

2 May 2018

Emailed to: fyi-request-7553-051f6b69@requests.fyi.org.nz

Dear Miss Forest

**Response to Official Information Act request : Digital Service Delivery Channel
(Our Ref: OPC/2839)**

We refer to your Official Information Act request of 3 April 2018. Your request referred to information from the financial year 2017. The Privacy Commissioner's financial year ends 30 June and the answers given in response to your request are from the period 1 July 2016 to 30 June 2017. Using our financial year also facilitates you comparing information published in our annual reports for that and previous years.

The online lodgement of complaints was introduced in 2015, with the web server on which complaints are lodged hosted by a third party provider. We included end-to-end encryption to securely transmit a submission to us ensuring that the third party provider could not access the information it contained. You will note on our website that we also provide a recommendation to users to lodge their complaints only from a trusted computer and not to use public wi-fi.

In your request we note that you characterise emails we receive from correspondents but not via the web forms as "insecure." We do not agree with that characterisation. They do not have encryption applied as that would be impractical in providing the service expected by our customers. In addition we ask complainants and respondents whether they wish to continue to use emails for future correspondence between them and our Office. They make the choice. Though we have well developed controls and security within our IT infrastructure, we cannot manage what steps users have taken to protect their own systems.

1) *How many privacy complaints did you receive in total FY2017?*

726 complaints received and investigated

2) *When does a complaint become an enquiry and other way around given complaints are labelled as enquiries if there is a difference between the two?*

We refer you to page 23 of the Procedures Manual: Dispute Resolution and Investigations.

<https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/2018-01-final-Procedures-Manual-Disputes-Resolution-section.pdf>

3) *What is the difference between a complaint and an enquiry if any in respect of 2)*

We refer you to page 23 of the Procedures Manual: Dispute Resolution and Investigations.

<https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/2018-01-final-Procedures-Manual-Disputes-Resolution-section.pdf>

4) *How many complaints did you receive originally submitted via the secure web form within your website within FY2017?*

340 were noted as received via the secure web form within our website

5) *How many complaints did you receive originally submitted via e-mail within FY2017?*

176 were noted as received by email other than via the secure web form within our website

6) *How long the secure web form channel submission has been live?*

The secure web form went live in April 2015

7) *How long the e-mail channel submission has been live?*

We do not have an exact date but for at least the past 10 years the Office has accepted complaints by email sent direct to us by potential complainants. In this time we have never experienced a security breach or data loss from an email correspondence from a malicious or third party incursion.

8) *Was any of the technical service delivery elements regarding handling complaints subjected to a review, audit or such and if any please provide a copy technical elements are your website secure form, complaint data handling and e-mail service delivery.*

We would apply our guidance regarding Data breaches as provided on our website. <https://privacy.org.nz/data-breaches/introduction/>

Oversight would be provided by the appropriate senior manager with the Privacy Commissioner remaining fully informed.

9) *If a member of a public has alerted you to potential complaint data breach, what actions do you take and who provides oversight to this?*

The matter would be referred to our technical service provider of the process in question, with oversight provided by the General Manager of the Office of the Privacy Commissioner, with the Privacy Commissioner remaining fully informed.

11) *How many alerts from the members of public related to 9) and 10) you received during FY2017?*

None from members of the public. We did identify a potential breach internally when an email was sent to a wrong email address. It was subsequently determined that no such email address actually existed

12) *How do you evaluate potential or materialised data breaches on your complaint data that you hold, have sent or received? e.g. do you have a policy*

We would apply our guidance regarding Data breaches as provided on our website.

<https://privacy.org.nz/data-breaches/introduction/>

13) *When you have to forward or transfer the data from or to another commissioner how do you handle this? e.g. do you have a policy*

All records are held in our electronic document records management system (Objective). We do not transfer the data across the Office we send a link to the data in Objective.

If data is referred to another government agency it is sent using Seemail, and secure email product used by government agencies.

14) *What technical delivery is used for the transfer in respect of 13) e.g. e-mail or "iron key" process using USB keys (MSD uses this) or physical paper form?*

All records are held in our electronic document records management system (Objective). We do not transfer the data across the Office we send a link to the data in Objective.

The Office does have "iron keys" if required, to transfer data outside of Objective should that be necessary.

15) *Has the transfer process from or to another body been formally designed and reviewed or is this up to the individual officer involved?*

Objective is an industry leader in electronic document management and is used extensively in New Zealand by government organisations.

16) *If you notice ad-hoc process created by individual officers relating to technical aspects of handling data and there is concern from a member public, is there any policy that addresses this?*

We do not have a formal policy, but the practice would be for the manager of the staff member involved to investigate the concern.

17) *During handling a complaint you need information from the complainant, complained party or a 3rd party, what data transfer method do you use or is this up to individual officer case-by-case basis?*

The data is transferred in the method requested by the individual parties to the complaint.

18) *Did the officers handling the complaints receive information security related training during FY2017.*

As part of induction all staff are made aware of the secrecy obligations under section 116 of the Privacy Act and sign a declaration acknowledging their understanding of these obligations.

19) *Is there any information security policy related to handling complaints data? please provide a copy.*

We refer you to page 14 of the Procedures Manual: Dispute Resolution and Investigations as relates to secrecy and privileged information.

<https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/2018-01-final-Procedures-Manual-Disputes-Resolution-section.pdf>

I would like also to request the below information regarding the data as part of the complaints;

a) How long has the current practice of copying the whole complaint data originally submitted and trusted via a secure https form into e-mail has taken place?

Our practice is to send the email to the address from which the email was received by the Office. The security around the lodgement process is to prevent a third party responsible for the administration of that process cannot access the information. Post receipt any information exchange is between our office and the complainant involved.

b) Do you classify the data within complaints? e.g. as containing sensitive or medical data etc.

No, unless there is a security classification of the information contained in the complaint or access to the complaint data is to be restricted to specific persons in the Office. Our records system allows for restricted access to be included if required.

c) Are there any retention rules applied and what are these?

All records are retained within Objective as official records.

d) Is the complaint data stored in any searchable database?

All records are held in our electronic document records management system (Objective). The database is searchable by authorised users of Objective.

e) Where else the complaint data is stored e.g. in e-mail inboxes/outboxes?

The policy and practice of the Office is to store information in Objective and not in email software.

f) If you receive a letter of complaint in paper form via post, do you digitize this?

Yes.

g) If the complaint in f) is digitized is it a subject of same treatment as originally digitally received complaint?

Yes.

h) Can I have a copy of your policy regarding of using e-mail and complaint data protection

Yes, copy attached.

i) Does the secure web complaint form from the front-end web server transmit the complaint data to an internal e-mail address or to a secure database or such and is it a secure channel and what internet protocols are used?

Complaints are automatically encrypted at time of submission on the website and emailed over the internet to a single, designated mailbox on the Privacy Commissioner's Exchange server.

The encrypted submission is automatically decrypted on receipt in the designated mailbox on the Privacy Commissioner's Exchange server.

While it is the intention to not store data on the website, the encrypted email submission may be held in queue on the website until it can be transmitted in the event that the Exchange Server cannot be reached.

Peer to peer PGP encryption is used as the internet protocol.

j) Are there e-mail forwarders in use where the complaint data gets copied incidentally to an officers personal e-mail for example.

No, we send the reference link to the record in Objective via email. Staff do not forward official records to personal emails.

k) Do you have rules with your e-mail provider in place that no e-mail forwarding in respect of j) can happen.

Yes.

l) Can you audit who and when has inspected data from individual data, e.g, if you are in possession of health information or other sensitive data as part of the complaint.

Yes. Included in our electronic document management system (Objective) is an audit capability which records any actions regarding access and use of any record.

m) Do you have any restrictions what data and when can individual officers access to e.g. only the cases they are handling.


No.

n) Do you encrypt any of the complaint data you handle by practice or is this up to the individual officers on case by case basis?

No, the data is secure within Objective.

You have the right to ask the Ombudsman to investigate and review my decision on your request.

Yours sincerely



Gary Bulog
General Manager

Encl. OPC email policy



Privacy Commissioner
Te Mana Matapono Matatapu

Office of the Privacy Commissioner

Internet and E-Mail Policy

August 2012

Internet and E-Mail Policy

Purpose of this Policy

To provide guidelines as to acceptable and/or unacceptable use of the Internet, e-mail and any allied services made available by the Office of the Privacy Commissioner.

Scope of this Policy

This policy applies to all staff of the Office of the Privacy Commissioner including contract staff and visitors lawfully on the premises, and any other persons having access to services made available by or through the network operated by the Office. All such persons are to agree to the conditions of this policy before given access to the computer system.

This policy also applies to users who may have access to the network from their homes.

POLICY

1. General Statement

- a) The computer network, access to the Internet, e-mail system and any allied services remain the property of the Office of the Privacy Commissioner and are valuable and critical components of our core business process. Internet and e-mail facilities are provided for staff to assist them in undertaking their job responsibilities.
- b) All Information and/or material entered or stored using the Office's computer facilities remain the property of the Office of the Privacy Commissioner.
- c) Staff should be constantly aware of the risk a virus can create on the Office's system. Any suspicious e-mail or electronic process must be deleted from the 'inbox' and the 'deleted' box without any action to open the document. Any suspicious item must be reported to the General Manager, or the Executive Secretaries if he is unavailable.
- d) Antivirus software installed on the network must be enabled at all times to ensure Internet and e-mail services have active antivirus protection operating.
- e) It is the Offices' practice that the General Manager will receive reports on a regular basis of how staff are using the Internet including the type of sites being visited.

2. Guidelines for use of the Internet and E-mail

- a) All users should be aware that Internet and e-mail transmissions can never be assured as being private or secure. Information can easily be sent to the wrong person or organisation. E-mails can be copied and used maliciously. What you may consider is 'personal' could become public on the Internet and e-mail.
- b) Internet and e-mail should be used for bona fide Office purposes only. (limited personal use of e-mail is permitted refer 2(e)) Use of these facilities is limited to the Privacy Commissioner, employees of the Office, authorised temporary workers or authorised contractors only.
- c) Users are responsible for the security of their individual passwords. Do not reveal your password to any other person unless agreed to by your manager. Passwords are to be changed when prompted by the computer system.
- d) Computers should be logged off or password protected when the computer is unattended.
- e) Limited personal use of e-mail is allowed within reason, but should not interfere with or be in conflict with business use nor breach of this policy. Personal use does not include access to other Internet or e-mail providers such as 'Hotmail' or other personal e-mail mailboxes. (This is a security measure)

Staff should exercise good judgment regarding the reasonableness of their personal use of the e-mail system. Staff may post personal messages to the network group but they are required to keep such messages concise for reasons of efficiency and courtesy.

Personal access to the Internet is to be undertaken at a time and in a manner that does not intrude upon work time and work responsibilities and must not interfere with the Office's functions, operations and objectives.

- f) The professional standards expected for all other forms of communication applies to e-mail messages. Language and tone will be professional, efficient and courteous. Incoming messages should be reviewed regularly (normally a minimum of three times a day) with timely relevant responses. Messages should only be directed to those with an interest or need to know. Staff should not enter into prolonged personal messages nor should it be used to distort current staff member's reporting lines.
- g) An automated "out-of-office" message should be set up during any absence from the Office for longer than 72 hours. For extended periods of leave the General Manager can, if requested by you, block messages from distribution groups reaching your Inbox during your absence, and so reduce the numbers of emails required to be reviewed upon your return.

- h) To prevent the accumulation of unnecessary e-mail messages, the contents of both “in-box” and “sent” mail folders should be reviewed and deleted monthly as appropriate for your individual needs and circumstances.

3. Specific Prohibitions

It is prohibited (and may constitute serious misconduct):–

- a) to use Internet and e-mail facilities to transmit or download obscene, objectionable or offensive material either internally or externally. This includes pornographic material, offensive language, any jokes, messages or other material which may be in breach of the Privacy Act or would create an intimidating or hostile work environment.
- b) to download software or attachments from e-mail or the Internet that have the potential to compromise the Office’s computer network. This includes ‘mail-bombing’, defined as either e-mailing copies of a single message to many account holders or sending large or multiple messages to a single user with malicious intent.
- c) to download or participate in any electronic use of games, videos and other software.
- d) to infringe copyright, trademarks and other intellectual property rights, perpetrate fraud or distribute defamatory statements or otherwise inflict harm on third parties.
- e) to receive or send unsolicited advertising mailings, whether commercial or informational, unless they are a part of Office communications and approved by the Assistant Commissioner Policy and Legal,.
- f) to use the Office’s Internet or e-mail facilities to set up personal businesses or circulate chain letters or other non work related material.
- g) to use the passwords or mailboxes of other persons.
- h) to buy and sell goods and services without prior managerial authorisation.
- i) to forward or disclose confidential Office information through messages to external locations.
- j) to send e-mails which:
- spread gossip, deride or criticise other staff, management or the work of the Office
 - express political views, or other potentially contentious or sensitive issues, which are not part of official duties and has the possibility to embarrass the Office

- send passwords or usernames
- make available confidential information held by the Office

It is the Office's practice that the General Manager will be notified immediately should an 'offensive' Internet site be visited and the General Manager will require reasons for that staff member accessing such a site. Staff are required to inform the General Manager immediately should they visit an 'offensive' site by accident or as a part of a complaint investigation or research project being undertaken.

4. Consequences of breach of the Office's Policy

A breach of this policy would be considered to be serious. Should a breach of the Office's Internet and e-mail policy occur, disciplinary action may be taken according to the seriousness of the breach.

Disciplinary action may result in a range of possible outcomes up to and including summary dismissal.

5. Monitoring Internet and E-mail usage

Although the Office, through specialised software, monitors staff use of Internet and e-mail facilities, it also places a high value on privacy, trust and individual responsibility. The Office retains the right to access electronic messages, files or data of all staff which are stored on its computer system to determine if there is a breach of this policy.

In the event that it is necessary to carry out an investigation or audit of Internet and e-mail usage, the Office will advise affected staff accordingly.

6. Declaration

All persons who use the Internet and e-mail services provided by the Office must be familiar with this policy and will sign a declaration in the attached format.



Privacy Commissioner
Te Mana Matapono Matatapu

Declaration for the use of Internet and E-mail Services

I have read and agree with the conditions of use explained in the Internet and E-mail Policy of the Office of the Privacy Commissioner.

I understand that breach of any of these conditions will result in my Manager being notified and depending upon the seriousness of the breach, further action may be taken in accordance with the provisions of that policy.

Name

Signed

Date