GENAZZANO
FCJ COLLEGE

Staying Safe Online

Guidelines and Recommendations

Updated 09/11/2015

Hyperlinks checked and updated:

Table of Contents

Internet monitoring

The College has invested in extensive firewall and internet filtering hardware and software to enable BYOD and College own devices to connect safely to the internet and the College network. All network traffic from College owned and BYO devices which are connected to the College network are monitored and filtered. This allows greater visibility into the activities of students and specific student use can be observed if required. At Genazzano we have a range of policies and protocols to assist us with managing student use of internet resources.

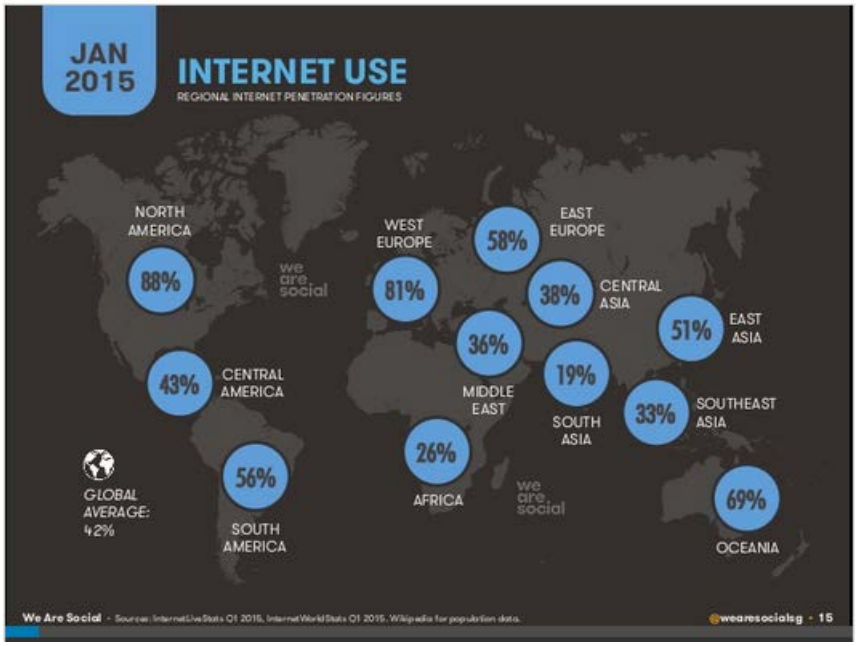


Figure 1 (source: http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015/)

The College firewall and filtering operates in the College environment. At home, parents will need to establish rules of use to ensure that the device is utilised in accordance with the Student Digital Technology Resources use Policy. Technologies such as the OpenDNS (https://www.opendns.com/) initiative allow parents to implement filtering in the home environment. The Australian Government Office of the Children's eSafety Commissioner (https://esafety.gov.au/education-resources/parent-resources/parental-controls) also provided advice on parental controls. Filtering tools can also be sourced from (http://sipbench.eu/index.cfm/secid.9) a safer internet program funded by the European Commission.

It is important to remember that the majority of Internet activity is positive. Care must be taken, however, especially when young people are new to the experience or the home has a wireless network enabling multiple devices to simultaneously access the Internet from various locations within the home. It is also important to note that even if the home internet connection is turned off, the internet can still be accessed via a Mobile phone.

We recommend using the following information as a guide for families to assist with providing a safe environment for internet usage, (general advice adapted from Office of the Children's eSafety Commissioner at (https://esafety.gov.au/) and (https://esafety.gov.au/education-resources/parent-resources)). There are four key elements to cybersafe practices in the home:

- education
- empowerment

- ensuring the safety of the computer/device
- supervision

These four elements work together towards providing positive and safe online use. The aim is not only to protect young people but to help them learn to make good decisions about internet usage. No web filtering technology is 100% fool proof so the best defence is observe online behaviours and assist your daughter in making a wise choice.

Education

An essential part of keeping your daughter safe online is making her aware of risks, and talking to her about how to avoid potential problems. The Office of the Children's eSafety Commissioner Website provides important Internet safety information (https://esafety.gov.au/esafety-information/esafety-issues) which provides a good starting point for discussion with your daughter.

Empowerment

Encouraging and supporting your daughter is a positive step towards making her feel confident about her Internet use. Young people need to know they can make the right choices. They also need to know they can talk to a parent if something happens online that makes them feel uncomfortable. It is important to keep lines of communication open.

Make the Device safe

One of the most practical ways to help children stay safe online is to set up the home computer with an Internet content filter and other security software. The College provides a filtering system for connected devices which is active whilst at school. Internet filtering solutions such as the OpenDNS, can provide a safe internet experience at home. A small change on your internet router can provide features such as anti-phishing and internet filtering on all internet-enabled devices which use the household internet connection.

Further information on specific internet filtering solutions can be found at https://www.opendns.com/home-internet-security/parental-controls/opendns-home/

It is important to note that this approach will not prevent students using features such as the 'WiFi tethering' option on many smart phones to gain access to an unfiltered internet connection. Parents are encouraged to participate in their daughter's use of the device and follow safe best practices. It should also be noted that the Open DNS service protects all devices using the household connect with the same level of filtering.

Supervision

Your daughter may behave differently online than she does in person. By placing the device in a family area, supervision becomes easier. It is widely accepted that internet connected devices should not be available for use in children's bedrooms.

Using the Internet safely at home

Before starting:

- talk with the family about the importance of staying safe online. For example, what is uploaded, tagged or posted online may not necessarily go away once it is deleted
- teach your daughter how to use the Internet safely. Use an educational program suitable for her age or learn about suggested guidelines, the website (https://esafety.gov.au/education-resources/parent-resources) can assist with this.
- The government has a Cyber Safety Help Button that can be installed on any computer or internet device which provides valuable resources for Cyber Safety (https://esafety.gov.au/complaints-and-reporting/cybersafety-help-button)
- Learn about the Internet and the types of Internet services children use – an excellent resource for parents is the parent eSafety guide accessed: (https://esafety.gov.au/education-resources/parent-resources/esafety-for-parents-basics)

Ensure a correct set up by:

- determining if your Internet service provider can assist with advice for staying safe online – if not, switch to one that can or adopt an alternative solution to provide this. Information can be obtained via:
    - Telstra (https://www.telstra.com.au/privacy/online-safety)
    - Optus (http://www.optus.com.au/about/sustainability/responsibility/cyber-safety/grown-ups/online-safety)
    - Vodafone http://www.vodafone.com/content/parents.html
- look at where the device is located – if it is in a bedroom, move it to a public/family area of the house where supervision is easier
- Ensure that a safe search engine is used for all web searches, e.g. Google Safe Search

Create family guidelines by:

- discussing the benefits and risks of going online
- ensure that young people feel that they turn to a trusted adult if they get into trouble
- create an Internet safety contract with children
- set house rules for Internet use; for example, set daily time limits for social media usage and online games

When online:

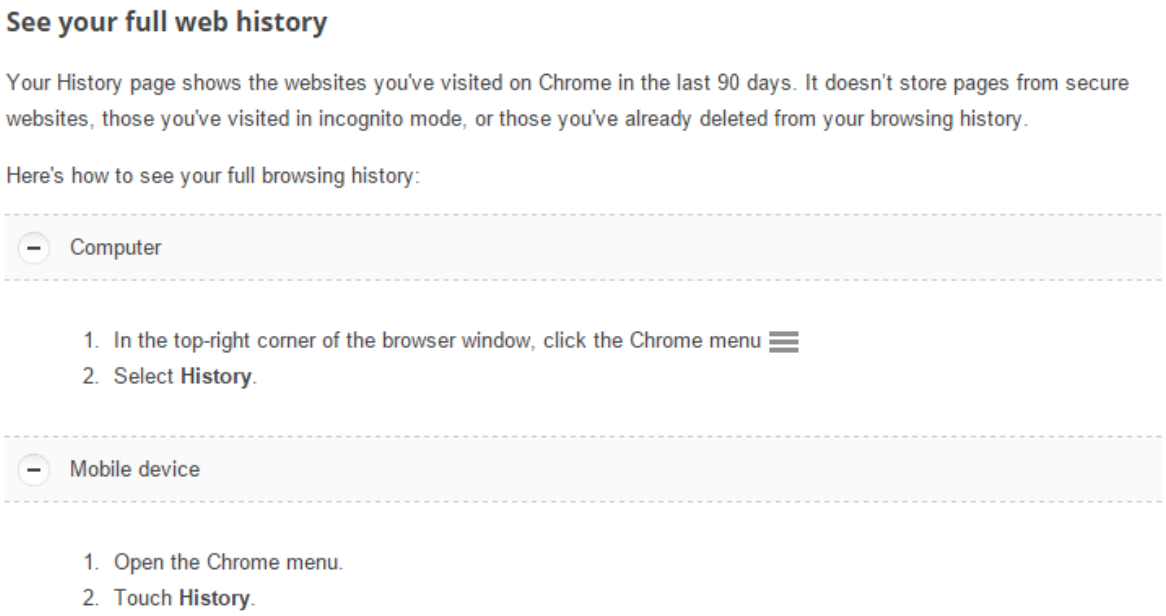
- stay involved in your daughter's use of the Internet and new technologies;
- work with your daughter to set up her account

- discuss what you and she may have read online (news, funny pictures and other entertaining information)
- remember a simple rule for online behaviour: if you wouldn't want your family to see it, don't post it!
- help the your daughter set up her profile and ensure she does not include too much personal information online
- check the privacy settings for Internet services and find out how to report abuse – many social networking, virtual networks and gaming sites have facilities to do this
- supervise and monitor the use of the Internet, particularly with younger children. If issues arise, address them quickly and know to whom problems should be reported
- above all, keep the lines of communication open – your daughter needs to be confident that she can talk to an adult about what's happening without being afraid that she will be automatically be banned from using the internet

Check the browsing history

Parents should be aware of how to have the capacity to look through the browsing history of the notebook/device. Internet Explorer keeps a 'trail' of the recently visited sites which can be easily accessed from the history menu. At school, teachers may, from time-to-time, request to see the browsing history on a student's device to ensure correct research procedures have been followed.

In Google Chrome



See your full web history

Your History page shows the websites you've visited on Chrome in the last 90 days. It doesn't store pages from secure websites, those you've visited in incognito mode, or those you've already deleted from your browsing history.

Here's how to see your full browsing history:

− Computer

1. In the top-right corner of the browser window, click the Chrome menu ☰
2. Select **History**.

− Mobile device

1. Open the Chrome menu.
2. Touch **History**.

In Internet Explorer

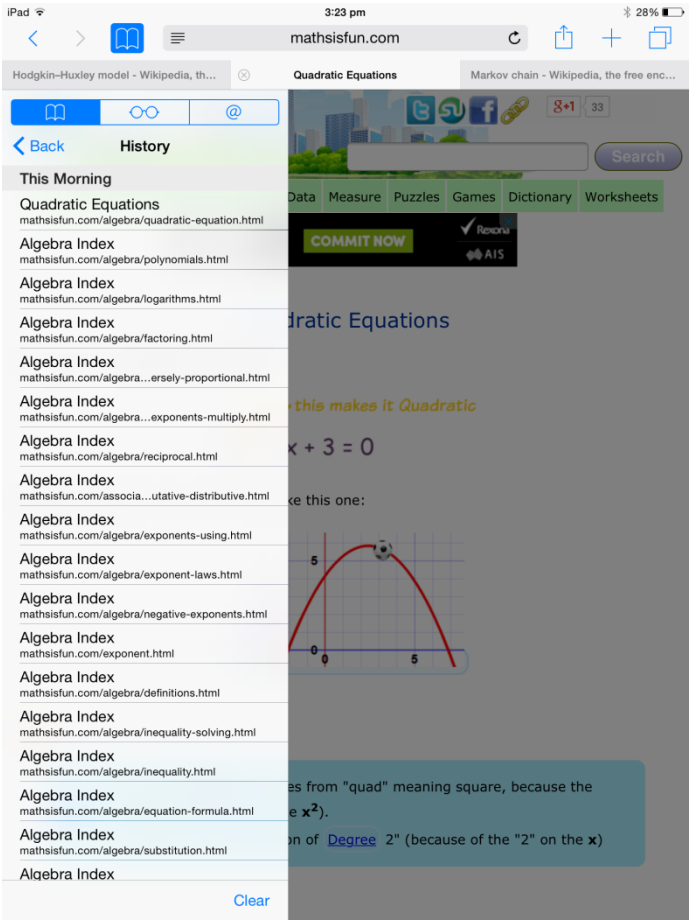
View your browsing history and delete specific sites

By viewing your browsing history, you can choose to delete specific sites, or return to a webpage that you've already visited.

1. In Internet Explorer for the desktop, tap or click the **Favorites** button ☆.
2. Tap or click the **History** tab, and choose how you want to view your history by selecting a filter from the drop down menu:
   - **View By Date** shows your last three weeks of history in chronological order.
   - **View By Site** shows a list of sites you visited in the last three weeks, but not the dates of your visits.
   - **View By Most Visited** shows your most visited sites in the last three weeks.
   - **View By Order Visited Today** shows only sites you visited today.

On an iPad

Open safari then select the book icon.

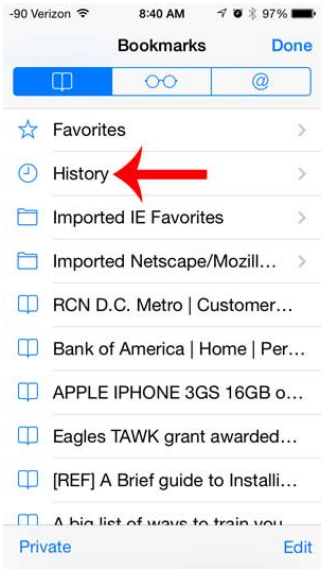


On an iPhone

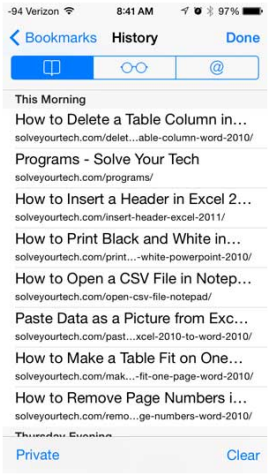
Step 1: Launch the **Safari** browser.

Step 2: Touch the book icon at the bottom of the screen. If you do not see the book icon, then scroll up on the page to display the menu at the bottom of the screen.

Step 3: Select the **History** option at the top of the screen.



Step 4: Select the book icon at the top of the screen to view your history. Note that all of the pages that have been visited on the device are sorted by the day or time on which they were viewed.



Social Media

Social media is ubiquitous and when used responsibly is a good way to stay in touch with those friends and family you do not have the chance to see or meet often. However, it is important for your daughter to realise that it is often difficult to control what happens to information and images that are posted online. Images shared can be distributed to others without your daughter's knowledge or consent.

Due to the instant and immediate nature of the medium social media can also be used as a means to harass and bully another person.

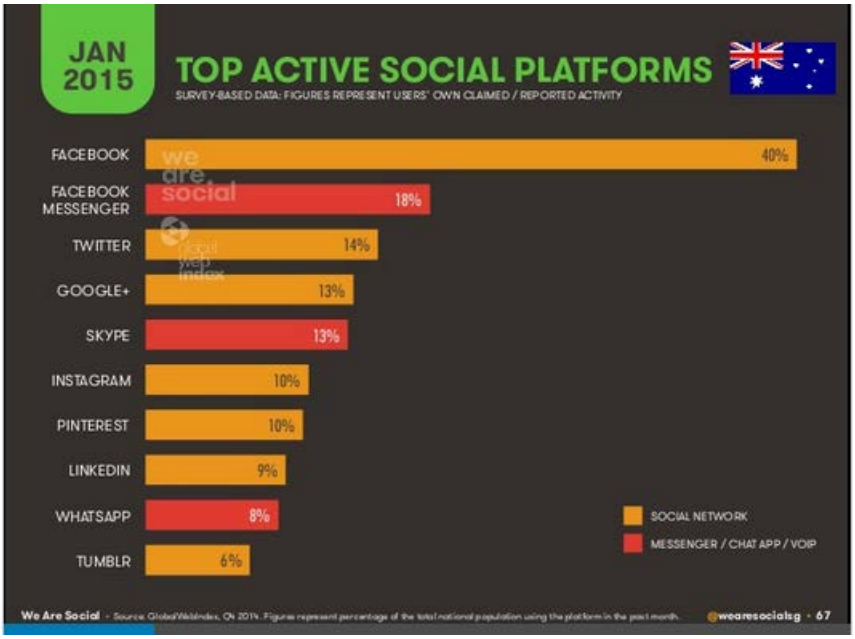
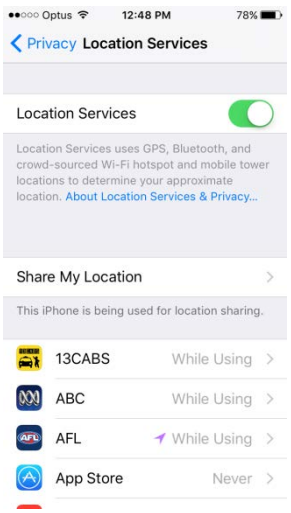


Figure 2 (source: http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015/)

Cyberbullying can be very confronting and incessant given the perceived anonymity and ubiquity of social media. If your daughter is experiencing such behaviours please note that Genazzano FCJ College has a zero tolerance approach to any form of bullying and any incident involving our students can be reported to the College; in addition, assistance can be found here https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/social-media-services-safety-centres . If your daughter is subject to Cyberbullying take a screen shot or picture of the offensive material in case you are required to submit it for further investigation.

Data Privacy & Surveillance

A good general rule of thumb is that anything you place online can be seen by anyone especially when it is posted on social media. Often when signing up for free online services you are automatically opted in to agreeing to give up your rights to your data and information. Applications like Snap Chat that tell users that they delete images after a certain time period actually do not[1]. Developers can access these images included location and time data as many devices by default geotag[2] images. Your daughter's mobile phone if Internet enabled may have location services switched on by default. Therefore, when a specific application is being used her location maybe being transmitted to a third party. It is advisable to discuss this with your daughter and work together to go through the settings on her phone so you both understand which application is using and possibly transmitting location data.



[1] http://www.thedrum.com/news/2014/05/09/snapchat-pictures-won-t-disappear-forever-and-data-collected-company-forced-admit (accessed 05/11/2015)
[2] https://en.wikipedia.org/wiki/Geotagging (accessed 05/11/2015)

Final comments

The contents of this document are a guide only and based on best practice and industry research. The nature of the online environment is constantly changing and therefore unforeseen services and technologies are regularly coming to the fore. The College cannot foresee all possible risks within our own network due to the nature of changing technologies however we mitigate these risks with internet filtering, virus scanning and internal policy and procedures. We also regularly conduct security audits of our network infrastructure to assist with early detection and further strengthen our IT security. However, once a device is no longer accessing our network we can no longer monitor internet traffic from a student's device. Therefore, it is important that parents play an active role in ensuring their daughters' online safety especially when they are not connected to our network.

If you have any questions please feel free to contact the IT Help desk on (03) 8862 1225 or email: support@genazzano.vic.edu.au or your daughter's homeroom teacher, team leader or alternatively the Director of Information and eLearning Technologies on (03) 8862 1261 or email Nathan.hutchings@genazzano.vic.edu.au or the Deputy Principal of Student Learning and Wellbeing on (03) 8862 1088 or email Lila.mcInerney@genazzano.vic.edu.au

Online resources

For further information please view the following websites:

https://www.esafety.gov.au/

https://www.scamwatch.gov.au/

https://www.cert.gov.au/about

https://www.communications.gov.au/what-we-do/internet/stay-smart-online

https://www.esmartschools.org.au/Pages/News.aspx