IN THE EMPLOYMENT RELATIONS AUTHORITY
CHRISTCHURCH

CA 112/07
CEA 7/06

BETWEEN	TONY WILLS Applicant	
AND	AIR NEW ZEALAND LIMITED Respondent	

Member of Authority:	Paul Montgomery
Representatives:	Andrew Little, Counsel for Applicant Peter Kiely and Daniel Erickson, Counsel for Respondent
Investigation Meetings:	31 July and 1 August 2006, 11 May 2007 at Christchurch
Determination:	12 September 2007

DETERMINATION OF THE AUTHORITY

Employment relationship problem

[1] The applicant was employed by the respondent as a storeman at the respondent's engineering base in Christchurch (ANZES) from 31 January 1998 until his dismissal for serious misconduct on 21 July 2005. Mr Wills claims his dismissal was unjustified and he seeks reinstatement to his former position, lost remuneration of $8,048 gross, compensation for hurt and humiliation and costs.

[2] The respondent says the applicant was justifiably dismissed after an extensive investigation and thorough consideration of his explanation. It resists the applicant's claims and declines to grant the remedies it seeks.

How the problem arose

[3] Mr Wills worked in the Marshalling Store and on the Parts Carousel. The applicant's work involved assembling aircraft parts for maintenance work prior to the particular job being commenced by engineers. This required him to source the necessary spares, be it locally or further

afield, and to prepare a complete package as specified by the maintenance planners so that when the aircraft arrived for servicing, the work could begin without delay.

[4] The position required the applicant to use the company's computer system extensively to receive part lists from the planners, to track down the parts required and then to assemble and often deliver the resulting package to the site where the aircraft was to be serviced. Mr Wills was also required to respond to *ad hoc* requests for parts from engineers within and beyond the Christchurch engineering operation.

[5] In August and September 2004, the company undertook an audit of internet use by employees in ANZES. The period covered by the audit was 31 March to 30 July 2004. The initial results identified a considerable number of employees whose usage the company decided needed to be investigated. After initial analysis, it was decided that nine employees warranted closer scrutiny and Mr Wills was one of those employees, along with four others in the Christchurch stores operation.

[6] The other four employees' actions were investigated and all four were dismissed on 26 November 2005. Mr Wills was not notified at this time that he also was under investigation.

[7] On 4 March 2005, Mr Mangos, the respondent's Logistics and Inventory Manager, and Mr Motet, an HR consultant contracted to the company, met with the applicant and two delegates from the Engineering Printing and Manufacturing Union (EPMU) in Auckland. At the meeting, the applicant was handed a letter outlining the respondent's concerns and requesting him to attend a meeting on 22 March 2005. Mr Wills was also given a copy of his Individual User Report (IUR), an explanation of the data it contained and contact details for the employee assistance programme.

[8] Owing to a range of delays, including the applicant being on stress-related sick leave, the formal meeting did not occur until 4 April 2005. Mr Mangos was unwell, so Mr Murray Bedford, the applicant's immediate manager, deputised for him. Mr Motet attended as did Mr Wills with Mr Kaye, the EPMU site delegate, and Mr Knight, the EPMU organiser.

[9] Mr Motet says he took Mr Wills through a number of policy documents the company was relying on. He says they were *the code of conduct, conditions of internet access, webmail, email/IT strategy and architecture and Disciplinary Policies*. Mr Motet also referred to a staff update of 6 September 2002, an email from Mr Mangos on 28 November 2001 and the Integrit-e booklet dated August 2004.

[10] Mr Motet's evidence was that Mr Wills said he was not aware of any of the policies he was shown, did not recall seeing the 2002 update although he accepted he had email access at that time, and that he did not recall receiving Mr Mangos' email in 2001. Mr Wills accepted he recalled browsing the Integrit-e booklet, remembered the cartoon of *Miss December* which was partially obscured by a message window indicating this was not a work-related image. Mr Wills confirmed that he did not go further to read the email policy.

[11] When Mr Motet asked Mr Wills if he (Mr Wills) thought it was appropriate to look at naked people on the company computer, both the applicant and Mr Kaye protested and sought a brief adjournment. On returning, Mr Wills told the meeting it was not a question he could answer with a yes or a no. He said he would not knowingly or deliberately seek out a site with naked people and that if he inadvertently accessed such a site, he would have reversed out of there. There is no significant dispute regarding the notes taken at this meeting.

[12] A further meeting took place on 15 and 16 June 2005. Again, the notes taken are not contested as a record. The parties traversed a significant number of issues and responses from the applicant and his representatives were heard by the company representatives. The original meeting notes were amended to include comments and questions from Mr Kaye and Mr Knight, and also amendments to the original notes requested by Mr Kaye. The final amendments also record the company's responses to the issues raised.

[13] On 21 July 2005, a meeting was convened to convey the company's decision. Mr Mangos explained his conclusions that the applicant was responsible for the total time recorded on his IUR, that is, 41 hours 35 minutes; that all internet activity under Mr Wills' user name took place when the applicant was working and using the SAP system; that the pattern of sites *pointed to a single user*; that instead of leaving offensive sites the applicant continued to browse and that Mr Wills' explanations were not credible.

[14] Mr Mangos also concluded that Mr Wills was aware of the relevant company policies as indicated by his signing off on his Personal Skills Record (PSR) and other documents and the applicant's awareness of the circumstances of the dismissal of a Wellington-based storeman some time earlier. Finally, Mr Mangos concluded that Mr Wills had spent *excessive time* on the internet for non work-related purposes. He then told the meeting that Mr Wills' actions were totally unacceptable and breached the necessary relationship of trust and confidence. He then told the applicant his employment was terminated with immediate effect.

The issues

[15] Mr Wills has consistently denied deliberately accessing any offensive or pornographic sites. He challenges the accuracy of the data on which the respondent relies and the investigative process employed by the company which resulted in his dismissal on the ground of serious misconduct.

[16] In order to determine this matter, the Authority needs to rule on the following key issues:

- What was the extent of the applicant's knowledge of the respondent's internet policies; and
- Did the respondent conduct the investigation fully and fairly in the light of the respondent's policies; and
- Was the respondent, on the basis of its investigation, entitled to reach the conclusion that the alleged breach of the applicant was established and that such behaviour amounted to serious misconduct which entitled the respondent to summarily dismiss the applicant; and
- Was the delay in investigating Mr Wills' actions unreasonable?

[17] The Authority, in this particular matter, has also to decide whether the matter of sharing passwords was significant and whether the assurance given that the meeting following the dismissals of Bisson, Gardner, Cameron and King precluded the respondent from taking disciplinary action against Mr Wills.

The relevant policies

[18] Above in this determination I have referred to the documents put to Mr Wills by Mr Motet at the meeting on 4 April 2005. One of those documents, the emailed update of 6 September 2002, provides a useful summary of the company's policy on personal use and visiting offensive sites.

> *Inappropriate use of computers*
>
> *From time to time the company discovers and investigates situations where employees have been involved in using company computers for viewing, storing or disseminating pornography and other offensive material, or material that could fall within sexual harassment guidelines.*
>
> *The company views these actions by employees very seriously. Prohibited actions involving inappropriate use of computer resources are clearly set out in the Air New Zealand human resources policy manual, under the email and internet monitoring policy. This policy sets out examples of inappropriate use of computer resources,*

> *including accessing and transmitting pornography and offensive material, and also provides examples of the legal liability and other risk of exposure which the company faces.*
>
> *The email and internet monitoring policy states that inappropriate use of the company's email and internet resources will be dealt with under the company's code of conduct and disciplinary procedures.*
>
> *The purpose of this bulletin is to emphasise and reinforce the seriousness with which the company views employees' involvement in pornography and other offensive material in the workplace. Employees who engage in such activities place the company at serious risk of one or more forms of legal liability and their actions will comprise serious misconduct. Those employees, who, after investigation, are found to have undertaken such activities, will face serious disciplinary action up to and including dismissal.*
>
> *There have been a number of instances where employment with Air New Zealand has been terminated in accordance with this policy.*

[19] The respondent's code of conduct was updated on 31 January 2003 and sets out the standards of conduct required of employees in going about their work. On p.4 of this document, the email and internet monitoring policy is set out. The section sets out examples of inappropriate computer use which include:

- Accessing or attempting to access prohibited sites for the purpose of viewing pornographic or other offensive material;
- Viewing, storing and disseminating pornography and material that falls within the sexual harassment guidelines or is otherwise considered to be offensive or inappropriate;
- Using offensive language in emails;
- Using search engines to search for non-company business related topics.

[20] The code then refers to the inappropriate use of email and internet which could expose the company to legal issues and advises staff that the company has developed an email and internet monitoring policy in order to protect the company's interests. Further, it advises that the company installed a tool to block access to undesirable internet websites containing material of an objectionable nature, for example erotica or pornography, which promote illegal, immoral or unethical activities and promotes mass distribution of unsolicited material. Staff are put on notice that email is screened randomly by the company to ensure it is being used for proper business purposes.

[21] Finally, the document states that breaches of the code are viewed seriously by the company and where appropriate are dealt with through the company's disciplinary procedures.

Conditions of internet access

[22] This document reads:

> *Please be aware that Corporate IT implements two important management processes around the provision of internet access:*
>
> - *Access to the internet is provided to support information gathering, research and for monitoring suppliers, competitors and new services. In order to ensure that the amount of use made of the internet is appropriate, monitoring of the amount of use individuals make of the internet is in place, and heavy or unusual patterns of use of the internet is reported to appropriate managers for their review.*
>
> - *Web pages from the internet accessed by users are automatically stored (or cached) for a time on Air New Zealand computers. Corporate IT will therefore from time to time review the material being accessed. Where this material appears to be inappropriate, and access appears to be systematic rather than accidental, analysis will be undertaken to identify the user accessing this material, and will be reported to appropriate managers for their action. Please be aware that this particularly applies to material of a pornographic nature.*

Email policy

[23] The relevant section of this significant document is, in the current context, *Log in IDs and passwords should not be disclosed to other parties or included in the content of the communication*.

Webmail

[24] This policy document sets out the terms and conditions relating to employees' use of Outlook and Korunet, the company's internal email system.

> *These terms and conditions are a contract between you and Air New Zealand Limited. You should read these terms and conditions carefully as they place certain requirements and liabilities on you. By using Air New Zealand Limited's systems, you acknowledge that you understand and accept these terms and conditions.*
>
> *You are entirely responsible for maintaining the confidentiality of your password and account. Furthermore, you are entirely responsible for any and all activities that occur under your account. You agree to notify Air New Zealand immediately of any unauthorised use of your account or any other breach of security. Air New Zealand will not be liable for any loss that you may incur as a result of someone else using your password or account, either with or without your knowledge. However, you could be held liable for losses incurred by Air NZ or another party due to someone else using your account or password. You may not use anyone else's account at any time.*

[25] Page 3 of this document states:

> *You agree not to:*
>
> *(b) Permit any other person to use your password.*
> *(c) Disclose your password to any other person including family members or those in apparent authority, including Air New Zealand help desk staff;*
> *(d) Keep a written record of your password.*
> *(e) Leave your computer unattended and logged on to the service.*
> *(f) Open emails or attachments software from unknown or untrusted sources.*
>
> *You are responsible for all actions performed using your ID regardless of whether that action is from you or from another person with or without your knowledge or consent.*
>
> *We may suspend or cancel your access to the service at any time by giving notice to you. If you do not use the service for 12 months, we may cancel your access to the service without notice to you.*

Integrit-e guide

[26] Under a section entitled *How we treat each other*, the booklet states:

> *Email and internet access is provided to enable us to effectively carry out our business. Nevertheless it is recognised that email and internet will occasionally be used by you for personal reasons. This is okay, provided business productivity is not impacted and personal use is in line with our policies and legal requirements.*
>
> *You cannot use email or internet resources to pursue private business interests or to view or forward inappropriate material.*

[27] Distilling the relevant elements in these policy documents, the company's policy in relation to private internet use is:

- Exploring the internet for personal use is not prohibited.
- Personal use must be in personal time, not company time.
- The company's internet is not to be used for private business purposes or to view and/or forward inappropriate material.
- Where material on web pages accessed by users appears to be inappropriate and access appears to be systematic rather than accidental (particularly in relation to pornographic material), users' offending will be reported to the appropriate manager for action.

[28] Examples of inappropriate use of internet resources include

- Accessing or attempting to access prohibited sites for the purpose of viewing pornographic or other offensive material.

- Viewing, storing and disseminating pornography and other materials that are considered to be offensive.

- Using search engines to search for non-business related topics is not permitted.

- Playing games on the company's computer system is an inappropriate use.

[29] Reviewing these documents, it is clear that they contain both consistencies and inconsistencies as to what is and what is not permitted or prohibited. A clear example is the recognition that the email and internet will occasionally be used for personal reasons, while the code of conduct prohibits the use of search engines for non-company business related topics. Further, there is no limit defined regarding private use except for the proviso that this be done in personal rather than company time and that such use should not impact on productivity.

[30] The code of conduct states that accessing or attempting to access prohibited sites is inappropriate. However, it was accepted in evidence that accidental and non-systematic access to objectionable sites is accepted provided the user reverses out of the site quickly.

Communicating the policies

[31] From material put before the Authority, it is clear that the company's standard approach to promulgating its policies is primarily to post them on the Korunet providing access to the particular policies by way of links on the home page. It is also clear that from time to time email reminders are sent and copies of these are also posted on staff noticeboards.

Disciplinary policy

[32] Invoking of the disciplinary procedures is the most serious action the company is able to take in relation to employees' conduct or performance. The policy clearly states that disciplinary action is a final resort in dealing with unacceptable behaviours. It makes it clear that disciplinary action is to be prompt, impartial, fair, consistent and with an emphasis on resolving the behaviour and obtaining non-recurrence of the relevant problem.

[33] The policy cites the reasons for invoking the disciplinary code and includes serious breaches of the company's policy regarding use of email and the internet and in particular accessing and transmitting of pornographic and other offensive material. It also cites the undermining of the trust

and confidence of the employment relationship as a ground for disciplinary action. The policy sets out six levels of disciplinary action and records that summary dismissal is to be considered only when the behaviour concerned is so serious that it destroys the very basis of the employment relationship and is to be invoked only after careful consideration of alternatives available.

[34] The document also sets out the matters the relevant manager is to consider. These include whether the employee acted in a manner which breached company policies; whether the employee's explanation was reasonable; the cost of the employee's action to the company; and whether in all the circumstances, the disciplinary action would be excessive. It also requires the manager to take into account the employee's length of service, previous work history and behaviour.

The test

[35] The appropriate legal test in this matter is set out in s.103A of the Employment Relations Act 2000. The Act states:

> *The question of whether a dismissal or an action was justifiable must be determined, on an objective basis, by considering whether the employer's action, and how the employer acted, were what a fair and reasonable employer would have done in all the circumstances.*

[36] In applying this test, the Authority needs to be mindful that the respondent's disciplinary process is not to be put under pedantic scrutiny. The approach is as set out in New Zealand (with exceptions) Food Processing etc IUOW v. Unilener New Zealand Limited {1990} 1 NZILR 35.

> *Slight or immaterial deviations from the ideal are not to be visited with consequences for the employer wholly out of proportion to the gravity, viewed in real terms, of the departure from procedural perfection. What is looked at is substantial fairness and substantial reasonableness according to the standards of a fair-minded but not over-indulgent person.*

The investigation meeting

[37] In the course of the investigation meeting, the Authority heard evidence from the applicant in person and from Mr Knight, the EPMU organiser. On behalf of the respondent, evidence was presented by Mr Filkin, an Application Services Manager from Gen-i, which provides IT services to the respondent, from Mr Mangos and Mr Motet.

[38] Consistent with his position throughout the company's investigation, Mr Wills maintained that while he was unaware of the finer points of company policy, he had not, during the period under review, shared his password with others. He acknowledged that he had left his work station

logged in under his details while absent on other tasks to enable other staff to access parts in his absence. He also told the Authority he knew that accessing objectionable sites was not permitted.

[39] Each witness responded openly and honestly to questions put by the Authority and counsel, which enabled the meeting to proceed efficiently. The issue of shared passwords was raised. Mr Kiely sought and was granted leave to have Mr Bedford rebut the evidence given in the Bisson and ors case that he had shared his password and log on details with Mr King. As a result, the Authority later received statements of evidence from Mr Bedford and responses from Mr Gardner and Mr King on this particular issue. The Authority reconvened the investigation meeting and heard from these three witnesses.

[40] Having considered that specific issue, the Authority accepts that Mr King was mistaken as he was given only generic passwords and log on codes by Mr Bedford, not his personal access codes.

Discussion and analysis

[41] There are several strands which need unwinding from the skein of this matter. The respondent's audit initially focused on excess internet use by employees. Having identified nine possible excessive users of its internet facilities, the company then identified access or attempted access to offensive sites by these users. Aspects of the company's investigation process need to be looked at, in particular its reliance on the communications used, the reliance on the applicant's Personal Skills Record and the company's adherence to its own disciplinary policies.

Reliance on disbursed policy documents

[42] A difficulty facing the company is Mr Wills' denying that he had seen the relevant policy documents. At the first formal investigation meeting, these documents were shown to him. Apart from remembering the Miss December cartoon, he said he was unfamiliar with all of them.

[43] The onus on ensuring its computer system is not misused lies with the respondent. Its failure to formally instruct an employee on what terms and restrictions apply to use immediately prior to access being granted, is serious. While access to policies through Korunet is provided, a formal induction and sign-off process and *in your face* message as part of the log on protocol are required.

Reliance on reminders prior to granting of internet access

[44] Mr Wills said he was on the email network when the reminder quoted above was issued, but does not recall it. That is scarcely surprising. At the time of the issue of that reminder, the

applicant did not have access to the internet, that being given *towards the end of 2003*. At that time, only the elements of the document relating to email would have been relevant to Mr Wills.

Reliance on the Personal Skills Record

[45] A matter at issue was the applicant's signing off his PSR with his supervisor, Mr Bisson. That was done on 1 November 2001. This was well before Mr Wills had access to the internet and the company draws a long bow in relying on a document relating to a component, which at the time, was not relevant to the applicant's competence to perform his duties. It is therefore understandable that neither Mr Wills nor Mr Bisson regarded the issue of internet use as relevant at the time the document was signed off by the parties.

[46] The respondent was entitled to question Mr Bisson on this issue but failed to do so. Having waived that opportunity to determine the facts on this issue, the company has failed to establish a credible link between the document signed in November 2001 and Mr Wills' knowledge of a specific element in that document two years later.

The respondent's disciplinary policy

[47] Turning to the implementation of the company's disciplinary policy in this case, it is of concern that this investigation was far from prompt. The respondent's position is that, given the number of related investigations and their scope, it simply did not have the resources to undertake Mr Wills' matter when it addressed those of four of his Christchurch colleagues. Mr Motet said, *there were only two Air New Zealand personnel who could be spared and committed to the exercise, being Terry Mangos and myself … We both had other work to attend to at the time therefore it was not possible to carry out Mr Wills' formal interview at the same time as the other employees were interviewed.*

[48] Simply put, once the respondent's senior management had decided the course of action it wanted followed, it was incumbent on it to provide the resources to carry the process through promptly. The respondent failed to provide the necessary resources and failed to commence its investigation of Mr Wills promptly.

[49] Further, there was little evidence that the applicant's previous good employment record was considered when the decision to dismiss was made.

The assurance given by Mr Mangos

[50] Following the dismissal of the four storemen on similar grounds to that of Mr Wills, Mr Mangos assembled the ANZES staff in Christchurch. At that meeting, he advised all available staff that four staff had been dismissed and explained the reasons for the dismissals. The Authority accepts that Mr Mangos told the staff that no others were under investigation and urged them to work together to meet ANZES's objectives.

[51] The Authority further accepts that at the time of giving this assurance to staff, including Mr Wills, Mr Mangos may have not been aware that Mr Wills had been identified as an excessive internet user and was to come under investigation. This implies that Mr Mangos was not advised of all the individuals in his division who were to be investigated. Such a failure to advise Mr Mangos of the company's interest in Mr Wills' activities, is quite extraordinary given that Mr Mangos, on his own evidence, was responsible for the investigations and was later to determine the fate of Mr Wills.

[52] It is also significant that Mr Wills, ignorant of the companies concerns, worked double shifts for several months to cover for the dismissed storemen and also assisted in training their replacements, only to be dismissed himself. On the evidence before the Authority, no recognition of the applicant's commitment to his employer in those difficult weeks was taken into account in determining the penalty for Mr Wills.

Determination

[53] Returning to the issues set out above in this determination, I address each in turn:

- I find that while the respondent has in place policies covering the use of the internet, those policies are disbursed across a number of free standing, and in part contradictory, documents. The company does not require, as a condition of access to its internet facilities, a clear cohesive document presented to an employee seeking the right to access and requiring that employee's signed acknowledgment that she/he understands and agrees to the terms of use. I find Mr Wills was insufficiently inducted and briefed on the terms of internet use prior to being given access to it. I find that Mr Wills' knowledge of the internet policies was sparse and rudimentary.

- I find the respondent, though advised of the (then) widespread practice of sharing access data and leaving computers on, could not safely conclude that Mr Wills was personally accessing or attempting to access objectionable sites. Mr Wills' evidence

was *I would log on when I started my shift and log off at the end. Sometimes during the shift, I logged onto two or three computers. I would log onto my regular computer; sometimes I logged onto the carousel computer and sometimes at least one other computer. This meant that I could do several things more or less at the same time without having to log in and out of different computers.*

For the same reason the respondent cannot be sure that any excessive personal use, which the respondent was unable to define, was personally undertaken by the applicant.

- I find that on the basis of its inquiry and investigation, the respondent had insufficient evidence that Mr Wills intended to gain access to objectionable sites and that he personally gained access to these sites deliberately.

- I find the delay in dealing with the allegations against Mr Wills was unreasonable and that Mr Wills was entitled to rely on the statement of his senior manager that no other Christchurch staff were under investigation. The notification of his being under investigation some 3½ months following the dismissal of his colleagues, undoubtedly heightened the degree of hurt and humiliation.

- I find that, viewed objectively, a fair and reasonable employer would not, given all the circumstances of this case, have dismissed the applicant as the respondent failed to ensure Mr Wills was fully instructed on the policies governing use of the internet. Further, once put on notice of the widespread practices at NZAES Christchurch of leaving computers logged on and of sharing access information, it failed to investigate these. Had it done so, a more corrective and educational, not to mention more widespread programme, might have resulted in the retention of Mr Wills and the eradication of a widespread, uncondoned practice.

- I find the applicant was unjustifiably dismissed.

- I find that Mr Wills did not knowingly contribute to the circumstances giving rise to his dismissal as he was unaware of the policies the alleged breaches of which were the foundation of his dismissal.

Remedies

[54] The applicant seeks reinstatement to his former role. Having considered the evidence in opposition, particularly in the light of the company's failure to appropriately induct Mr Wills, I order that the respondent reinstate Mr Wills to his former position or to one no less advantageous without loss of seniority and benefits. As Mr Wills is currently employed and presumably required to give notice to his employer, the parties' counsel are to agree a date on which the applicant is to resume his employment with the respondent. If this cannot be agreed, leave is reserved to have the Authority make a specific order.

[55] Mr Wills sought lost remuneration of $8,048. I order the respondent to pay the applicant the sum of $8,048 gross.

[56] I accept the applicant's hurt and humiliation was heightened by the combination of the announcement by Mr Mangos and the delay. I have considered this together with his compensation claim for hurt and humiliation arising from the dismissal and have balanced these with regard to the order for reinstatement. I order the respondent to pay Mr Wills the sum of $5,000 without deduction pursuant to s.123(1)(c)(i) of the Act.

Costs

[57] Costs are reserved.

Paul Montgomery
Member of the Employment Relations Authority