MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

14 JUN 2017

Tony Meyer
fyi-request-5886-b953046f@requests.fyi.org.nz

Dear Tony

Thank you for your email dated 16 May 2017, to the Ministry of Education requesting the following information:

- *Please provide a copy of all information used in preparation of the "Urgent message from Ministry re WannaCry Ransomeware" email that was sent to schools on Monday the 15th of May, 2017, by Katrina Casey. This includes, but is not limited to, links to external sources of information, transcripts and summaries of discussions held in person and over audio media, internal advice, and advice received from external organisations.*

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

When preparing the message to schools, the Ministry relied on advice and guidance from CERT NZ and the National Cyber Security Centre. Both of these sources are publicly available at the following links:

- www.cert.govt.nz/businesses-and-individuals/recent-threats/alert-wannacry-ransomware-used-in-large-scale-international-attacks
- www.ncsc.govt.nz/newsroom/response-to-wannacry-global-ransomware-attack/

In addition, we also received brief advice from Network for Learning (N4L). This advice is summarised in the attached response which was provided to schools. I have attached this to the letter as **Appendix One**.

I trust the information provided is of assistance. Should you have any concerns with this response, I would encourage you to raise these with the Ministry. Alternatively, you are advised of your right to ask an Ombudsman to review this response. You can do this by writing to info@ombudsman.parliament.nz or Office of the Ombudsman, PO Box 10152, Wellington 6143.

Yours sincerely

Zoe Griffiths
Deputy Secretary
Business Enablement and Support

Urgent message from the Ministry of Education

The weekend media reported on a virus called WannaCry that is targeting computers of public organisations and private companies around the world.

Some schools may have been affected by this virus and we are writing to let you know what you should do and what we are doing to protect schools.

What is WannaCry?
WannaCry is malicious software that is taking control of computer systems by blocking access to a device, then demanding a ransom to unblock it. The virus, a type of ransomware, is largely being spread through emails when users click on links or attachments. Once a device is infected, the virus can quickly spread to all devices using your organisation's network.

You can read more about WannaCry in New Zealand from CERT (Computer Emergency Response Team), the lead government agency monitoring the situation and providing advice on cyber security threats.

How can you protect your school?

- **Keep your software up to date** - Ensure all devices connecting to your school's network are patched with the latest software updates. The virus is affecting devices using older versions of Microsoft Windows software (XP through to 2008 R2) by exploiting flaws in Microsoft Windows SMB Server. Turn automatic updates on wherever possible.

- **Be cautious of email attachments and links and remind your staff and students to do the same –** Everyone should apply a duty of care when clicking on links and opening email attachments. Note: these could be sent by people you know including students or staff who are unaware their devices have been infected.

- **Check CERT for updates** - Visit CERT's advisory page, which provides updates and guidance on cyber security threats: https://www.cert.govt.nz/it-specialists/advisories

- **Don't become complacent** and make sure back up files are kept off site

If your school has been infected, please report the incident to CERT immediately via its website: https://www.cert.govt.nz/businesses-and-individuals/report-an-issue/ and do not pay the ransom.

What is being done about it

N4L has blocked all traffic on the Managed Network that is attempting to connect to malicious IP addresses known to be associated with this virus. They are also actively monitoring the Managed Network to spot traffic patterns that may indicate suspicious activity from connected devices.

Web safety and cyber security requires continuous vigilance, education and duty of care around how devices are used. This virus may evolve and we will continue to work closely with our technology partner, Spark, and government agencies such as Ministry of Education, CERT and Netsafe to help schools keep their online environments safe for teaching and learning.