MEMO

To: National CEOs

From: **Jim Green**, **Chair NBAG**

Date: 20 November 2018

Re: Recommended IT Access Principles for District Health Boards

**Preamble**

In response to the opportunity to provide consistent access to publicly available IT information and communication platforms for all staff working within DHBs, the National Bipartite Action Group have worked jointly with the National CIOs group, to develop the below principles to guide DHB policy and practice.

We recognise that our workplaces are open 24 hours a day, 365 days a year and enabling staff to readily access publicly available IT information and communication platforms for reasonable personal use is appropriate and in keeping with a modern 24/7 work environment. Access is offered in recognition of a mature, respectful relationship between employer and employee as a requirement of the good faith employment relationships, and as a benefit (not a right) in respect of reasonable general personal use.

**Principle 1. Access for personal use**

DHBs will enable staff access to publicly available IT information and communication platforms for reasonable personal use, including:

* + The Internet
	+ Social Media
	+ Third party e-mail providers

via methods of access preferred by each DHB, including Wireless internet access for personal devices where this is available.

Access is subject to:

* + the technical mitigation of security risks to the satisfaction of the DHB
	+ adherence to organisational policy or policies covering personal use of a DHB’s computer systems and networks, including staff obligations regarding protecting DHBs systems and information, and a clear definition of inappropriate use.

**Principle 2. System Security**

DHBs have a responsibility to maintain the security and integrity of their IT systems. This means that from time-to-time when a DHB faces a significant IT security risk, or any other unanticipated threat, there may need to be an immediate response that restricts the access referred to in Principle 1. In those cases, employees and unions will be notified as quickly as possible and normal access will be communicated on and restored as quickly as possible. DHBs will undertake communications and other activities to raise staff cybersecurity awareness.

DHBs privacy (trade-offs) - personal access will require data collection from staff…

Also the principles should mention ethical and moral use of access since this will be a big reputational risk for organisations

**Principle 3. Consultation**

All organisational policies relating to the use of workplace technology should be developed and reviewed in consultation with staff and unions. Where security is not at immediate risk, any changes to workplace technology access should involve consultation with staff and unions, with as much notice as possible.

**Recommendation**

That all DHBs:

* Adopt the principles as a guiding document to ensure alignment of policy and practices across all DHBs.

**Response from the National DHB CIOs**

The national CIOs have agreed to support the recommendation (subject to the changes proposed in red) but note that the adoption of the principles and the associated policy changes is an organisational decision for each DHB. The role of CIOs is to provide advice to the decision makers regarding access for personal use about the risks (including appropriate mitigations) and to enact agreed policy.

CIOs will share relevant DHB policies to encourage alignment across DHBs.