MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

[redacted]

7 NOV 2018

Dear [redacted]

On 3 October 2018, you emailed the Ministry requesting, under the Official Information Act 1982, the following information:

- *How many attempts were made to access websites classified as pornographic in 2017 at the Ministry.*
- *How many employees were warned or disciplined for accessing or attempting to access pornography websites in 2017.*

The Ministry allows staff to use the internet, including social media, for reasonable personal use. The Ministry defines 'reasonable' as not letting it interfere with work or productivity, and 'personal' as not part of the employee's job. Staff are responsible for limiting their personal internet usage to a reasonable amount, and managers are responsible for ensuring that they are doing this.

Staff using the internet are bound by the Public Service Code of Conduct issued by the State Services Commissioner, as well as the Ministry's own Code of Conduct, both of which require employees to be professional at all times. The Ministry's Code of Conduct requires employees to comply with all Ministry policies, including its Information Technology (IT) policy, Information Security Policy, the End User Policy and the Ministry's Internet Policy.

The Ministry's Information Security Policy requires employees to keep personal use of Ministry technology (including emails and internet use) within reasonable limits, and to never use Ministry information or technology in a way that violates New Zealand law.

A copy of the Ministry's intranet page advising of the Ministry's End User Security Policy, and details regarding the Ministry's Internet Policy are attached for your reference.

The Ministry's IT systems block a range of content including adult material such as references to nudity, sex, adult content and sex education. If a Ministry staff member attempts to access an inappropriate site containing any or a combination of the words listed above they are denied access to the site.

MSD National Office / 56 The Terrace / Off Aurora Tce / Wellington 6011
56 The Terrace / Aurora Tce / Wellington City 6011 / New Zealand
Fax: 04 918 0099 / **www.msd.govt.nz**

The Ministry only holds historical file logs for a maximum of three months due to the large number of these files, and the cost of holding them. Consequently, there are no log files available for the period that you have requested. The historical log files hold a significant amount of information around cyber incidents, which may include attempted access to inappropriate and adult content, cyber security threats and attacks, information and privacy breaches and data and information loss. It does not currently allow reporting to distinguish between the different types of incidents. As such, the Ministry is unable to provide you with the number of attempts Ministry staff have made to access websites classified as pornographic in 2017 as it is not held by the Ministry and there are no grounds to believe that the information is held by another department or Minister of the Crown or organisation. Your request for this information is refused under section 18(g) of the Official Information Act.

The Ministry is only aware of one case that was raised during 2017 regarding inappropriate access to a pornographic website, however following investigation, this was not substantiated.

The principles and purposes of the Official Information Act 1982 under which you made your request are:

- to create greater openness and transparency about the plans, work and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

This Ministry fully supports those principles and purposes. The Ministry therefore intends to make the information contained in this letter and any attached documents available to the wider public shortly. The Ministry will do this by publishing this letter and attachments on the Ministry of Social Development's website. Your personal details will be deleted and the Ministry will not publish any information that would identify you as the person who requested the information.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with this response regarding Ministry staff accessing pornographic sites in 2017, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Yours sincerely

p.p. Stephen Crombie
Deputy Chief Executive, Corporate Solutions

End User Security Policy

The End User IT Security Policy provides general guidance to Ministry staff about IT security concerns that all staff need to be aware of while working for the Ministry. It does not speak to any aspect in depth, but additional, more detailed information is available in other specialised policies. It complements the Ministry Code of Conduct.

On this Page:

Overview

The Ministry's Information Communications Technology (ICT) systems hold sensitive Ministry and client information. Ministry employees are expected to help the Ministry keep the information as well as the ICT infrastructure safe. To clarify these expectations, the Ministry has produced a series of ICT Security policies. These policies intend to:

reduce the risk of MSD computer hardware, systems and assets being misused;
ensure compliance with legislative, statutory and contractual requirements;
ensure business continuity by complying with best practice; and
ensure the confidentiality, availability, integrity and accuracy of the information held electronically by the Ministry.

Scope

This policy applies to all Ministry employees and vendors, contractors, consultants and agents of the Ministry that have access to or use of the Ministry's ICT systems. Any references to "staff members", "employees", or "users" within this document should be read as including everybody within this definition of scope.

Deference to the "Codes of Conduct"

This policy document is a Ministry policy and therefore defers to the Ministry Code of Conduct and the State Services Standards of Integrity and Conduct. The Codes [http://doogle/business-groups/organisational-solutions/who-we-are/it/it-performance-and-strategy/it-security/end-user-security-policy.html#Definitions23] take precedence in all incidences of any conflict between the rights and obligations described in this policy document and either of the Codes.

Precedence over other policy statements

This policy document replaces, and takes precedence over all existing policy addressing the same content, that existed prior to the effective date of this policy (with the exception of the Codes).

Logoff from Workstations

All staff members must log off from their workstation each night. This will ensure automatic updates can take place. (note - shutting down is not required)

Keep Smartcard Safe

Staff members' smart cards must be securely stored when not in use.

Inappropriate Material in E-mail

No staff member may create, attach, or include e-mail content that could be seen as inappropriate or offensive. If staff members receive inappropriate e-mails, they should report this to their manager.

Personal Use of E-mail

Staff members are only allowed the moderate personal use of Ministry e-mail provided that it does not expose the Ministry to any liability or put the reputation of the Ministry at risk.

Personal Use of Internet Access

Staff members are only allowed the moderate personal use of Internet access provided that it does not expose the Ministry to any liability or put the reputation of the Ministry at risk.

Report Computer-related Security Incident

All staff members should report any computer-related security incidents to their manager and MSD Service Desk [http://doogle/helping-you/msd-service-desk/contact-us.html] . This could include:

loss or damage of computer equipment
receiving computer viruses
any unauthorised access to Ministry computers
suspected compromise of the privacy of Ministry data.

Downloading Material in Violation of Copyright

Staff members must not download or use any online material protected by copyright without permission of the copyright holder.

Internet Sites with Offensive Material

Staff members must not knowingly visit Internet sites that contain material that could reasonably be seen as inappropriate or offensive.

Monitoring Internet and E-mail Trends

The Ministry monitors e-mail and internet use trends and may provide findings to any manager where use is a concern.

Loading of Unauthorised Software

Staff members must not introduce or install any unauthorised software onto workstations.

Password Compromise

Where passwords are known or suspected to be compromised, the affected password must be changed immediately.

Writing down Passwords

When a user writes down a password (whether hard copy or electronically) it must be stored securely. Papers containing passwords must be discarded securely.

Secret Passwords

Staff members must keep their passwords secret and must not share passwords.

Personal Use of Workstations

Staff members are entitled to reasonable use of Ministry workstations for personal use but any personal data stored on Ministry workstations is stored at the owner's risk. The Ministry is entitled to access and review all data stored on its systems or workstations and is not responsible for any loss or disclosure of stored personal data.

Encryption of Removable Media Data

The Ministry requires that all Ministry information, which is physically transported using removable media, must be encrypted in accordance with Ministry standards.

Removable Media for Data Transport

Removable media may be used for temporary storage of MSD information, for example when the data is being transported between places of work. Temporary storage specifically excludes the use of removable media for backup purposes.

Removable Media Limitations

When using Universal Serial Bus (USB) attached devices to transport Ministry information, Ministry approved, hardware encrypted devices must be used. Such devices must be purchased through IT Customer Services. Removable disks, e.g. DVD's and CD's may only be used under approval from the CIO.

Enforcement

If the principles set out in this policy statement are not met, staff members may be considered in breach of the policy. Conduct that is considered unacceptable by the Ministry is likely to result in disciplinary action against the staff member concerned. Such disciplinary action may include dismissal.

Definitions

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/ or unusable to anyone without the tools/ information needed to reverse the encryption process.

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes, but is not limited to flash memory devices such as thumb drives, cameras, MP3 players, and PDAs; removable hard drives (including hard drive-based MP3 players), optical disks such as CD and DVD disks, and floppy disks.

Content owner: Process Improvement **Last updated:** 22 August 2018

Using the internet

Internet access is available to approved users only. It is a business tool that supports work activities. When using the internet you must not participate in any activity that violates the Ministry's Code of Conduct and/or the Ministry's computer use or business security policies. Users must comply with this policy.

On this Page:

Permitted internet use

Only authorised people may access the internet. Any other private connection to a global network from an MSD PC/laptop is not allowed. Users must ensure they have the appropriate delegated financial authority before accessing user-pays internet services.

If you are an authorised user, you may use the internet:

to conduct research and investigation as part of your job

to retrieve news stories and other information of interest and relevance to the Ministry and/or the performance of your duties

for professional development activities, such as maintaining currency with issues in a field of knowledge. This includes personal development activity, such as university associations and professional societies.

Contact IT Operations if you need an executable file installed. Executable files may also be supplied from authorised vendors as ZIP files, which must be scanned for viruses and loaded by IT Operations.

You may access the World Wide Web for reasonable personal purposes providing you do not use it inappropriately. Keep the amount of personal time spent on the internet to a minimum.

> Applying for internet access [http://doogle/resources/helping-staff/forms-templates/msd-service-desk/access-requests.html#WirelessInternetAccessRequest15]

Inappropriate internet use

You may not download, send, forward or store large quantities (several megabytes) of software, graphical and other forms of information from the internet for personal or inappropriate use. Downloading commercial software in violation of its copyright is prohibited. This includes executable files, movie files and screen savers.

You may not use the internet to:

sell or otherwise disclose client information for personal gain

engage in newsgroup postings or chat groups for private purposes

visit sites that contain material that any reasonable person would consider obscene, objectionable, or offensive

subscribe to any website for personal use without permission from your manager

register Ministry addresses on any website as a forwarding address for any inappropriate material

engage in any form of gambling.

Your internet use must not interfere with the work of your business unit, or cost the Ministry an unacceptable amount of money.

You must not knowingly:

interfere with or disrupt any network or information service, any equipment or anyone using that equipment

propagate a virus, Trojan Horse, trap-door, back-door or any other malicious program code

print and/or forward material that is obscene, objectionable, or likely to be offensive

make or post indecent remarks and proposals

post any users' personal details for non-business purposes to any internet site, including their email address

use the internet at work for the purpose of private trading purposes

engage in any activity that violates New Zealand law or the Ministry's policies.

These lists are not exhaustive. If you require further clarification discuss your intended use with your manager. If you use the internet inappropriately, disciplinary action may be taken.

State Services Code of Conduct [http://www.ssc.govt.nz/display/document.asp?docid=7193]

The Ministry's Code of Conduct [http://doogle/working-here/working-for-us/standards-of-behaviour/index.html]

Objectionable material is as defined in Section 3 of the Films, Videos and Publications Classification Act 1993.

All of the conditions set out under permitted and inappropriate email use also apply to internet use.

Films, Videos and Publications Classification Act 1993 [http://www.legislation.co.nz/act/public/1993/0094/latest/DLM312895.html?search=ts_act_Films%2BVideos&sr=1]

Information about Email use [http://doogle/resources/helping-staff/policies-standards/business-security/computer-use/using-email.html]

Posting information

Users may not participate in any email forum or post information onto any newsgroup without the prior permission of their immediate manager. Any material posted on the internet, including email forums and newsgroups, that identifies the Ministry as the originating site must:

be approved by the user's manager

be factually correct

not be defamatory or contain anything that is offensive, abusive, threatening, or objectionable.

Content owner: Communications and Engagement **Last updated:** 30 August 2016