PURPOSE

This protocol supports Bay of Plenty District Health Board (BOPDHB) policy 2.6.2 and sets the standards expected from staff when accessing the internet via BOPDHB-computers and / or network resources.

STANDARDS TO BE MET

1. General Rules

1.1 Staff use of the Internet for business purposes that supports the goals and objectives of the BOPDHB is permitted and encouraged.

1.2 The Internet should only be used as part of the normal execution of an employee's responsibilities and in a manner that is consistent with the BOPDHB standards of conduct.

1.3 Information communicated via the Internet should be subject to the same protocols and publication standards as traditional means of communication (e.g. approval by Manager, review by appropriate higher levels).

2. Access Rules

2.1 Internet access is to be controlled via individual accounts and passwords. Employees must not share passwords, user identification or other secure information. Sharing of logins puts the login owner at risk if their login is used inappropriately by another user. BOPDHB reserves the right to withdraw system access from users who persist in sharing their passwords and logins.

2.2 Group or shared login accounts are not to have general access to the internet. Where group or shared logins are required to enable accessing of reference sites used in clinical processes, the Chief Information Officer (CIO), Information Management or authorised delegate may authorise access to those identified sites.

2.3 BOPDHB reserves the right to monitor, restrict, suspend or terminate a user's internet access to any site, upon authorisation by the CIO, Information Management or authorised delegate.

3. Appropriate Use

3.1 Staff using the internet must ensure that the use they make is appropriate. This includes but is not limited to:

a) Conducting research and investigation in support of service planning, service provision and / or output delivery. Note, however, that this does not provide staff with a right to access sites that are deemed inappropriate under clause 7 below.
b) Communication and information exchange with Government agencies and other organisations as required by business (if relevant).
c) Retrieving news stories or other information of demonstrable interest to the organisation.
d) Professional development activity, such as maintaining clinical/professional knowledge and currency with, and / or debating, issues in a field of knowledge. This includes personal development activity, such as university associations and professional societies.

4. Copyright

4.1 The presence of a body of work on the Internet does not necessarily mean that there is automatic right to copy. Work may only be copied where the author has expressed or implied that authorised copying can occur. Staff should not post any information protected by copyright unless permission has been officially provided. Users must abide by all software licensing agreements, copyright laws and other applicable regulations.

5. Inappropriate Use

5.1 Staff must not use the Internet for inappropriate purposes as this may be deemed as serious misconduct. Inappropriate purposes include, but are not limited to:

a) Visiting sites that contain material that is obscene, objectionable, likely to be offensive or which contains "adult content".
b) Visiting of gambling, gaming, on-line shopping, chat rooms, or on-line dating sites.
c) Soliciting for personal gain or profit and/or the participation in on-line auctions.
d) Making or posting improper, indecent, threatening, racist or sexist remarks and proposals.
e) Uploading or downloading commercial software in violation of its copyright.
f) Downloading any software without gaining approval from the Information Technology (IT) department helpdesk.
g) Passing off personal views as representing those of the organisation.
h) Any activity that violates New Zealand law and/or codes of conduct.
i) The transfer of non-work related pictures or audio information, including but not limited to, the viewing or downloading of films or the listening to or downloading of music, TV and video across the internet.
j) Excessive personal use during working hours.
k) Any usage in contravention of 2.6.2 P4 Sensitive Data.
l) Any access utilising the BOPDHB Free Public Wi-Fi facility during work hours.
m) Publishing threatening or offensive material and messages or publishing online invasive or distressing photographs or videos.

5.2 BOPDHB reserves the right to block sites deemed inappropriate.

6. Monitoring of Use

6.1 Procedures will be in place to enable the regular monitoring of individual Internet usage.

6.2 The Information Management service has the right to monitor, retrieve and read all internet use and communication under the following circumstances:

a) Legitimate business need including but not limited to:
   i. routine system administration and / or network traffic management.
   ii. a manager's request to ensure the grounds he / she has approved his/her staff's internet use are being complied with.
   iii. access to information when the employee is unavailable, but timing is critical.
b) Reasonable suspicion of prohibited activities.

Information obtained in these circumstances may be disclosed to line managers of staff members involved and other authorities if necessitated by the information retrieved.

7. Internet Use Audit

7.1 On a monthly basis internet Usage Reports identifying users with high levels of Internet use shall be compiled by the Information Management (IM) service and when deemed required for escalation forwarded to members of the BOPDHB-Executive Committee.

7.2 The Executive Committee member responsible for a staff member identified within the monthly report shall follow up with that staff member as to the appropriateness of the internet usage.

7.3 Managers will have the ability to obtain internet usage reports for their direct reports.

7.4 If the audit and subsequent follow up indicates inappropriate usage then:

a) if the inappropriate usage contains material that is obscene, objectionable, or likely to be offensive (e.g. pornography) the GM Corporate Services (GMCS) or authorised delegate will be informed.

b) the Executive Committee member responsible, in conjunction with the People & Culture team, shall determine the level of response appropriate for the level of abuse.

8. Breach of Policy and Protocol

8.1 Any breach of this policy and protocol will be investigated and may be subject to action under policy 3.50.13 Investigation and Disciplinary.

ASSOCIATED DOCUMENTS

- Bay of Plenty District Health Board policy 2.6.2 Digital Communication
- Bay of Plenty District Health Board policy 2.6.2 protocol 1 Email Usage
- Bay of Plenty District Health Board policy 2.6.2.protocol 3 Social Media
- Bay of Plenty District Health Board policy 2.6.2.protocol 4 Sensitive Data
- Bay of Plenty District Health Board policy 2.6.2 protocol 5 Cloud Services
- Bay of Plenty District Health Board policy 3.50.13 Investigation and Disciplinary