Online Safety & Content Filtering

Bolton Clarke

ABN	90 010 488 454
Address	Level 44 Musk Avenue Kelvin Grove 4059 QLD

How to contact us:

Phone	1300 306 331
Email	support@internet.boltonclarke.com.au
Website	www.boltonclarke.com.au/internet

Contents

Online safety and content filtering

This document is intended to provide useful information about online safety.

This document incorporates requirements under the *Online Safety Act 2021* (Cth), which sets out obligations for online service providers and users to promote a safer online environment. This includes tips on safeguarding your children from inappropriate websites and keeping your devices secure while connected to the internet.

Tips to keep your children safe when they are using the internet

You should always supervise your children when they are online. Anyone can access and insert content on the internet. And children can access inappropriate and undesirable content just as easily as they can access any other content. Adult supervision can help children avoid accessing inappropriate content. At the very least, a supervising adult can give context that minimises the harm that inappropriate and undesirable content can cause to children.

Tips to keep your children protected when they use the internet

- Talk with your children about what they do (and who they talk to) online. These online habits will change over time, so it's important you have these talks with your children on a regular basis.
- Put computers (and encourage the use of other connected devices) in communal spaces, such as the living or dining rooms, discouraging internet use in childrens' bedrooms.
- Have your child select appropriate "screen names" for their email address, instant messaging and gaming accounts.
- Consider using software designed to protect your child online, including but not limited to content filtering software, and security software.
- Talk to your child about "online etiquette" and what is acceptable behaviour online.

Rules you should set for your children when they use the internet and social media

- Never reveal any personal details that someone could use to trace them. This includes (but isn't limited to) their full name, address, phone number, and the name of their school or friends.
- If they find something they see online disturbing, they should let you, their teacher, or their friends know.
- If they see or hear their friends doing something inappropriate online, remind them of the right thing to do, and the dangers of not doing the right thing.
- Understand that not everything they read online is true. And people may not be who they say they are online. Be discerning and think for themselves on what they think is right or wrong.
- Let you know when they have made a new friend online.

Family Friendly Filters

What are filters?

Filters are typically computer programs that allow parents and IT system administrators to control what users can access online, through a list of blocked or allowed websites and programs.

For more information about filters and staying safe online, Visit the Office of the eSafety Commissioner website.

What are family friendly filter programs?

"Family Friendly Filters" are independently tested products aligned with eSafety's classification guidance. While filters are not legally mandatory for Internet Service Providers (ISPs), we support their availability and inform customers how to enable them.

ISPs are not required to monitor all traffic proactively, but we must comply with eSafety notices and relevant Online Safety Codes/Standards when illegal or restricted material is identified.

With the large number of filters available on the internet, it can be hard to choose the most appropriate one for your internet. To assist families in choosing a filter, Communications Alliance has created the family friendly filter program. The family friendly filter program is a list of filters pre-approved by Communications Alliance.

The filters on the family friendly filter list all meet criteria set out in the relevant industry code and are subject to rigorous vetting and testing by Communications Alliance.

There are 4 classification levels for certified filters.

- Class 3: Recommended for children under 10 years old.
- Class 2: Recommended for children between 10 and 15 years old.
- Class 1: Recommended for children over 15 years old.
- There are also filters that block websites on the eSafety commissioner's prohibited URL filter (PUF) list and are recommended for adults aged 18+.

For more information, visit the Communications Alliance's Friendly Family Filters page.

Important considerations about filtering software:

No filtering solution is foolproof. While the main advantage of filtering software is that it makes it harder to access inappropriate content, it also offers other useful features, such as restricting access to the computer and/or the internet to certain times.

When choosing a content filtering solution, keep in mind that websites are not the only online services.

Inappropriate content may exist on websites or online services that are not blocked by content filters, such as:

- File Transfer Protocols (FTP)
- Internet Relay Chat (IRC)
- Instant Messaging
- Emails
- News websites

- Online forums
- File sharing

Adult content is not the only concern for children using the internet. You should also warn your children about "stranger danger" when browsing and interacting with people online.

How filtering software works:

Filtering software works using one (or a combination of) the following three methods:

White lists:

A white list is a list of websites deemed "safe" for the general population. If a filter uses white listing, only websites on the white list are accessible, with all other websites and content blocked. Websites on a white list are generally educational or entertainment websites. White listed websites have been thoroughly vetted, and should never contain inappropriate or adult content of any kind.

The limitations of white lists:

- As anything not on the white list is blocked, a lot of useful content is restricted alongside inappropriate content - hindering users' online experience.
- Filtering companies may be impartial, and white list certain websites while blocking other websites that provide similar content.

Black lists:

A black list is a list of websites containing content the list's creator deems inappropriate. If a filter uses black listing, only websites on the black list are blocked, with the rest of the internet being accessible. Black lists are monitored regularly to ensure inappropriate content is added to the black list as soon as it appears on the internet.

Black lists are often categorised into themes, so users can choose the types of content they want to block.

The limitations of black lists:

- Black lists are generally not available to the public, as software providers keep their black lists secret to avoid it being duplicated by competitors.
- Due to the sheer volume of content on the internet, and the speed in which users can create new content, it is impossible to block every instance of inappropriate content through black listing it. Due in part to this, black list filters are often used in combination with keyword filtering (see below) so that demonstrably inappropriate content is blocked by default.
- Filtering companies may block websites that do not contain inappropriate content at their discretion, such as websites that criticise their software and websites that promote competitor offerings.

Keyword filtering

When a user accesses a web page, they are downloading that information. A keyword filter reads the page as it downloads it, searching for a list of key words that the software creator deems inappropriate. If the keyword filter discovers an inappropriate keyword, it either blocks access to the website or removes the inappropriate words from the version of the page displayed on the user's screen.

The major advantage of keyword filtering as it can scan the entire internet for inappropriate content, and doesn't require a list of websites.

The limitations of keyword filtering:

- Keyword filter is not able to discern otherwise appropriate words being used in an inappropriate context. Many words used in hate speech, or in content that is of a sexual, violent, or criminal nature are words that have a neutral meaning. Creators of inappropriate content take advantage of this and purposely appropriate words to ensure keyword filters don't block their content.
- Software that only removes inappropriate words from content will still display images and the rest of the website's content. This could lead to incomplete sentences that take on an entirely new meaning.
- Software that restricts access to the entire page based on it containing inappropriate keywords will lead to pages that use keywords in an appropriate context being blocked. This can be very frustrating for users trying to access content on the internet.
- Filtering companies may be biased when deciding which keywords to block. Like the other methods, this opens the door to anti-competitive practices, as the filtering software providers can add their competitors' names to the list of banned keywords.

Useful websites for more information

Stay Safe Online is an initiative by the Australian Government that aims to provide all Australian internet users with practical e-security tips to help them stay safe online. Its website contains information including (but not limited to):

- How to secure your computer and connected devices.
- Best practice tips for making online transactions.
- Tips to keep children safe online

Complaints

You can report any offensive or illegal online content including cyberbullying and image-based abuse to the Office of the eSafety Commissioner. Click here to access the eSafety Commissioner's content reporting form.

You can also report this content to our team by contacting us:

How to contact us:

Phone	1300 306 331
Email	support@internet.boltonclarke.com.au
Website	www.boltonclarke.com.au/intouch