



4 October 2021

[Redacted]

Tēnā koe [Redacted]

Thank you for your email of 14 September 2021 to the Ministry of Education, requesting the following information:

[Please provide each type of information in the form of an itemized list, with sub lists for examples if applicable.]

- 1. Any categories or specific websites that must be inaccessible to students in high schools, with at most two examples when possible, preferably in the form of hyperlinks/URLs*
- 2. Any categories or specific websites that may be blocked at the school's discretion*
- 3. Any tools (filter services, device administration tools, tools provided by another website or service) used to restrict internet access*

Your request has been considered under the Official Information Act 1982 (the Act).

Any categories or specific websites that *must* be inaccessible to students in high schools, with at most two examples when possible, preferably in the form of hyperlinks/URLs

Schools are responsible for providing a safe and secure environment for students and staff. Network for Learning (N4L) and the Ministry provide tools, support, and guidance, but ultimately each school board determines the settings for their own school. The only websites that must be blocked are defined by the Department of Internal Affairs' Digital Child Exploitation Filtering System. Further information is available at dia.govt.nz/Censorship-DCEFS.

Any categories or specific websites that may be blocked at the school's discretion

Schools can request to have specific URLs blocked. Schools may also choose to block a variety of categories of content. These categories are available at fortiguard.com/webfilter/categories.

Of the categories, 14 are blocked by default, but can be unblocked at a school's discretion. These relate to Child Abuse, Discrimination, Drug Abuse, Explicit Violence, Extremist Groups, Hacking, Illegal or Unethical, Proxy Avoidance, Other Adult Materials, Pornography, Peer-to-peer File Sharing, Malicious Websites, Phishing, and Spam URLs.

Any tools (filter services, device administration tools, tools provided by another website or service) used to restrict internet access.

As part of schools' internet connection, they are provided with a number of products and services, which are outlined at n4l.co.nz/managed-network/.

These include web filtering, firewall, DNS threat protection, and DDoS protection. Schools may also choose to use their own tools instead of, or in addition to the ones provided by N4L or the Ministry.

Please note, the Ministry now proactively publishes OIA responses on our website. As such, we may publish this response on our website after five working days. Your name and contact details will be removed.

Thank you again for your email. You have the right to ask an Ombudsman to review this decision. You can do this by writing to info@ombudsman.parliament.nz or Office of the Ombudsman, PO Box 10152, Wellington 6143.

Nāku noa, nā

A handwritten signature in black ink, appearing to read 'Scott Evans', with a stylized flourish at the end.

Scott Evans

Hautū Te Puna Hanganga, Matihiko | Infrastructure and Digital