APEX
New Zealand's specialist union for allied, scientific and technical employees

New Zealand Resident Doctors' Association

Paper to National BAG
Employee Access to DHB Digital Communication Platforms

24 October 2017

BACKGROUND:

As we all know the access and use of digital communication platforms for undertaking work, communication, and life in general is pervasive both in the workplace and at home, and increasingly so. Where in the past the lifeblood of communication in the workplace may have been the pen, meeting, or telephone, today it is the keyboard and the smartphone, and the digital communication platforms that each can access.

Increasingly DHB staff communicate with each other, and their employers and unions, via txt, e-mail, website, and social media messaging. Access to digital communication platforms has become as important for day-to-day business, and to the operation of the health sector unions, as is access to a phone, meeting room, whiteboard, or pen and paper. It follows that consistent and convenient access to digital communication platforms is essential to the efficient ongoing conduct of union business.

THE PROBLEM

There is a variability amongst DHBs on the extent to which staff can access websites, social media platforms and e-mail providers on DHB computer equipment and/or via their own personal devices using DHB WiFi. In addition to variability between DHBs APEX has encountered situations where computer access for staff has been severely curtailed at short (or no!) notice due to cyber-security concerns. Sometimes the curtailment is temporary, but sometimes staff access to an e-mail server that they have come to rely upon (g-mail as an example) has been extinguished without notice, consultation or explanation, on a permanent basis.

Clearly DHBs own and control their digital systems and are responsible for ensuring their security. And it goes without saying that we all benefit from system vigilance and security consciousness; heaven forbid that a New Zealand DHB should suffer the embarrassment and clinical damage that occurred at the NHS earlier this year. However there is a reasonable level of notice and consultation with staff and unions about digital changes that should be described (role for NBAG) and generally aspired to. For the moment a number of DHBs are falling short of how a reasonable employer would behave.

EXAMPLE

Below is an example of APEX tackling the matter with a DHB earlier this year:

> *'On another unrelated matter also associated with modern technology I note from information gleaned at a recent session of APEX delegate training that [the Employer] has unilaterally introduced changes to staff ability to access electronic media, websites, and e-mail platforms on [the Employer] equipment whist at work. I am advised that the changes were in response to*

the hacking crisis last month which impacted widely around the world and notably very badly on the NHS in Britain.

Whilst we can understand the need of the DHB to respond swiftly to possible attacks on your IT systems, we would point out that the use of these systems is integral to union members, and delegates in particular, being able to operate and fulfil their obligations in good faith under the code. In the modern world the IT system is as integral to the work of operating effective union representation in the workplace as notice boards, meeting rooms, and access to the telephone. At the very least there needs to be consultation when changes to the system are being mooted, and [the Employer] needs to understand that our view is that the good faith of the union/service relationship dictates that there are certain reasonable expectations of access and ability to use DHB IT systems that should be beyond the discretion of the DHB to remove.

I would be pleased to discuss this further if indicated as appropriate. Of particular concern to a number of delegates is their inability after the changes to access G-Mail.

This was followed up by seeking a response to some particular questions:

Thank you for your email and apologies for the delay in responding. The protection of [the Employer] DHB's IT systems is paramount to ensuring patient privacy, safety and care. As with other organisations, [the Employer] DHB will take all necessary steps to ensure our IT systems security and functionality are safe from threats. This will at times mean the blocking of various websites, including access to Gmail via the [the Employer] DHB network. Since the recent 'Wannacry' ransomware cyber-attacks, a decision was taken by [the Employer] to restrict access to all external services and websites via the [the Employer] DHB network that could pose a threat to DHB systems and services. The recent cyber-attacks were mainly effected using email services, and as a sensible step non-DHB managed email services were blocked from the [the Employer] DHB network (the same blocking may not apply for [the Employer] DHB iPads and mobile devices on the external 3G/4G network).

In relation to your specific questions

1. What is the expected timeframe for requests to have extended IT access processed?

For general items the response times for IT service requests are set at a standard 8 days. As part of on-going work in the IT security space, we will review all online non-DHB services currently blocked and determine if access can be restored.

2. Is it a given that 'I need access to my personal e-mail so that I can undertake union business' will be automatically treated as a valid reason?

Union delegates are welcome to use their [the Employer] DHB email address to undertake reasonable levels of business in their role as a delegate. Access to Gmail via [the Employer] DHB network will not be granted to any [the Employer] employee at this time, for reasons of IT security. Gmail is not an [the Employer] DHB provided system and is not deemed part of the managed IT system. Access to such services remains at the discretion of [the Employer] DHB and where granted, requires that the use is not excessive or inappropriate and does not result in expense or harm to [the Employer] DHB, or otherwise violate our policies.

3. That you concur with our view that changes to IT Access policies for staff should be the stuff of consultation with unions.

Policy changes are consulted on. [the Employer] DHB will not consult on external website access as these relate to security issues. Throughout this entire process, regular communications have been issued … informing people of the reasons for the restrictions and encouraging them to log issues with the [the Employer] service desk. As with most changes impacting staff, the [the Employer] will notify and consult where appropriate. Employees at [the Employer] DHB will always be notified about IT changes that may or will impact them.

RECCOMENDATION

That National Bag agree to the following guidelines for digital communication platform use and promulgate them to DHBs.

Preamble:

In recognition of the important role played by access to digital communication platforms for staff and their unions in fulfilling their obligations under the General Requirements (section 4) of the Code of good faith for public health sector, the following is recommended:

1. There is a general recognition that staff and union representatives in particular require as much as is practicable unfettered access to DHB digital communication platforms including:
    a. Local intranets
    b. The Internet
    c. Social Media
    d. Third party e-mail providers
    e. Wireless internet access for personal devices where this is available.

2. The communications access in 1. above shall be subject to the relevant DHB policies applying to digital communications and the Internet provided that such policies:
    a. Only apply restrictions on access that are reasonable for the purposes of maintaining cyber-security and ensuring compliance with reasonable community standards.
    b. Have been developed in consultation with the relevant unions.
    c. May only be changed subject to consultation with the relevant unions and by reasonable notice to affected staff.

NOTE: It is acknowledged that from time-to-time in the modern environment DHBs face malevolent third party attacks on their IT systems which require immediate response. This may often include a requirement to establish immediate restrictions on all staff access to the IT system. Nothing in these guidelines restricts the ability of DHBs to respond to such emergency situations as required. In such situations staff and their unions will be notified of the threat posed, and the restrictions required, in as timely a manner as is practicable.