Inland Revenue
Te Tari Taake

26OIA1746

18 December 2025

[redacted]

Dear [redacted]

Thank you for your request made under the Official Information Act 1982 (OIA), received on 5 December 2025. You requested the following:

> *Just wondering if the recent revelations that Jevon McSkimming used police work devices to access inappropriate material have prompted any actions to detect or prevent any kind of similar thing happening within your organisation?*
>
> *If so, what actions were taken?*

Information being released

Inland Revenue did not require any remedial action on monitoring and blocking of web content, as these capabilities have been in place for over six years.

All web traffic passes through a proxy that logs activity and controls access based on destination and user permissions. Attempts to disable or circumvent these controls would raise alarms to the Cyber Security team.

All web traffic requests are monitored, logged and retained. The Cyber Security team are alerted to attempts to access malicious sites or download malicious files. We apply preventative measures to limit the likelihood and impact of a security event, including restricting what websites staff can access and what staff can run on their machines.

Examples of site classifications that are blocked are listed below, all access to sites hosted using The Onion Router (TOR) are blocked:

- Other Adult Material
- Adult Themes
- Lingerie/Bikini
- Nudity
- Pornography
- Body Art
- Adult Sex Education
- K-12 Sex Education
- Other Drugs
- Gambling
- Other Illegal or Questionable

- Copyright Infringement
- Computer Hacking
- Questionable
- Profanity
- Mature Humour
- Anonymizer
- Online Chat
- Militancy/Hate and Extremism
- Tasteless
- Violence
- Weapons/Bombs
- Other Security
- Spyware/Adware
- Peer-to-Peer Site
- Social Networking Adult
- Remote Access Tools
- Newly Revived Domains

There are some Inland Revenue staff that require access to blocked material for work purposes. This access is permitted on a per-user basis and all access requests are logged. Their access is extended to permit only those categories required.

We do not permit Inland Revenue staff to install applications and browser extensions on their machines and prevent staff running unauthorised applications.

Publishing of OIA response

We intend to publish our response to your request on Inland Revenue's website (ird.govt.nz) as this information may be of interest to other members of the public. This letter, with your personal details removed, may be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the OIA's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of officials.

Thank you again for your request.

Yours sincerely

[redacted]

Jay Harris
Enterprise Leader – Information Security Office