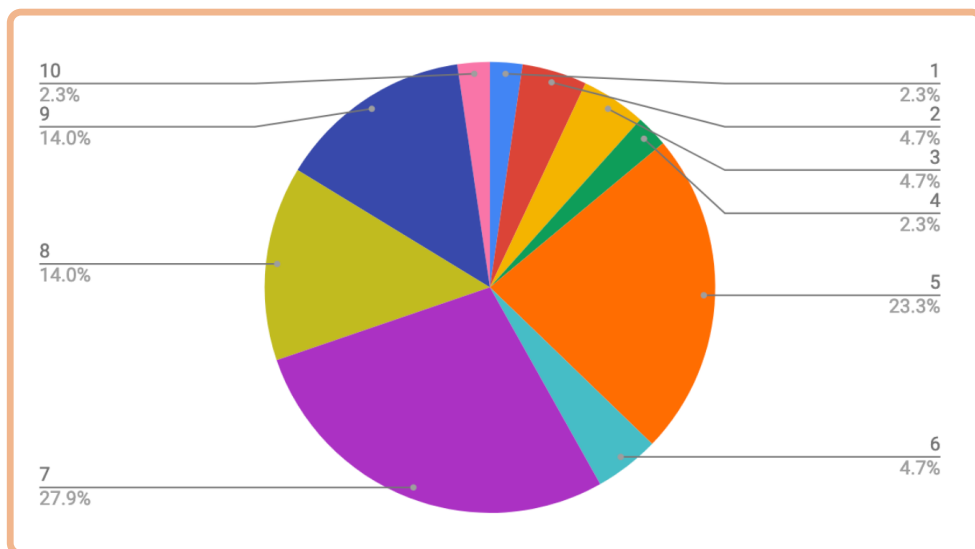
- awareness on the privacy violations of using the Internet and social media specifically.
- the tools to reduce these privacy risks when using the Internet.

FACTS & FIGURES

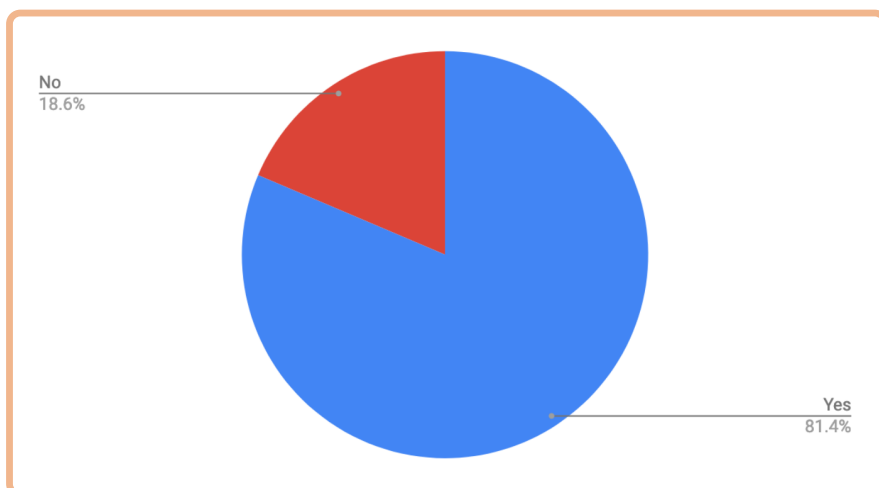
A summary from our evaluation sheets after running privacy sessions in a school in Rugby with Year 7-8.

How important from a scale of 1 to 10 are privacy issues to you?

(1 being not important at all, and 10 being extremely important).



86.2% of the young students gave an answer between 5-10, showing that most thought that privacy issues was a concern to them.



Do privacy issues seem more important to you now that you've taken the session?

This chart shows that most students found the session helpful and made them realise more how important privacy issues online were.

"Younger people still document their lives online but are not familiar with their settings...[they] are more at risk and targeted and more information is gathered about them."

- Dr Srimi (Professor in Texas specialising in data privacy)

LESSON PLAN

This lesson plan encourages young people to start thinking about the importance of their privacy online and the privacy issues that comes with social media. It is designed for use with a PowerPoint presentation which will be sent along with this guide and provided with a Google Slides link below.

The lesson plan is for use with young people aged between 11 and 18. The activities can be used in a stand-alone, interactive lesson in PSHE, or the PowerPoint presentation can be used alone with the Notes under each slide to be given as an Assembly to year groups. The activities enable young people to learn independently and as part of a group, and to apply their learning into their everyday lives to better protect their online activity.

Resources

For the main lesson, you will need:

- a whiteboard.
- Laptop and projector.
- **Staying Safe Online Presentation** (use the Notes under each slide as guidance for what to say for each slide) -> Link: <https://docs.google.com/presentation/d/1-e72zOc8nW6ZtKzMFuiFAkOxZSNLGxmTelTqMI8YPDg/edit?usp=sharing>
- Printing out **Activity Sheet 1** to give to individual students OR pairs / groups for them to brainstorm.
- Printing out **Handout 1** to give out at the end of class so students can better secure their privacy settings on Social Media if they want to.

Further Information

- **Big Brother Watch** Privacy Factsheets
<https://bigbrotherwatch.org.uk/factsheets/privacy-factsheets/>
- **Human Rights Watch** 'Everyday Encryption' Online Game
<https://www.hrw.org/everyday-encryption>

Activity 1:

(5 minutes)

BRAINSTORMING

Aim: to introduce the topic of privacy online.

Introduce to the class that you will be discussing topics dealing with privacy online. Start by asking the class to think of a word when they hear the word 'Privacy' when it comes to the Internet. Ask them which ones these are and write keywords that come up on a whiteboard.

Ask the class if privacy issues online are a concern of theirs. Get them to put their hands up for Yes or No, and ask for their reasons for whichever answer they gave.

Then, split the class into pairs or small groups. Get the groups to brainstorm on specific topics and what they know about those topics using **Activity Sheet 1:**

- Ghost profiles
- VPNs
- Web-tracking and cookies

Activity 2:

(10 minutes)

PRIVACY SETTINGS PRESENTATION

Aim: how to better protect yourself on social media and what are ghost profiles.

Put up the **Staying Safe Online Presentation** and introduce the first topic that will be discussed; Ghost Profiles. Feedback from each group what they thought a Ghost Profile is.

Then go through each slide and discuss what Ghost Profiles are and educate them on why it's important and why they should care. Clear up any questions they may have throughout the presentation and at the end. Then, ask the class now that they know what ghost profiles are, if it is something they are concerned about and get them to feedback why or why not.

** Let them know that at the end of the class, there will be a handout for them they can take home on how they can better secure their privacy settings online (**Handout 1**).*

Activity 3:

(10 minutes)

VIRTUAL PRIVATE NETWORKS (VPNs) PRESENTATION

Aim: how a VPN can better protect your online activity.

Using the **Staying Safe Online Presentation** again, move on to the next topic; VPNs. Feedback once again from groups on what they had brainstormed a VPN was from the first activity. Ask the class if anyone already uses a VPN.

Start with a quick quiz at the start of the powerpoint, getting the students to put their hands up for which answer they think is correct. Then, go through each slide and discuss what VPNs are and educate them on why they should consider to start using one and how it better protects their online activity. Clear up any questions they may have throughout the presentation and at the end.

Activity 4:

(10 minutes)

WEB TRACKING PRESENTATION

Aim: what is web tracking and cookies, and how they can limit the amount of data that is tracked.

Continuing with the **Staying Safe Online Presentation** and moving on to the third topic; Web Tracking. Again, feedback from their brainstorms from Activity 1 to see how much the class knows and what web-tracking is.

Then go through each slide and discuss what Web Tracking is and educate them on why it's important and why they should consider ad blockers. Ask the class if they have ever been online shopping for shoes etc. or looking up something, and the advertisements that come up after are on that specific thing. Explain that this happens due to web-tracking. Clear up any questions they may have throughout the presentation and at the end.

Activity 5:

(10 minutes)

TERMS AND CONDITIONS PRESENTATION

Aim: to raise awareness on the importance of terms and conditions and why they should consider reading them.

Continuing with the **Staying Safe Online Presentation** again, move on to the next topic; Terms & Conditions. Ask the class to raise their hands for Yes or No if they have ever read the Terms and Conditions of any website online, and ask them their reasons for reading them or not.

Then, go through each slide and discuss what are Terms and Conditions and educate them on why they should consider to start skimming through them so they are aware of what they are signing up for. Clear up any questions they may have throughout the presentation and at the end.

Activity 6:

(5 minutes)

FINAL CONCLUSIONS

Aim: to draw the lesson to a close

Ask the class again the same question you asked at the beginning of the lesson; whether privacy issues online are a concern of theirs now they have taken the lesson? Get them to put their hands up for Yes or No. Estimate whether the numbers have changed.

Then ask if anyone had said a different answer at the start of the lesson and ask those who did, what made them change their answer after taking the session?

Ask what they did not know before taking the session and what they have learned.

Then, draw the lesson to a close and give out **Handout 1** and explain how the handout details how they can better secure their privacy settings online.

Activity Sheet 1

Brainstorming

VPNs

Ghost Profiles

Web Tracking

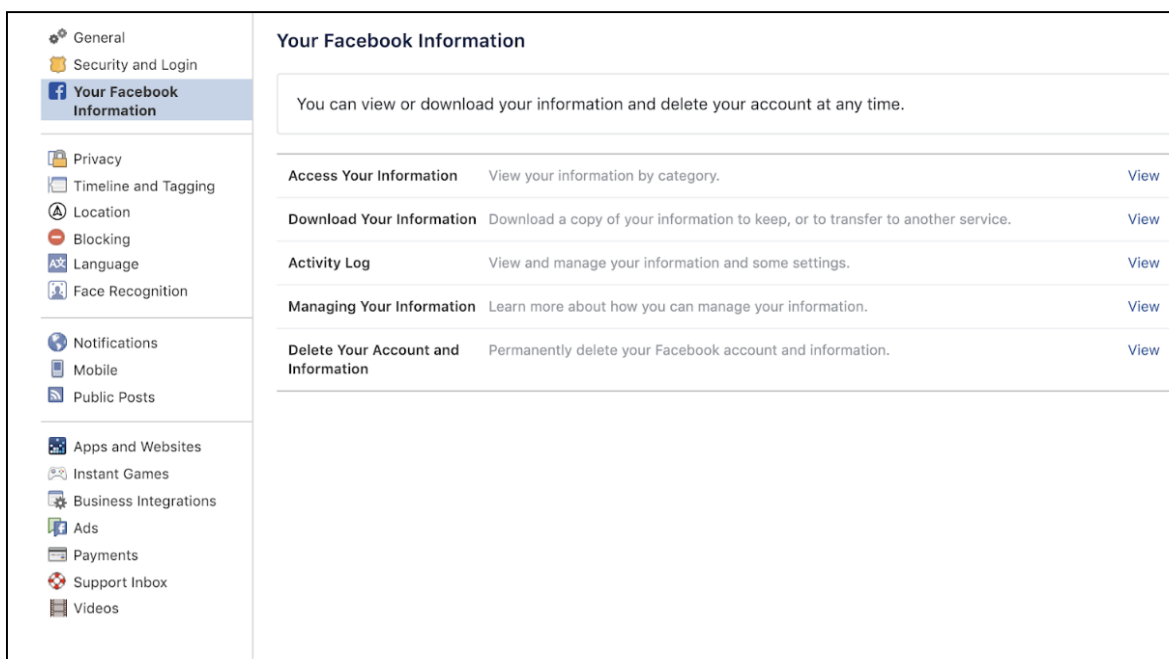
Handout 1

Securing your Privacy Settings on Social Media

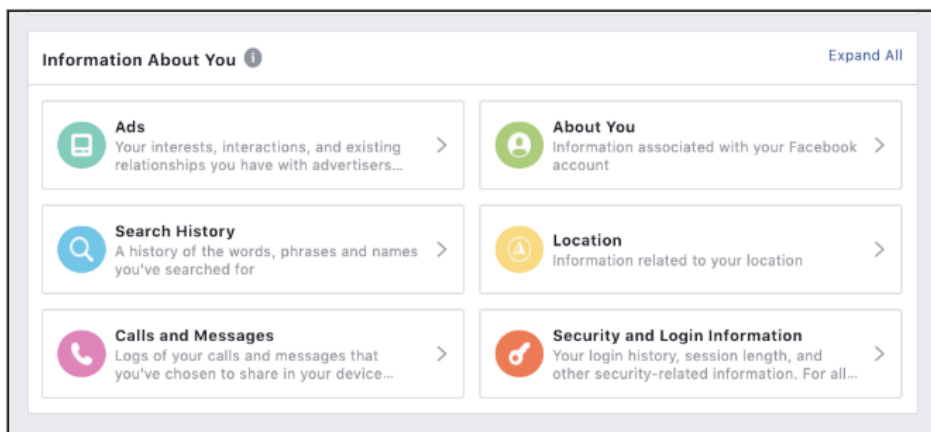
FACEBOOK

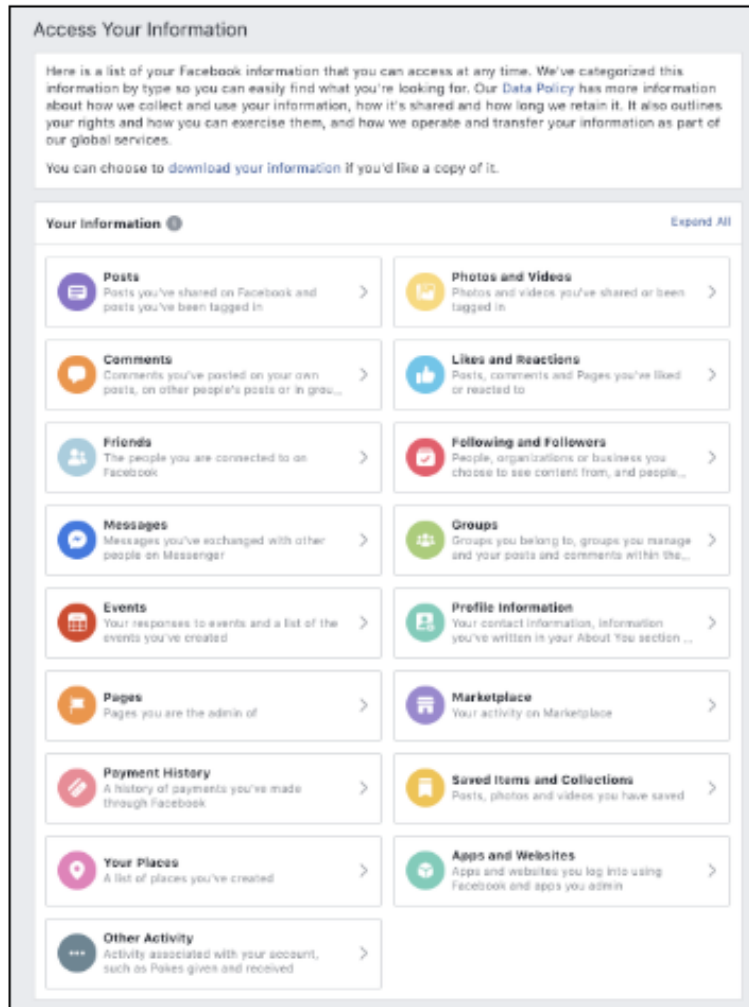
What does Facebook know about you?

1. Go to your settings on Facebook and click on the 'Your Facebook Information Tab'. Click 'View' in the 'Access your Information' section.

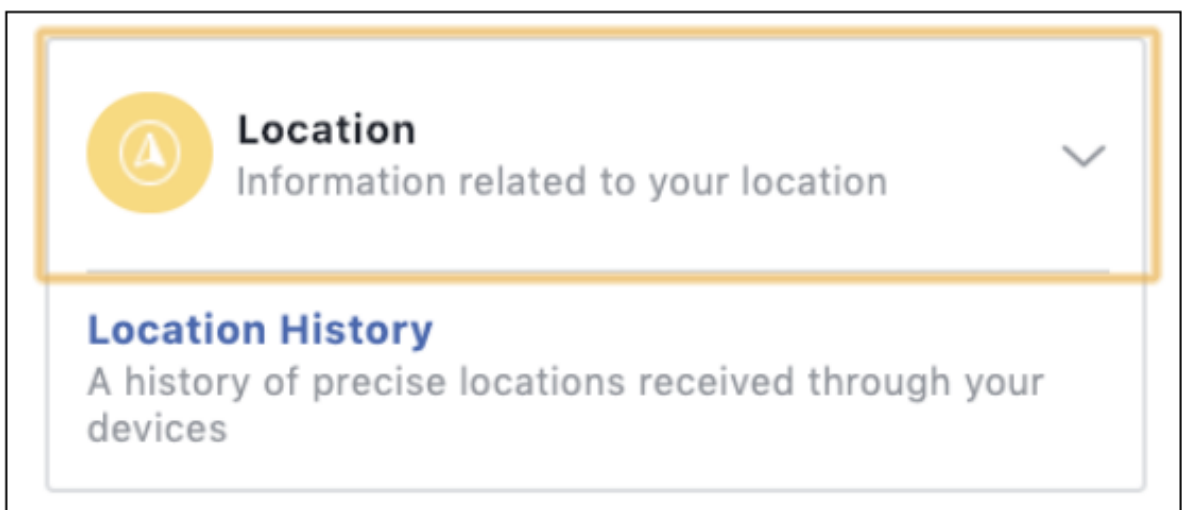


2. A page will come up entitled 'Access your Information' where you can see all the kinds of information Facebook collects on you.





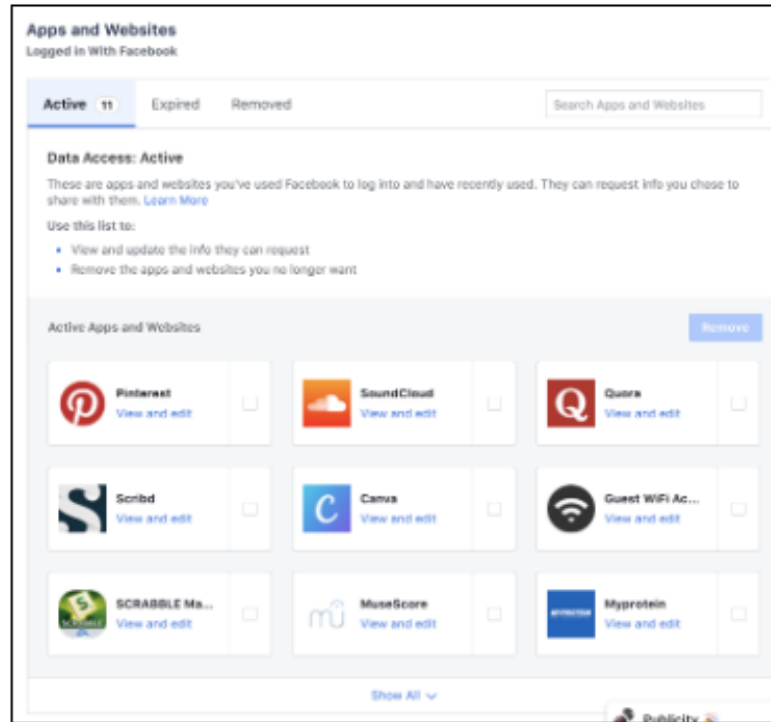
For example, one piece of information Facebook collects on you is your location and it does this mostly through the Facebook app on your phone if you have 'Location Services' enabled.



So how do you better protect yourself?

Another important thing to know is that ‘Apps and Websites’ section under the ‘Access your Information Page’ shows all the apps and websites which can access all this information through your Facebook.

Make sure you disable these apps and websites if you do not want them to be able to access your profile.



Limiting Audience

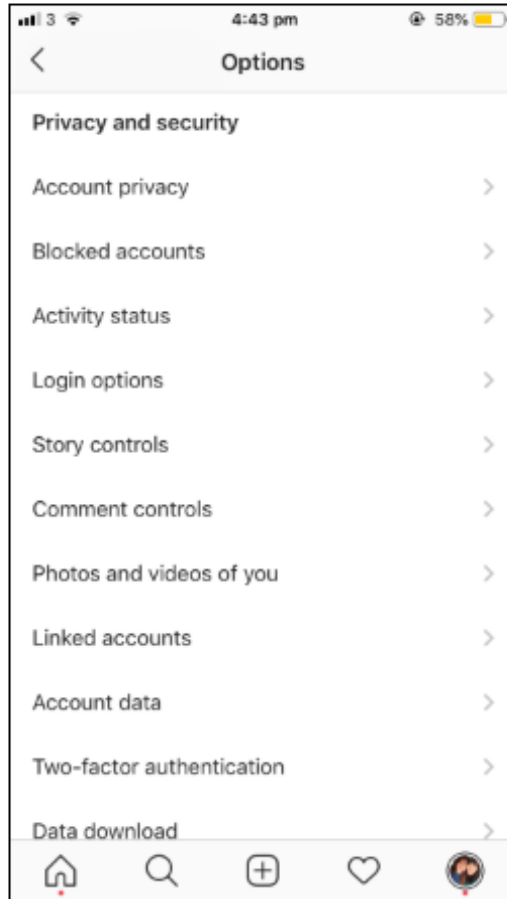
To ensure your profile is only seen by people you want, go back your ‘Settings’ again and this time, click on the ‘Privacy’ tab on the left. In this section, you can choose settings which will help protect your privacy better.



INSTAGRAM

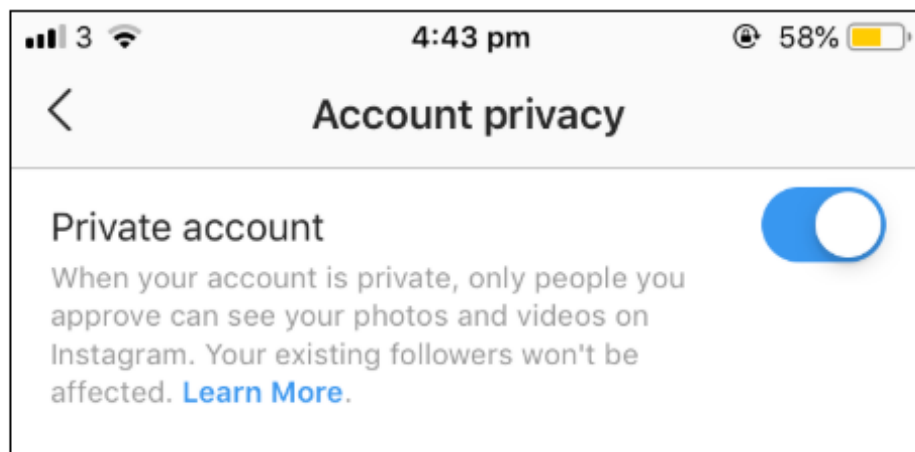
Improve your privacy settings

Go to your Instagram account 'Settings' and go to the 'Privacy and security' section.

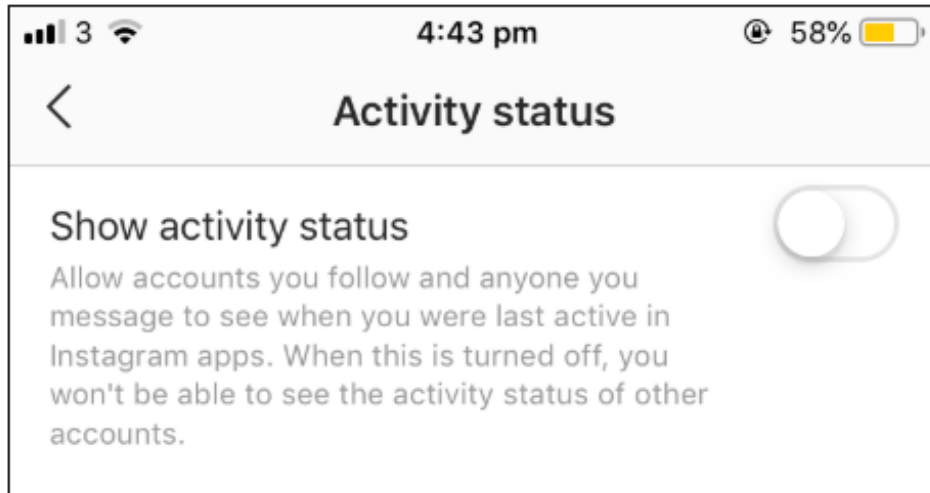


In each section, you can improve the privacy of your Instagram account.

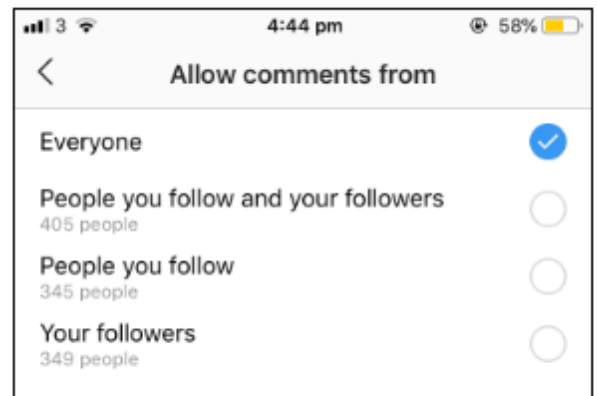
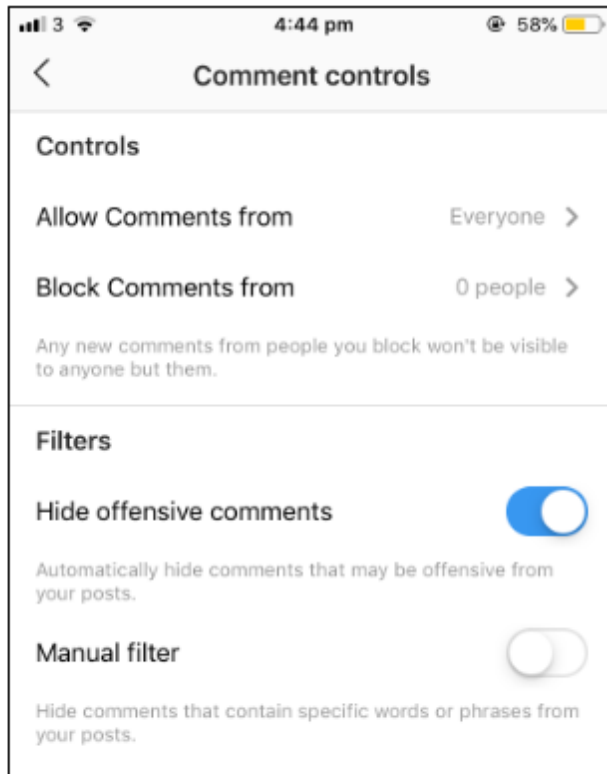
Account Privacy: you can make your account private instead of public so you control who sees your profile.



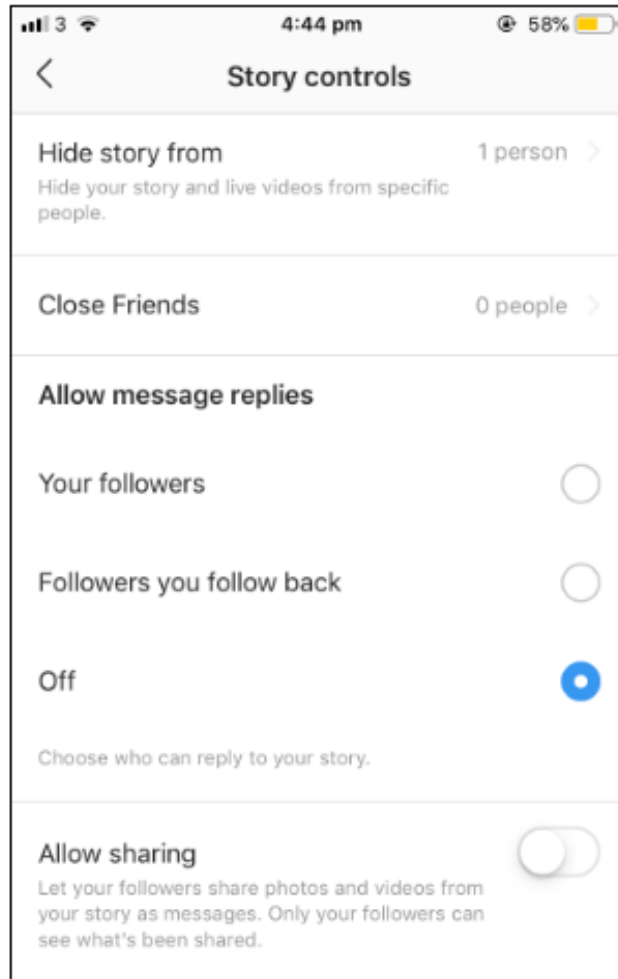
Activity Status: you can disable your activity status so those you follow and message cannot see when you were last active.



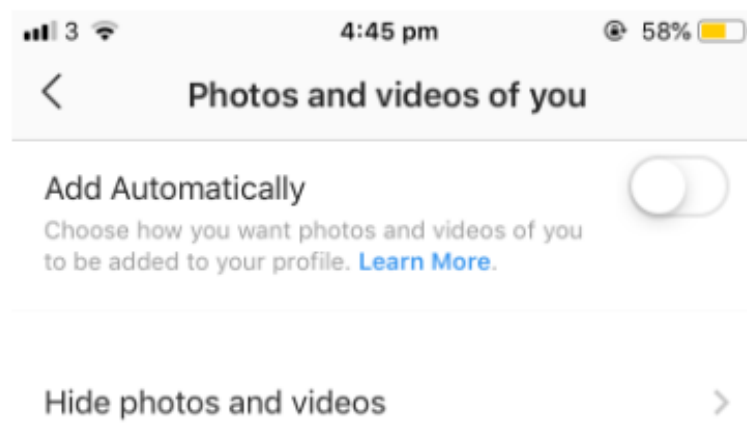
Comment Controls: you can also limit who comments on your photos, block comments from specific users and hide offensive comments.



Story Controls: you can control who sees your story by hiding it from certain people, making your stories only available to certain people under 'Close Friends' as well as whether you want message replies or sharing of your stories.



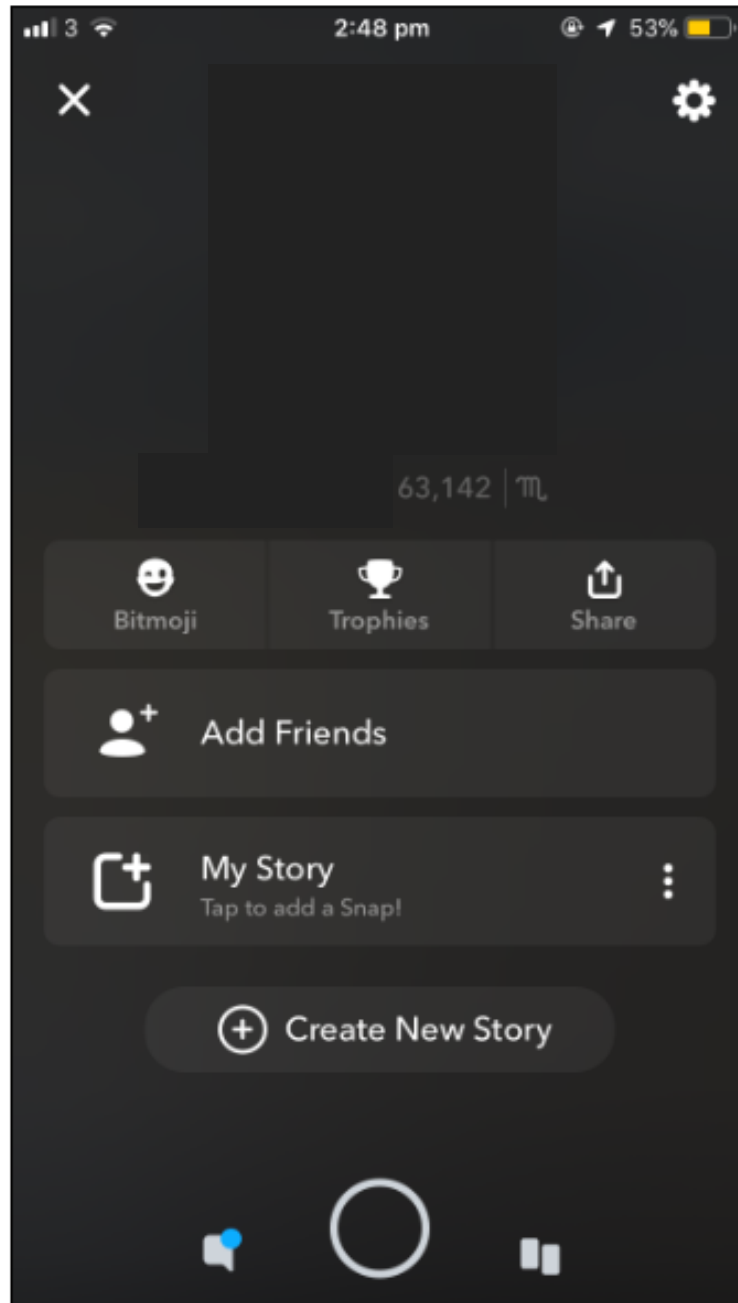
Photos / Videos of you: you can also control the photos or videos of you that other post and whether you want others to see these.



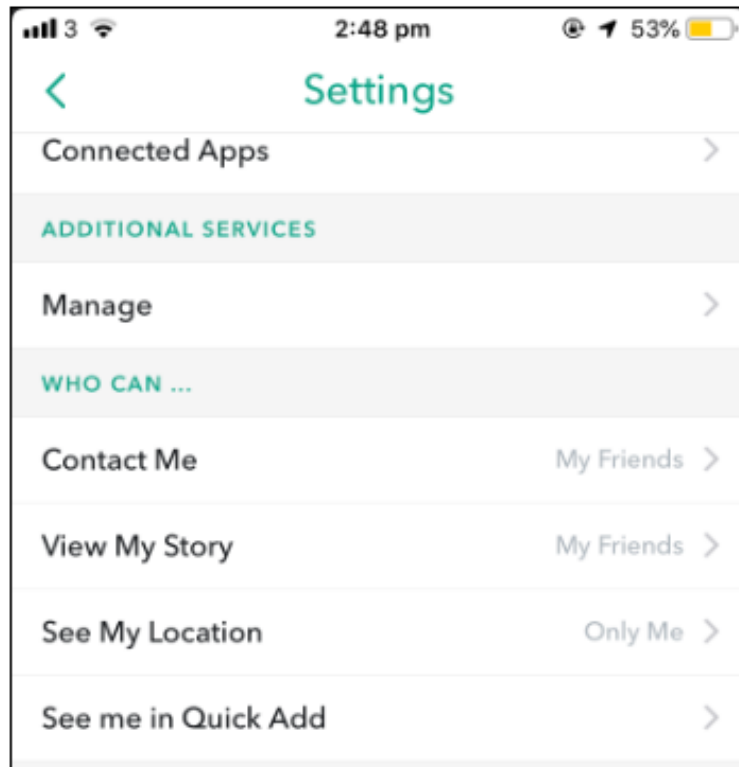
SNAPCHAT

Improving your privacy

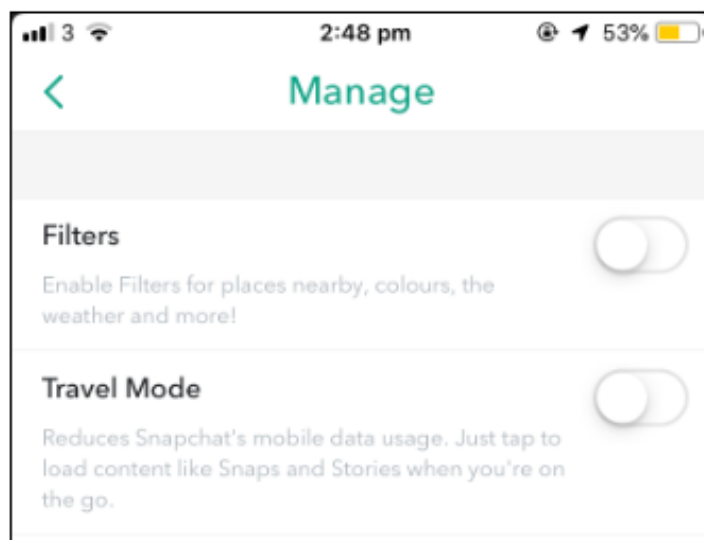
You can also improve your privacy settings for Snapchat by going to your profile and clicking the little cog in the top right hand corner of your screen.



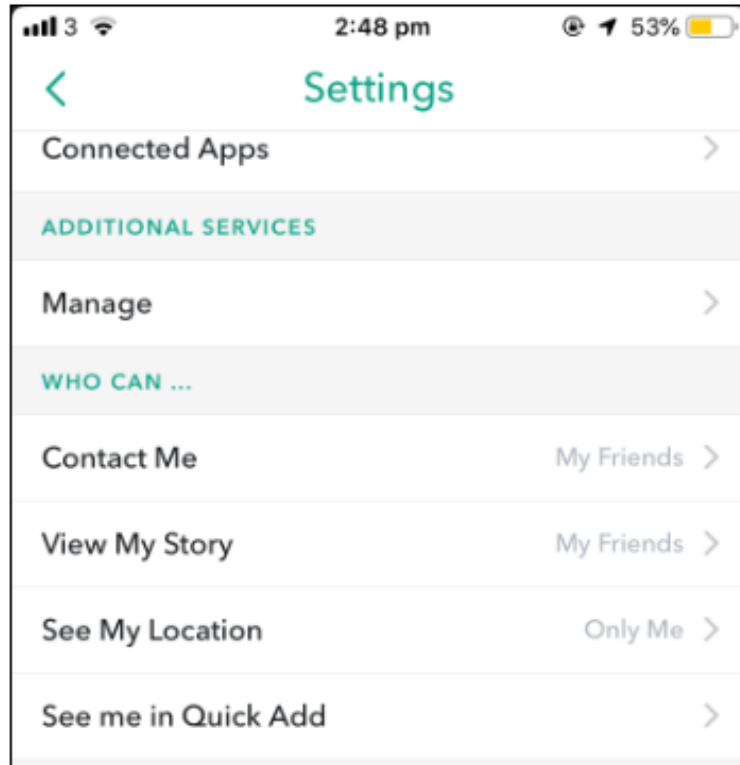
In Settings, you can control your privacy settings under the 'Who Can...' section where there are different sections for different settings.



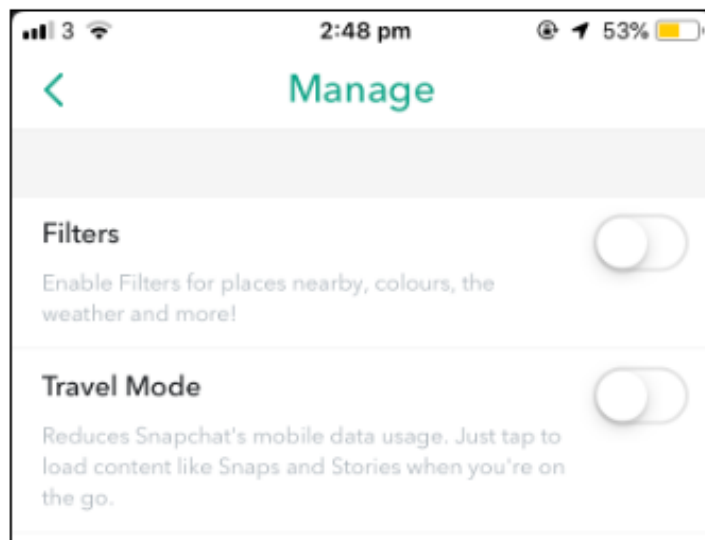
Under the 'Manage' section, if you disable the 'Filters', you would not be allowing Snapchat to track your location (which is what allows Snapchat to give you places nearby and tell you the weather as well).



In Settings, you can control your privacy settings under the 'Who Can...' section where there are different sections for different settings.



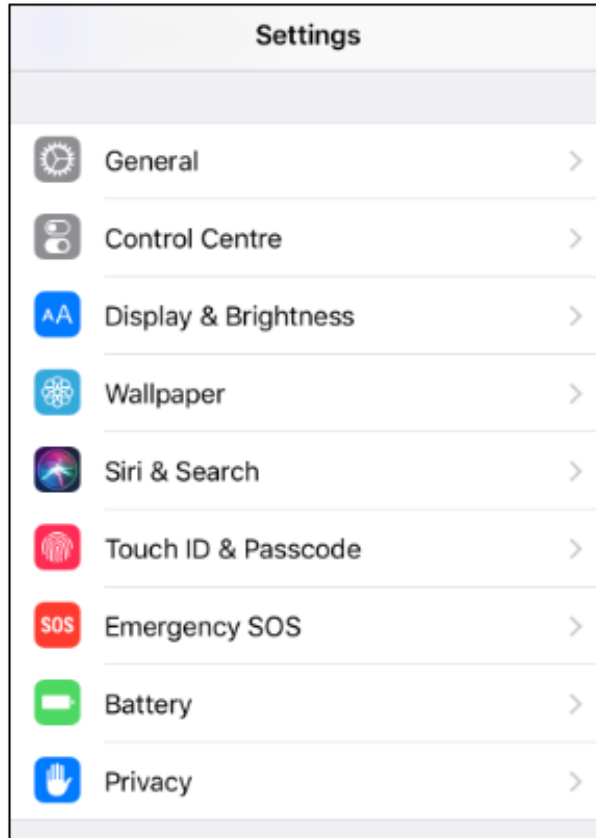
Under the 'Manage' section, if you disable the 'Filters', you would not be allowing Snapchat to track your location (which is what allows Snapchat to give you places nearby and tell you the weather as well).



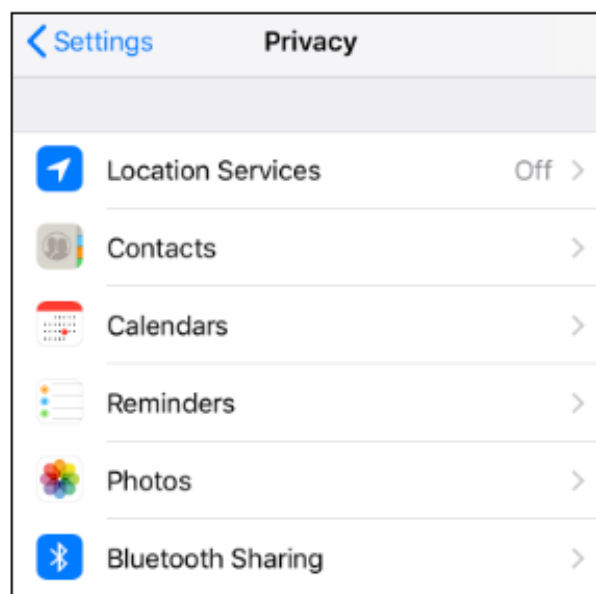
TURNING OFF YOUR LOCATION (iPhone)

How to stop apps and websites tracking your location

iPhone: go to the 'Settings' app and tap through to the section entitled 'Privacy'.



This is what the 'Privacy' section in Settings looks like and we just need to tap through on the first section entitled 'Location Services'.



Disabling your Location Services means apps and websites cannot track your location on your phone constantly. It helps to limit the time in which apps can tell where you are currently located.

