**STAFF USE ONLY**

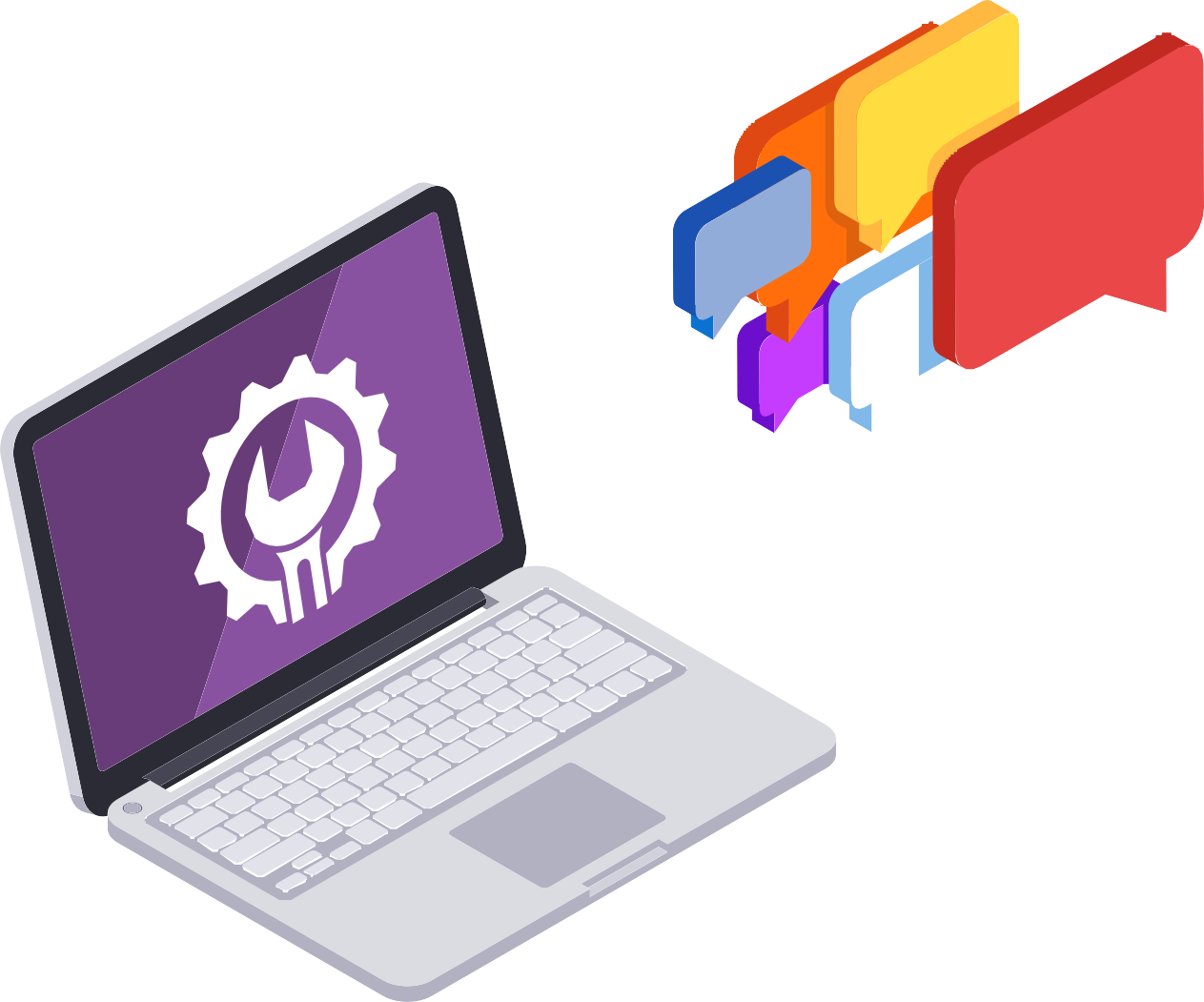
**Glossary of Online Safety Terminology**

***Contact us***

[**www.2simple.com.au**](http://www.2simple.com.au/)Tel:03 8001 5024

Raising Standards Through Creativity

[Email: support@2simple.com.au](mailto:support@2simple.com.au)



**Glossary of Online Safety Terminology**

**2018-2019**



**Digital Technologies Coordinator**

**Mr Teacher**





# Adware

**Chatroom**

A place on the internet where one or more people can chat.

Software application which displays adverts and can redirect searches.

# App

**Chatroulette**

Strangers interacting over text-chat and webcam. Lots of users post sexual images.

Short for application, typically used to refer to a piece of software designed for a particular purpose.

# Block

**Circumventor Sites**

Parallel websites that allow children to bypass sites their adults have blocked.

To block someone from contacting a user on a social media account for example.

# Blog/Blogging

**Cookie**

A small file which records a user’s personal preferences, shopping choices and other information.

An updated webpage containing users’ opinions/experiences/ observations.

# Bot

**Creeping**

Someone who follows someone

else’s social network profile closely.

A program that can do things without a user needing to give instructions. Many bots are malware.

# DHHS

**Cyberbullying**

The use of electronic communication to bully someone.

Tasked with Esafety and Child Protection.

**Fabotage**

Accessing someone else’s social media account without their knowledge and changing information on it.

**Firewall**

A security system that protects an internal network from an external one such as the internet.

**Gamer Tag**

An alter ego made from an alias, picture or avatar. Sometimes these are offensive.

**Griefer**

Someone who deliberately harasses online gamers during a gaming session.

**Decoy App**

These apps help children hide videos/images from their parents.

**Digital Footprint**

A person’s trail of data on the

internet that can last indefinitely.

**Emoji**

A small digital image used to express an idea, action or emotion

in electronic communication.

**Hacker**

A person who uses technology to gain unauthorised access to information.

**Grooming**

Someone who gains a child’s trust

for sexual exploitation or trafficking.

**Gamer**

A person who plays video games including online, likely with other online users.

**Identity Theft**

A crime where data is pieced together from an individual to impersonate them for financial gain.

**IM**

Instant message sent between users via the internet. These are very popular with younger generations.

**Netiquette**

Netiquette is the code of good behaviour on the internet. As the internet changes, so does netiquette.

**In-app purchasing**

Purchases of services or products are possible within some apps, such as game apps, and real money is required by them.

**Pharming**

Directing a user to a bogus website that pretends to be a real one in order to extract information from them.

**Incognito browsing**

This allows a user to browse the web without their history being recorded on their device.

**Phishing**

Emails which appear legitimate but are fake, and entice a recipient to share confidential information.

**ISP**

An internet service provider gives access to the internet (A sentence within this has been deleted as NA to Aus, can’t add a comment, hoping you’ll see the red!)

**Photo Sharing**

Some apps allow users to share images for a few seconds. These apps can be very damaging to children.

**Malware**

Software which is made to disrupt, damage or gain unauthorised access to a device.

**PM**

Private or personal message sent via the internet. Popular feature available on many social media platforms.

**Spam**

Messages sent to large numbers of users for the purpose of phishing, spreading malware and advertising.

**Virus**

A virus can do many things such as steal data and control a device.

They are often caught from email attachments and downloading from a website.

**Profile**

Often social media sites will allow users to create their own personal profiles which other users can see.

**Spyware**

Software that covertly collects information from a device without the device user’s permission.

**Selfie**

Self-portrait photo often taken at arm’s length using a Smartphone and uploaded to social media.

**Trojan**

A type of malware which is disguised as legitimate software and accesses confidential information.

**Sexting**

Sending and receiving sexually explicit images/videos via IM, text or social media.

**Troll**

A user who posts inflammatory messages typically on Social Media sites to upset others.

**Social Media**

Websites and applications where users can share content and participate in social networking.

**Video Hosting Sites**

Websites and apps which allow users to post and view video clips, like YouTube.