



**BAY OF PLENTY**  
DISTRICT HEALTH BOARD  
HAUORA A TOI

## OIA REQUEST

**Received:** 25 February 2021  
**Due:** 24 March 2021  
**Response Date:** 12 March 2021  
**Subject:** Unauthorised Use/Disclosure of Personal Information

Cnr Clarke St & 20th Ave  
Private Bag 12024  
Tauranga 3143  
New Zealand  
Phone 07 579 8000

---

In response to your request under the Official Information Act, please find our response below:

### Request

What policies, procedures and agreements does the Bay Of Plenty District Health Board have in place to prevent unauthorized use or disclosure of personal information that it provides to agencies or organizations that are contracted to the DHB or acting on its behalf eg NGO sector, other agencies.

### Response

Our agreements with providers have specific clauses on confidentiality. For example:

**B35.5** Each of us will ensure all Confidential Information is kept secure and is subject to appropriate security and user authorisation procedures and audits.

Please see Policies 2.6.1 Management and Use of Information and 2.6.1 Protocol 2 Acceptable Use below.


Please note that this response may be published on our website as part of our proactive release practice.

Yours sincerely

**DEBBIE BROWN**

Senior Advisor Governance and Quality



	Policy Name: <b>Management and Use of Information</b>	Policy No: 2.6.1
	File Name: 2.6.1	Issue Date: Feb 2021 Review Date: Feb 2022

## MANAGEMENT AND USE OF INFORMATION

### POLICY STATEMENT

It is the Bay of Plenty District Health Board's (BOPDHB) aim that all information and records should be appropriately obtained, and managed to ensure their accuracy, timeliness, completeness and protection.

### EXCLUSIONS

There are no exclusions.

### REFERENCES

- The Privacy Act 2020
- The Health Information Privacy Code 2020
- The Public Records Act 2005
- The Official Information Act 1982
- National Archives of New Zealand various standards for the Creation, Management, Storage and Destruction of Public Records and Archives
- New Zealand Information Security Manual (NZISM)
- Security in the Government Sector (SIGS)

### ASSOCIATED DOCUMENTS

- [Bay of Plenty District Health Board policy 0.0 Glossary of Terms / Definitions](#)
- [Bay of Plenty District Health Board policy 2.6.1 protocol 1 Management of Information](#)
- [Bay of Plenty District Health Board policy 2.6.1 protocol 2 Acceptable Use](#)
- [Bay of Plenty District Health Board policy 2.6.2 Digital Communication](#)
- [Bay of Plenty District Health Board policy 2.6.3 Software and Technology Management](#)
- [Bay of Plenty District Health Board policy 2.6.4 Access Control](#)
- [Bay of Plenty District Health Board policy 2.6.5 IT Network Security](#)
- [Bay of Plenty District Health Board policy 2.6.6 Mobile Device Management](#)
- [Bay of Plenty District Health Board policy 2.5.1 Health Information Privacy](#)
- [Bay of Plenty District Health Board policy 2.5.2 Health Records Management](#)
- [Bay of Plenty District Health Board policy 2.5.2 protocol 3 Access to Personal Health Information from a Health Record](#)
- [Bay of Plenty District Health Board policy 2.5.2 protocol 5 Retention and Destruction of Inactive Health Information](#)
- [Bay of Plenty District Health Board policy 3.50.13 Investigation and Disciplinary](#)
- [Bay of Plenty District Health Board policy 3.50.02 protocol 5 Employee Records](#)

Manual Name: Organisation	Page 1 of 1	NOTE: The electronic version of this document is the most current. Any printed copy cannot be assumed to be the current version.
Section Name: Info Technology	Version No: 5	
Policy Steward: GM, Corporate Services	Authorised by: Chief Executive Officer	

**PURPOSE**

The purpose of this protocol is to define the acceptable activities and behaviours when using Bay of Plenty District Health Board (BOPDHB) owned or supplied information systems and technology. It is intended to:

- ensure BOPDHB information systems and technology are used appropriately in serving the interests of BOPDHB, our clients and customers in the course of normal operations.
- protect BOPDHB, its staff and its patients from inappropriate use by individuals, either knowingly or unknowingly. Inappropriate use exposes BOPDHB to risks including malware attacks, compromised systems and services, reputation damage and legal challenge.

**STANDARDS TO BE MET**

**1. General**

- 1.1. BOPDHB reserves the right to set, review and publish policies, protocols and standards of use of its information system and technology assets. All staff, contractors and third-party users must comply with these when using DHB information systems and technology.
- 1.2. BOPDHB’s staff, contractors or contracted third parties, are responsible for their use of BOPDHB Information Systems and Technology and for exercising good judgement regarding the appropriateness of that use.
- 1.3. For security, network maintenance and system performance purposes, the DHB reserves the right to monitor DHB information systems and network traffic on either a periodic or ad hoc basis to ensure compliance with this policy.

**2. Acceptable Use**

- 2.1 BOPDHB’s Information System and Technology assets should only be used as part of the normal execution of an employee’s responsibilities and in a manner that is consistent with the Bay of Plenty District Health Board’s values and standards of conduct.
- 2.2 Staff use of BOPDHB’s Information System and Technology assets for purposes that support the goals and objectives of the Bay of Plenty District Health Board is permitted and encouraged.

**3. Unacceptable Use**

- 3.1. Staff must not use the BOPDHB’s information systems and technology for inappropriate or unacceptable uses which includes, but is not limited to:
  - a) Unauthorised copying of material subject to copyright laws including activities such as digitisation and distribution of images from copyrighted publications and films, copyrighted music, and the installation of any copyrighted software for which BOPDHB or the end user does not have an active license.
  - b) Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email spam etc.).
  - c) Using BOPDHB information systems and technology to create, procure, store or transmit material that is obscene, objectionable, likely to be offensive or which contains “adult content”.

Issue Date: Feb 2021	Page 1 of 2	NOTE: The electronic version of this document is the most current. Any printed copy cannot be assumed to be the current version.
Review Date: Feb 2022	Version No: 4	
Protocol Steward: IT Manager	Authorised by: GM, Corporate Services	

- d) Using BOPDHB information systems and technology to communicate discriminatory, disparaging, defamatory or harassing comments or otherwise engaging in any conduct prohibited by BOPDHB's policies or the Shared Expectations (Code of Conduct).
- e) Making bogus or fraudulent offers of products, items, or services originating from any BOPDHB account.
- f) Effecting security breaches or unauthorised disruptions of network communication including, but not limited to:
  - i. accessing data where the user is not an intended recipient,
  - ii. logging into a server or account that the user is not authorised to access,
  - iii. circumventing DHB approved user security processes,
  - iv. operating any unauthorised security scanning device or software,
  - v. using any program / script / command, or sending messages of any kind, with the intent to interfere with, or disable, the activities of other users.
- g) Engaging in unauthorised electronic communication which may harm or tarnish the image, reputation and/or goodwill of BOPDHB and/or any of its employees.
- h) Revealing your user logins to others or allowing use of your login by others. This includes family and other household members when work is being done at home.

3.2 Staff must not attempt to bypass BOPDHB security and/or privacy controls and mechanisms

#### 4. Non-Compliance With Protocol Standards

Failure to comply with this Protocol may result in the suspension of all access privileges and could lead to disciplinary action up to and including dismissal from employment, or, in the case of contractors, termination of contract.

#### ASSOCIATED DOCUMENTS

- [Bay of Plenty District Health Board policy 0.0 Glossary of Terms / Definitions](#)
- [Bay of Plenty District Health Board policy 2.6.1 Management and Use of Information](#)
- [Bay of Plenty District Health Board policy 2.6.1 protocol 1 Management of Information](#)
- [Bay of Plenty District Health Board policy 2.6.2 Digital Communication](#)
- [Bay of Plenty District Health Board policy 2.6.3 Software and Technology Management](#)
- [Bay of Plenty District Health Board policy 2.6.4 Access Control](#)
- [Bay of Plenty District Health Board policy 2.6.5 IT Network Security](#)
- [Bay of Plenty District Health Board policy 2.6.6 Mobile Device Management](#)
- [Bay of Plenty District Health Board policy 3.50.13 Investigation and Disciplinary](#)

Issue Date: Feb 2021	Page 2 of 2	NOTE: The electronic version of this document is the most current. Any printed copy cannot be assumed to be the current version.
Review Date: Feb 2022	Version No: 4	
Protocol Steward: IT Manager	Authorised by: GM, Corporate Services	