Determination Number: CA 98/06
File Number: CEA 76/05

Under the Employment Relations Act 2000

BEFORE THE EMPLOYMENT RELATIONS AUTHORITY
CHRISTCHURCH OFFICE

BETWEEN	John Bisson (First Applicant) **AND** Carl Gardner (Second Applicant) **AND** Andrew Cameron (Third Applicant) **AND** Martin King (Fourth Applicant)
AND	Air New Zealand Limited (Respondent)
REPRESENTATIVES	Andrew Little, Counsel for Applicants Peter Kiely and Daniel Erickson, Counsel for Respondent
MEMBER OF AUTHORITY	Paul Montgomery
INVESTIGATION MEETING	18 April 2005 19 April 2005 20 April 2005
DATE OF DETERMINATION	3 July 2006

DETERMINATION OF THE AUTHORITY

Employment relationship problem

[1] The four applicants were employed by the respondent in its Christchurch Engineering Services operation. Each claims to have been unjustifiably dismissed from his employment and seeks permanent reinstatement, reimbursement of lost remuneration and compensation for hurt and humiliation.

[2] The respondent denies the dismissals were unjustified and declines to accept the applicants' claims.

The facts

[3] The applicants had been employed by the respondent for various lengths of time; John Bisson for 32 years; Carl Gardner for four years; Andrew Cameron for three years; and Martin King for a total of three years. All worked in stores functions and John Bisson had been a charge hand for 31 years.

[4] In early 2004, as a result of an incident within the respondent's Engineering Services Division, the company's General Manager of Human Resources for the Division initiated a review of the internet use by all employees in that division between 31 March and 24 July 2004. The results raised concerns regarding internet use by a number of employees, including the four applicants.

[5] In September 2004, the respondent engaged Gen-i, a specialist information technology company, to study the data and produce individual internet user reports (IURs) for each of the employees concerned. Those reports linked user identities to sites visited, the dates and number of visits or attempted visits.

[6] The internet use of each applicant was broken down to identify sites designated as *personal use*, as *prohibited use*, sites to which access had been blocked by the respondent's specialist monitoring software, sites with no category assigned and the browse times to internet explorer sessions.

[7] The Gen-i team was required to produce an IUR for each employee setting out a usage summary for adult/sexually explicit sites and for personal interest sites as well as a breakdown of the sites visited, the dates on which they were visited and the number of visits. As 13 internet users were under scrutiny, this task was not completed until 11 November 2004.

[8] Soon after providing the IURs to the respondent, the Gen-i team discovered there had been an element of what I shall call *double counting* and after modifying the programme, re-ran the reports and then completed an exercise involving manually checking the IURs against the original spreadsheets. This confirmed the accuracy of the IURs and the efficacy of the modified programme.

[9] These *second reports* indicated in respect of the four applicants that in the period covered by the review:

- Mr Bisson – 4008 sites visits involving 32 hours' browsing time;
- Mr Gardner – 8303 site visits involving 43 hours 53 minutes' browsing time;
- Mr Cameron – 2,059 site visits involving 31 hours 29 minutes' browsing time;
- Mr King – 12,857 site visits involving 60 hours 34 minutes' browsing time.

[10] On 20 October 2004, the respondent's Divisional Logistics and Inventory Manager, Mr Terry Mangos, held meetings with each of the applicants at which they were given an envelope containing a letter requesting them to attend a formal disciplinary meeting, a copy of their individual IUR and contact information for the Employee Assistance Programme.

The relevant policies

[11] The Authority was provided with copies of the respondent's policy documents:

(1) **Code of Conduct**: This document, authorised and updated on 31 January 2003, contains the standards of conduct required of employees in going about their work. The most important of these standards are listed and include the obligation to provide Air New Zealand's internal and external customers with a consistently high level of service, to preserve the best interests of Air New Zealand and to exercise proper constraint when using ANZ's resources such as not to waste money, equipment or time.

On p.4 of this document, the email and e-net monitoring policy is set out. The section points out that the internet is becoming an integral part of the job of Air New Zealand employees, however, these computer resources are also open to inappropriate use. It then cites examples of inappropriate use which include but are not limited to:

- 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.

The policy then covers inappropriate use of email and the 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. Finally it advises that the company has installed a tool which blocks access to undesirable internet websites which contain material of an objectionable theme, for example erotica or pornography, which promotes illegal, immoral or unethical activities and promotes mass distribution of unsolicited material. The policy also puts staff on notice that email is randomly screened by the company to ensure that it is being used for proper business purposes.

Finally, the document advises that the company plans to implement an email and internet monitoring tool which will scan and strip files found to contain viruses and/or logic bombs in email attachments and web downloads, strip attachments of particular file types from emails, record words used in search engines, scan outgoing emails for offensive language and scan and examine local area network server user directories for non work-related files.

Breaches of the Code are viewed seriously and where appropriate are dealt with through the respondent's disciplinary procedures.

(2) **Conditions of Internet Access**: This document reads:

> *Please be aware that Corporate IT implement 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 news 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.*

(3) **Email Policy**: This is an extensive document of some 14 pages. However, the relevant policy in the context of the current case is *Log in IDs and passwords should not be disclosed to other parties or included in the content of the communication.*

(4) **Web Mail**: This is a document which sets out the terms and conditions applying to employees using Outlook and Korunet which is the airline's internal email distribution system. It reads:

> *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 Limited 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.*

A little further down on p 2 of the document, the policy reads:

> *You agree to use the services only to post, send and receive messages and material that are proper. By way of example, and not as a limitation, you agree that when using an Air NZ site/service, you will not:*
>
> - *Defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others.*
>
> - *Publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, obscene, indecent or unlawful topic, name, material or information.*

On p 3 the relevant parts of this policy read:

> *Air NZ reserves the right to monitor your use of the Air NZ sites/services and to remove any materials in its sole discretion. Air NZ reserves the right to terminate your access to any or all of the services at any time, without notice, for any reason whatsoever.*

Further down the page, the document reads:

> *You agree not to:*
>
> *(a) Select an unsuitable password such as family or street names, birthdates or months, sequential numbers, parts of personal telephone numbers or other easily accessible personal data, or number or letter combinations that may be easily identified.*
>
> *(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 NZ 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.

(g) Access the Air NZ sites/services from a PC accessible to the general public (for example in an internet café) unless the PC is controlled by Air NZ or an Air NZ partner.

You are responsible for all actions performed using your user 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.

(5) **Disciplinary action – policy and procedures**: Use of the disciplinary procedures is the most serious action the company can take in relation to an employee's conduct or performance. The document affirms that where the need for disciplinary action arises, the company will discipline employees fairly and in compliance with legal requirements and contractual obligations. The document states that the purpose of any disciplinary procedure is to address:

- A serious performance shortfall;
- An allegation of misconduct (whether or not considered to be in breach of the Code of Conduct);
- Behaviour that is harmful or potentially harmful to any person or to Air New Zealand;
- Behaviour that is allegedly in breach of the law.

Further, it makes it clear that disciplinary action should be seen as a final resort in dealing with problems, especially performance-related problems, and that where any form of disciplinary action needs to be taken, it will be handled as promptly as possible in the circumstances, impartially, fairly, consistently and with an emphasis on resolution and non-recurrence of the relevant problem. The policy states that dismissal is regarded as appropriate only in the most serious of cases and only after the Group General Manager of the Division and/or the Group General Manager Human Resources and Organisational Change have been consulted.

The policy goes on to cite the reasons for disciplinary action and the two points most relevant to this matter are:

- Serious breaches of company policies relating to the use of email and the internet; particularly matters relating to the accessing and transmission of pornography and other offensive material.

- Undermining the trust and confidence of the employment relationship.

In respect of dismissal, the policy states that this sanction, the strongest available to the company, should be used only after very careful consideration of alternatives. Then, in relation to summary (or instant) dismissal, the policy states this is a dismissal without notice and should be considered only where the behaviour concerned is considered to be so serious that it destroys the very substance of the employment relationship.

In the section headed *Disciplinary Procedure for Misconduct*, a range of guidelines is provided to managers dealing with cases of misconduct. Managers involved in such investigations are urged to involve the relevant Human Resources Manager at an early stage, arranging for an appropriate preliminary investigation which may involve interviewing individuals or organisations, and a framework for conducting the initial interview with the employee. The manager conducting the interview is tasked with fully explaining the reasons for the investigation to the employee and should state that Air New Zealand views the issue seriously and that, depending on the seriousness of the case and the outcome of the investigation, that disciplinary action up to and including dismissal could result. All relevant information gathered by the manager is to be presented to the employee and the employee must be given a reasonable opportunity to comment on the information, explain their case and provide any further information or opinions that they consider relevant to the case. The policy urges the interviewer that the interview should be adjourned as necessary to consider further information or views put forward by the employee and that in some circumstances, further consideration or investigation may be needed.

Following the preliminary investigation and the initial interview, the manager may be required to undertake further investigation and interviews as appropriate. Company representatives are urged to consider all relevant matters, and to investigate further where necessary the outcome of any such further investigation or consideration which need to be advised to the employee for input and explanation. In the event that the manager considers it more likely than not that the employee has acted improperly, the manager should give due consideration to all factors before establishing the appropriate action to be taken. Finally, if it is considered that disciplinary action is appropriate, the manager is to advise the employee concerned and clearly outline the specific reason(s) for the course of action being taken. The manager initially is to give notice of dismissal or other disciplinary action verbally to the employee and in the presence of any representative they may have chosen to be present.

After notifying the employee verbally, the manager is required to send a letter to the employee stating:

- The reasons for the investigation;
- The reasons for disciplinary action;
- The type of disciplinary action decided upon;
- The effective date and duration (if any) of the action;
- The consequences of any further breaches;
- Any commitments by the employee to make reparations;

- Follow up action to be taken (if any).

In a section entitled *Deciding on Appropriate Disciplinary Action* the document says that in deciding what disciplinary action to take, the manager must consider the following: Did the employee act in a way which endangered customers, members of the public, employees or company property? Did the action cause Air New Zealand to be potentially liable at law? It then lists 12 questions that the manager must consider. The ones relevant particularly in the context of this case are:

- What were the costs or potential costs to the company of the employee's action? Did the employee act in a way that contravened clear instructions or company policies and procedures?

- What explanation was given by the employee? Was it reasonable?

- What are the employee's length of service and previous work and behaviour records? Have there previously been negative reports? Have there been positive reports?

- Is there a belief that the employee has been dishonest in their actions or explanations? What is the evidence to support that belief?

- Has this type of incident happened elsewhere in the company? How was it handled? What was the outcome and penalty?

- What will be the effect on morale if adequate disciplinary action is not taken? Will it weaken the authority of management or supervision and make it more likely for this type of incident to occur in the future?

- Is the proposed disciplinary action excessive in the particular circumstances?

The issues

[12] In order to determine this matter, the Authority is required to answer the following questions:

- Did the actions of each of the applicants relied on by Air New Zealand amount to serious misconduct?

- Was the decision of Air New Zealand to dismiss each of the applicants justifiable in all the circumstances?

- What, if any, remedies are due to the applicants in the event they are successful in their claims?

The respondent's investigation

[13] On 28 October 2004, Mr Mangos commenced the company's formal investigation and interviewed Mr Bisson. Mr Mangos was accompanied by Mr Richard Motet, a human resources adviser who had assisted in the preliminary aspects of the investigation. Mr Motet attended the investigation and disciplinary meetings involving each applicant. The remaining three applicants were interviewed on 29 October 2004.

[14] Mr Bisson was accompanied by Mr Lance McKay, a senior Union delegate, and by Mr Ken Campbell, a colleague.

[15] Mr McKay alone attended the initial formal meetings with Messrs Gardner, Cameron and King.

[16] The format followed in each meeting was similar with Mr Motet providing the applicants with company policy documents; the Code of Conduct, the Conditions of Internet Access, Web-mail, the IT Strategy and Architecture and the Staff Update issued on 6 September 2004. Mr Motet referred each applicant to what the respondent's minutes refer to as *the relevant areas of each document*.

Mr Bisson

[17] Mr Bisson, at the relevant time, was employed in the Marshalling Stores and was responsible for bringing together packages of parts or items for scheduled maintenance and refit work on an aircraft prior to its arrival. On receiving a list generated by the planning section, it was his responsibility, along with others, to source the necessary parts and physically bring the packages together to enable the aircraft engineers to complete the particular task. As parts arrived, they were logged onto the system and as they were issued this fact was also recorded along with the particular job and the aircraft to which they were allocated.

[18] When an aircraft engineer is appointed to undertake a particular task, he or she would present the storeman with a service order and either the storeman would enter the relevant data and direct the engineer to where the packaged parts are, or alternatively the engineer would enter his or her own details on the computer and take the package. Mr Bisson says an engineer would perform this function himself if the storeperson was not present and they needed the package. As a charge hand, Mr Bisson was frequently involved in attending meetings with the planners and others. These meetings were held away from the marshalling store and his usual area of work.

[19] Returning to the meeting on 28 October 2004, Mr Bisson says the meeting was opened by Mr Mangos who pointed out it was a formal meeting and that they were dealing with an issue of serious misconduct, the outcome of which could be anything from a warning up to and including a dismissal. The applicant then goes on to say that at that point, Mr Motet took over running the meeting and that he was given *a whole lot of company policies and asked if he was aware of them*. Mr Bisson said that he was not familiar with any of them. This is confirmed by the minutes prepared by the respondent.

[20] Mr Bisson then went through each site category and advised that he had not visited any of them. The applicant then read from a statement he had prepared which stated that after receiving the company's letter of 20 October 2004, he had changed his password and advised his staff to do the same. In the course of discussions, a Mr Steve Marshall, another storeman, said that engineers were regularly on the applicant's computer and so Mr Bisson says he removed his handwritten log ons and passwords from his desk. He also pointed out that over a particular month the company had 23 apprentices each serving one week in the marshalling store for training in the stores procedure, none of whom had been issued with log ons or passwords. Mr Bisson says that he had no alternative but to allow them to use his password and log on. Further, the applicant said that it was necessary for engineers to have open access to the marshalling stores area 24 hours a day seven days a week in order to complete aircraft engineering work on time. It is also clear that Mr Bisson challenged the amount of time he allegedly spent on the internet saying that he would not spend 30 minutes a week on the internet and certainly not in excess of 38 hours over the period in question. Mr Bisson also referred to a French national seconded to the respondent from New Caledonia for a

period of five months for training in stores and to learn English. Again, he says, he provided his log on and password for the trainee's use.

[21] Mr Bisson repeated that he had not spent time on the sites and confirmed that he had given out his log in and password in order to facilitate the operations of the business. Mr Motet reminded the applicant of the policy stating that users are fully responsible for all activities under their user name and password. Mr Motet asked Mr Bisson how the sites came to be recorded, saying *John, are you saying it is not you?* Mr Bisson advised that 90% of the activity on the site was not his. Mr Campbell then said that he could confirm this and Mr Motet asked Mr Campbell if he had observed the sharing of log ins and passwords, why he had failed to act upon it. Mr McKay suggested that the biggest failing was that they had to get around systems in order to get things done.

[22] The matter of receiving and forwarding emails was briefly discussed and the applicant acknowledged he sometimes forwarded. He referred in his evidence to them as *joke emails that I did not consider to be inappropriate and that sometimes I forwarded them to others*. Mr Bisson says he was given the opportunity to bring in front of the meeting any other matters. However, he said there were none and when asked whether he believed he had had a fair opportunity to give his explanation, agreed that he had. The meeting concluded at that point.

Mr Gardner

[23] Mr Gardner was employed by the respondent in the Rotable Store which deals with repairable and serviceable parts. They are taken out when they need servicing or repairing and then re-installed in the aircraft following service. The Rotable Store also deals with extruded items, customer-owned spares and dangerous goods.

[24] This meeting began very much as the one with Mr Bisson with Mr Motet tabling company policy documents and asking Mr Gardner if he was familiar with them. Mr Gardner told the meeting that he had been shown the policies that morning.

[25] When invited by Mr Motet to comment on the sites visited, Mr Gardner said he recognised some but not all sites and when asked to account for the number of sites visited, Mr Gardner advised that a considerable number of people had access to his log in and H drive, including leading hands and staff from Avionics. Mr Gardner also advised that he had been asked to give his log on to trainees by a leading hand and gave the name of that leading hand to Mr Mangos. He also said that on occasions he had returned to his work station and found sites on his screen that he had not accessed. Mr Gardner said he did not keep a written record of his password but also said that he had not seen or signed off on any company policies regarding inappropriate use of internet and email facilities. He added that his password had been given out to ease the workload during times of high pressure. This is consistent with his evidence before the Authority where he says *As far as I know, the practice of leaving terminals open and allowing engineers to log parts out of the system was known to the local management and condoned and accepted. I have certainly not been aware that it is a breach of policies or accepted practice.*

[26] Mr Mangos also asked Mr Gardner whether he had supervised any unauthorised use of the internet and Mr Gardner replied that he had briefly and gave examples of people playing games or looking at *Trade Me*.

[27] Mr McKay suggested that Mr Gardner may not have received the Internet Staff Updates on their obligations relating to web mail and internet use.

[28] In reply to a question from Mr Gardner, Mr Mangos advised that the company had a benchmark on costs of email and internet use but that it may be more important to review overall usage patterns and contents of sites visited. The issue of trust, he said, played a significant role.

[29] Similar to the earlier meeting, Mr Motet asked if Mr Gardner and Mr McKay had any other matters they wished to raise and as there were none, Mr Motet asked Mr Gardner if he had had a fair chance to present his explanation and Mr Gardner confirmed this was the case. The meeting then closed.

Mr Cameron

[30] Mr Cameron was employed as a storeman in the Rotable Store. The meeting began as did the others with Mr Mangos cautioning the applicant about the seriousness of the matter and that the investigation was taking place in the context of serious misconduct which may result in disciplinary action up to and including summary dismissal. As with the earlier meetings, Mr Motet tabled the company policies and asked Mr Cameron whether he was familiar with them. Mr Cameron advised he was not aware of the policy or of Korunet or of the staff advice email dated 6 September 2002 or of such notices posted on the noticeboard.

[31] Mr Motet asked Mr Cameron to comment on the amount of time he had spent on the internet and the contents of some of the sites accessed. Mr Cameron said he was shocked at the adult/ sexually explicit sites listed in the report and said that he looked at sites regarding hot rods and this sometimes led to inappropriate sites. However, if he accessed these inadvertently, he exited promptly. The applicant acknowledged that he spent quite a lot of time on the internet and had browsed on banking sites and had looked at lingerie sites as possible presents for his wife. Mr Motet asked why these sites appeared on his IUR and Mr Cameron said it was the engineers who were doing this while he was away from his work station, confirming he had shared his log in and password as he was under pressure to perform his duties, particularly at nights. He accepted that at times he left his work station computer open.

[32] Mr Cameron said he usually browsed during quiet periods or during breaks. Mr Motet asked if he had received any instructions to give his password to others and Mr Cameron said he had not been instructed to do this.

[33] Mr Cameron said that earlier warnings would have been appropriate regarding his use of the internet and would have prevented him by alerting the applicant to usage patterns.

[34] Mr Motet asked the applicant if he had any other matters he wished to raise at the meeting and Mr Cameron said there were none. Mr Motet asked Mr Cameron if he felt he had had a fair opportunity to present his explanation and Mr Cameron confirmed this was so.

[35] In his evidence before the Authority, Mr Cameron said that Mr Motet had asked if stores people had access to his log in and password and that he had replied no. He said that they would have had their own computers. However, engineers had access to both his log in and password.

Mr King

[36] This applicant was employed in the Marshalling Store when he rejoined Air New Zealand and in evidence said that *during the first three to four weeks their IT department could not supply me with the appropriate access to programmes to carry out my task so I was given Murray Bedford's log on initially and was then requested to start using my leading hand's log on until mine could be*

established. During this period Murray (Bedford) asked me to transfer to the Rotable Store where I continued working until my dismissal.

[37] Again, the meeting began with Mr Mangos issuing a caution as to the seriousness of the matter and the possibility of disciplinary action up to and including summary dismissal.

[38] Again, Mr Motet tabled the company policies and asked Mr King whether he was familiar with them. Mr King's response appears to have been that *commonsense applies*. After explaining to the applicant how the hourly rate was calculated, Mr Motet told Mr King that high personal use and the contents of the sites visited were of particular concern to the company and invited Mr King to comment on the sites recorded in his IUR. Mr King said that a number of sites did not *ring a bell* with him but that some sites may have been visited. Mr Motet advised that all sites visited were under Mr King's user ID and either attempting to enter or actually entering unauthorised sites was not acceptable.

[39] Mr Motet then asked Mr King if he had given others his log in and password and Mr King said that in order to facilitate issuing of parts and business continuity, he had done this. He said that it was not common for him to give out his password except to engineers. He also accepted that he usually left his computer logged on and confirmed that no store staff had access to his log in and password.

[40] Mr Mangos asked if the hits were Mr King and he acknowledged that they were but he said he would need the time of day to be clarified. Mr King also said he was aggrieved that the use of internet was hardly monitored, despite what was set out in the Code of Conduct. He expressed the view that it was up to management to bring overuse to staff attention early on. Mr Mangos replied that no monitoring should be necessary and that he trusted members of his team to behave in a way that reflected his confidence in them.

[41] The minutes record that Mr King handed a reference from a fellow employee commending Mr King's work habits to the company representative. Mr Motet asked Mr King whether he had other points he wished to bring to the attention of the meeting and Mr King confirmed that he had not. Mr Motet asked Mr King if he felt he had had a fair opportunity to put his explanation forward and Mr King confirmed that this was so. The meeting was then closed.

[42] For the record, each set of minutes prepared by the respondent carries the annotation *Minutes taken by TM on 28 October and collated by RM on 1 November 2004.* This is somewhat puzzling since only Mr Bisson was interviewed on 28 October and the other three applicants on 29 October. It does, however, confirm that Mr Mangos, as senior executive present, was taking minutes at each of the meetings.

[43] The company representatives met with Mr Bisson, Mr Gardner and Mr Cameron again on 19 November 2004 and with Mr King on 22 November 2004. The purpose of the meetings was to provide each of the applicants with any further explanations regarding matters each of them had raised in the previous formal investigation meeting. Various issues were discussed with each of the applicants and their representative, and the company then prepared a written response to each of the matters raised by each of the applicants or Mr McKay in those meetings.

[44] The issues raised by each applicant were itemised and responded to in a document prepared for each applicant and presented to them at the meetings convened by the respondent on 26 November 2004.

The final meetings

[45] On 26 November 2004, the respondent's representatives met with each applicant to provide feedback from the earlier meetings and to deliver its decisions.

John Bisson

[46] During the investigation, Mr Bisson had noted that out of the 120 days of the review period, only 13 days showed hits under his log in and password. The company's response was that his IUR showed heavy activity throughout the review period. That activity was almost exclusively not work-related with a considerable percentage of access being to sites containing offensive material, whether endeavoured to be accessed or actually accessed.

[47] Mr Bisson advised that he would occasionally receive internet joke material which was not hard core giving the example of girls with big bosoms. He said that if they were humorous, he would flick them on. The company's response was that the email policy specifically prohibited the transmission of inappropriate material and that Mr Bisson's example was considered to be offensive material.

[48] Mr Bisson had denied seeing pictures coming up and had never had porn pictures come up. Occasionally he would get the Access Denied screen. The company's response was that given the large number of sites either endeavoured to be accessed or actually visited, it did not find Mr Bisson's explanation credible.

[49] Mr Bisson, in a statement made to the respondent's representatives, pointed out that had he received a warning under the terms of *levels of disciplinary action – policy and procedures*, he would have taken immediate action that would have resolved the problem. The company's response acknowledged Mr Bisson's long service with the company and that there were no concerns in respect of his work performance. However, given his length of service, it was expected that Mr Bisson would understand the company's expectations of behaviour and conduct himself accordingly.

[50] Mr McKay had stated that the biggest problem was establishing what Mr Bisson actually accessed compared with other sites visited during his log on. Mr Bisson had indicated his log on details were up on the wall adjacent to his computer. The company's response was that sharing of passwords is in direct violation of company policy which specifically prohibits the practice and that Mr Bisson was responsible for all actions performed using his user ID regardless of whether that action was from him or from another person with or without knowledge or consent from Mr Bisson.

[51] Mr Mangos then read the following statement:

> *I have found you have spent excessive time on the internet accessing internet sites, during work time and using company computer equipment.*
>
> *The nature of many of the sites you accessed, or attempted to access, was totally inappropriate as we recounted to you examples from a selection of these sites.*
>
> *Your action in sharing your password is a direct violation of company policy which specifically prohibits this practice.*
>
> *I believe your actions are totally unacceptable and have breached the trust and confidence necessary in the employment relationship.*

I find these factors taken both separately and in combination amount to serious misconduct.

Given my findings of serious misconduct I have decided you will be summarily dismissed from employment, effective today.

I will follow this up with a letter.

Mr Gardner

[52] After clarification of some issues relating to minutes of earlier meetings, Mr Gardner said that he did not recognise any of the sites sampled by Mr Motet as part of the company's investigation. The company replied that, given the large number of sites visited, that it did not find the explanation credible. He did not accept that Mr Gardner did not recognise or recall either endeavouring to access or having actually accessed any of the sites.

[53] Mr Gardner had stated he did not recognise or understand the sites reflected against his user profile and that he did not have a clue what they were. He had gone to a friend's house to sample some of the sites but had said he did not recognise them. Mr Gardner said he had not accessed any pornographic sites and was bewildered by the number of sites reflected in the report. The company's response was that, given the large number of sites visited, that the explanation was not credible. It also noted that Mr Gardner had shared his passwords and that he remained fully accountable for all actions performed using his user ID regardless of whether that action was by him or by another person. The company made it clear what the policy was and it required individuals to take all possible care to prevent a password from being disclosed to anyone else.

[54] At the conclusion of this interchange, Mr Mangos read a statement identical to the one quoted above.

Mr Cameron

[55] Mr Cameron had stated that he had not accessed sites set out in the sample, saying he did not recall the sites and stating there was no way he would be looking at images of males. He had claimed these and the other offensive sites were not the result of his actions and that it must have been engineers who had access to his password. The company's response was that policy prohibits employees giving passwords to others and that Mr Cameron remained fully accountable for all actions performed under his user ID.

[56] Mr Cameron had told the company that he recognised a particular site classified as adult/ sexually explicit and had told the company this was a blocked site. He accepted also that he recognised the lingerie site which he visited while looking at possible gifts for his wife. The company responded by saying that, given the large number of sites either endeavoured to be accessed or actually visited, it did not find his explanation credible and did not accept that Mr Cameron recognised only one or two of the sites recorded in his IUR.

[57] Mr Cameron asked why he had not received a verbal warning from Mr Mangos in terms of the disciplinary policy and the company responded by saying that its policy clearly indicated that employees whose actions comprise serious misconduct after investigation, will face disciplinary action up to and including dismissal.

[58] Mr Cameron had said that if the total internet time recorded was divided by the number of working days, this would amount to around 30 minutes a day which was well within the time allocated for breaks in the course of the day. The company said that it recognised the occasional use of internet/email services for personal use, which was acceptable provided such personal use was in accordance with company policies. It found Mr Cameron's usage to be in clear breach of the policy as this refers to the number of sites containing inappropriate material. Further, it pointed out that the company's computer facility is not a recreational facility.

[59] At the conclusion of this feedback, Mr Mangos again read to Mr Cameron the company's conclusions which are identical to the document cited above in relation to Mr Bisson.

Mr King

[60] In the course of the investigation, Mr King had stated that some of the sites were familiar to him but some he did not recognise. He had asked for the times he had visited the sites to be provided and the company provided a more detailed printout. Mr King had indicated that he did recall looking at adult dating sites and that he had looked at naked women on the computer system. The company responded by saying that it did not find Mr King's explanations credible and pointing out that he was accountable for all actions performed using his user ID regardless of whether that action was by him or by another person with or without his knowledge or consent.

[61] Mr King had advised the company he had given his password to certain engineers to allow for the flow of work to continue and keep the Rotable Stores open when he was not present at his work station. The company reiterated its policy that employees were not to give their passwords to others, stating that the practice was specifically prohibited. In response to Mr King's expressed view that people may be accessing sites in down time when there was no work tasks to be done, the company reiterated its view that its IT system was not a recreational facility. It found that Mr King's usage was in breach of policy in respect of the high level of personal usage together with the number of sites recorded containing inappropriate material.

[62] Again, the meeting concluded with Mr Mangos reading from a document similar to that read to the other three applicants.

[63] All four applicants received a letter directed to their home addressed dated 26 November 2004. Except for the names of the addressees and their personal addresses, the letters are identical. It is set out below.

> *Dear …*
>
> *This is to confirm my verbal notification that your employment with Air New Zealand Limited was summarily terminated on 26 November 2004.*
>
> *A copy of the written notes I referred to at that meeting are attached. These notes contain the detail of the company's consideration of your explanation.*
>
> *The reasons for your termination are:*
>
> 1. *The time spent on the internet during working time for non work-related purposes.*
>
> 2. *The nature and content of the sites visited.*
>
> 3. *Your claim of sharing your user ID and password.*

You had an opportunity to explain your actions at meetings held on 28 October 2004, and again on 17 November 2004. These explanations have been thoroughly considered and I do not believe your explanations were acceptable.

I formed the view that these actions comprised serious misconduct. As a result of your actions, I have terminated your employment effective 26 November 2004.

Final instructions in respect of termination administration are to be forwarded to you.

Yours sincerely,

Terry Mangos
Logistics and Inventory Manager

The Authority's investigation meeting

[64] The Authority was assisted by evidence from the four applicants; Mr John Kay, the Union's delegate for the Stores personnel and trainees and who attended the final meetings with the applicants; Mr Michael Camp, an aircraft engineer; Mr Stephen Tippet, a team leader; Mr Evan Belworthy, a production leader; and Mr Jason Turner, a business process analyst. All were, at the relevant time, employees of Air New Zealand.

[65] For the respondent, the Authority heard evidence from Mr Mangos, Mr Motet and Mr Scott Forrest, a team leader from Gen-i.

[66] I record the Authority's appreciation of the thorough and detailed preparation undertaken by counsel, Mr Little, Mr Kiely and Mr Erickson.

[67] In the course of the investigation meeting, a number of relevant issues came into clearer focus as a result of questioning by the Authority and counsel. Mr Kay gave evidence of the widespread practice of sharing passwords and supported this evidence with signed statements from 186 staff who said they had either used another employee's log on and password or shared their log on and password with other employees, or both. These documents dated 6 December 2004 were not available to the respondent during its investigation process. It reflected a very disturbing practice within the Christchurch Engineering operation.

[68] The applicants and their witnesses confirmed this widespread practice, several stating that they had been instructed by team leaders to use the team leader's log on and password. Mr King's evidence was:

> *Upon rejoining Air New Zealand I worked in the Marshalling Store. During the first 3-4 weeks their IT department could not supply me with the appropriate access to programmes to carry out my tasks so I was given Murray Bedford's long on initially, and then was requested to start using my leading hand's log on until mine could be established.*

[69] In reply to questions from the Authority, Mr King stated that Mr Bedford gave him his log on details and later instructed Mr King to use that of his leading hand.

[70] Mr Bisson's evidence was that he had his access information written down next to his computer to enable his own staff and engineers to source essential parts in his absence. The

Marshalling Store has an *easy issue area* which contains stock covering some 2,000 general hardware items and engineers are able to draw from this stock as it is needed using *slim* computers – that is, computers loaded with only the software necessary for this task. This applicant pointed out that engineers do not have access to the other stores functions undertaken by the applicants nor access to other sections of the SAP programme. His evidence was that his tasks frequently took him away from his work station and he, like his fellow applicants, took steps to enable engineers to book out parts other than those held in the easy access area.

[71] Mr Bisson also confirmed that at one time 23 apprentices were posted to Stores for a week's induction training and none had log ons or passwords so he provided them with his own. Further, he confirmed that during the period in question, Elvis Caunes, a trainee from New Caledonia, used his access data and visited travel and dating sites. Mr Bisson also clarified a statement he made in the course of the investigation by the company. He had said to Mr Motet, *90% of this is not mine*. He said in evidence that he was referring to the total internet report, not the two pages of pornographic sites.

[72] Each of the applicants testified that he had had no formal training in the computer systems but had been taught by fellow stores employees. Each denied he had seen the respondent's policy documents until they were given to them at the first formal meeting when Mr Motet drew his attention to the relevant passages. Each applicant told the Authority that before having internet access installed on his work station, he had received no induction of any kind as to its proper use.

[73] All of the applicants admitted some personal-interest use of the internet in relation to such information as motor racing, news, motor vehicles, celebrities, banking, games, cameras, photography, vineyards and sport. Mr King admitted he visited dating sites as at the time he was *on his own*. Mr Cameron said he had visited lingerie sites in search of gifts for his wife and that on occasions linked offensive *pop up* sites would come up on screen and he would delete them. Each applicant denied he had personally and intentionally visited adult/sexually explicit sites.

[74] The evidence of Mr Tippet was invaluable as it set out process issues within the Christchurch Engineering operation in relation to granting of authority and access or IT applications and transactions. His evidence was that he, with Mr Bisson, was a member of the Materials Focal Team. He said:

> *The team's objective is to implement improvements related to the supply of materials to production that increased productivity by reducing inefficiencies and frustrations. In the past, the Materials Focal Team has introduced some initiatives that have required the charge storeman in the marshalling store to perform new functions within the ANZEF business system, CERES. In some cases, these new functions have required access to IP applications and transactions that are only available to the charge storeman. When Mr John Bisson, as the charge storeman, has not been at work, his duties have been passed on to other marshalling store staff to perform in his absence. Because these storemen have not have access to appropriate IT applications and transactions, they have used John Bisson's log on and password in order to perform his duties. An example of this happening relates to a problem we were having in aircraft maintenance last year with the inability to, within CERES, credit inventory back into the warehouse that had been purchased "direct to job" but not used during the maintenance visit. The problem was addressed by the Materials Focal Team and a simple remedy was found which required the use of a transaction that only the charge storeman had access to. While John Bisson performed the bulk of this work, there were times when he was not at work and other marshalling store staff*

performed this function in his absence. Because they did not have access in CERES of a charge storeman, they used John Bisson's log on and password.

Ordinarily if the function needed to be performed by another staff member in John Bisson's absence, then they should be granted the access to the transaction. However, it should be noted that the process of getting a person access in CERES for specific transactions that are outside the scope of their normal position has not been timely in the past nor has the temporary nature of the access suited the operations of the relevant department. It can take up to three weeks to get an application for IT access processed and often the access is only given for a short period of time which means that access may need to be repeatedly requested. The user often requires the access immediately as they are already doing the job. It is highly probable that this lack of timeliness and the temporary nature of the access contributed to the practice of sharing log on and password information.

In my observation, this practice of sharing log ons and passwords has been occurring reasonably frequently in Christchurch aircraft maintenance. As the "informal business systems support expert" I am, along with another staff member who works for me, often approached to assist people in getting access to IT applications and transactions. In many cases, the request to us is only made after a period of time in which that person has already been performing their tasks using another staff member's log on/password.

It is highly likely that John Bisson, like many people in Christchurch aircraft maintenance, was not aware that the LAN account access and CERES access were in fact different and, like a lot of people, he had set up the same log on/passwords for these. The risk here is that if a CERES log on/password is being shared, the person receiving it can also get access to the owner's LAN account which includes their personal folders, files, email and internet.

[75] At the investigation meeting, when questioned by the Authority, Mr Tippet made the observation that in his view the applicants' understanding of information technology was basic as distinct from his own, as his role as the business process analyst for the Christchurch Aircraft Maintenance Unit requires extensive and detailed understanding of the systems in place and how they might best be modified to ensure greater efficiencies.

[76] The respondent presented to the Authority a considerable amount of complex yet essential documentation. The Authority was particularly assisted by the evidence of Mr Forrest who detailed the process underpinning the respondent's internet review and the checks that were made to ensure the final IURs were accurate.

[77] Other documents presented to the Authority for its investigation were the policy documents referred to earlier in this determination and also a number of updates posted on Korunet, the company's internal electronic communication system.

[78] In his evidence, Mr Mangos makes it clear that the respondent has in place detailed policies and procedures relating to computer and internet use. He does not accept that the applicants were not made aware of policies relating to email and internet usage. He goes on to say that all of Air New Zealand's employment policies can be accessed through the employee intranet (also known as Korunet) to which all four applicants had access. He says *employees are required to regularly access the Korunet for various reasons, for example to read the weekly bulletins given by Air New Zealand's Chief Executive Officer. A link to Air New Zealand's "HR On-line" where company policies can all be accessed is clearly visible on the front page of the Korunet.*

[79] Mr Mangos also stated that employees are regularly reminded about policies and cites an email he sent on 28 November 2001 to a number of staff within the Engineering Division including the first, second and third applicants, drawing their attention to email and internet policies. Mr Mangos accepts that Mr King did not receive the email as he was not at that time within the Engineering Support Services Support Team. Further, he points out that other regular notices are also sent to employees drawing their attention to the content of particular policies and he cites an email sent to staff in February 2002 which clearly referred to passages in the company's Human Resources Policy Manual. He is of the view that all of the four applicants would have received that email. Again he refers to another update sent in September 2002 reminding all employees of the guidelines relating to computer use. He goes on to say that updates are emailed to all staff with computer access, which included the four applicants, and hard copy versions are placed prominently on all employee noticeboards.

[80] Mr Mangos also stated that at meetings held in March 2004 in Christchurch to discuss the results of a Gallup Poll conducted by the company in late 2003, the company took the opportunity to table the reasons for the dismissal of a storeman in their Wellington operation. He says *those meetings were attended by all the Christchurch engineering base staff members in my team including the four applicants*. He goes on to say, *in the light of this, I am extremely surprised that the applicants now say they did not know it was a breach of Air New Zealand's policy to access inappropriate or offensive material using Air New Zealand's computer facilities.*

[81] In relation to the sharing of log in and password details, Mr Mangos said that he categorically refuted that it was necessary for employees to share log on IDs and passwords. Further, he said he did not consider it necessary for engineers to have knowledge of a storeman's log on ID and password as engineers have their own log on which enables them to access the stock data view programme which allows engineers to view the parts in stock and the availability of parts and to determine where they are. He says *it is entirely unnecessary for the engineers to in fact access the stores system to carry this out.*

[82] Mr Mangos gave evidence as to the events at each of the meetings held with each of the applicants. He says *Richard Motet took detailed notes of what was discussed* [sic] *in those meetings. These were later reduced to a set of typed notes.* This is consistent with Mr Motet's evidence which says *the content of the discussions at the formal meetings is as recorded in the typed notes which were derived from written notes taken by me at the time.* However, as noted above, the evidence of both witnesses is in contrast to the footnote on each of the typed minutes stating *minutes taken by TM* [Terry Mangos] *on 28 October and collated by RM* [Richard Motet] *on 1 November 2004.* Mr Mangos made it clear to the Authority that it was he and he alone who was responsible for making the decisions in relation to the four applicants and that the role of Mr Motet was that of an adviser.

[83] In answer to questions Mr Mangos conceded that he was not aware that any manager had drawn the relevant policy documents to the applicants' attention. He also conceded on the issue of contract, that he was *unaware* whether the respondent was providing the applicable policy documents to staff at the time IT access is granted. Mr Mangos confirmed that access to the internet was through the applicants' direct line manager and did not accept that there was a low threshold for access to the company's IT systems. When asked whether he had enquired on whether the applicants had been inducted at the time of access being granted, Mr Mangos replied that he did not enquire on that point. Finally, Mr Mangos accepted that prior to the first formal meeting the respondent had had no knowledge of the sharing of passwords. When asked what steps were taken to investigate the issue of shared passwords Mr Mangos replied that he did not investigate this. In particular he did not investigate the information provided by Mr Bisson that Elvis Caunes had accessed his log on and passwords for a considerable part of the period in question.

[84] In his evidence, Mr Motet concentrated initially on the range of documents relevant to the matter at hand which have been noted earlier in this determination. He pointed out that the IT Strategy Architecture policy provided that employees *should not disclose their user ID or password to any other person*. The witness then went on to direct the Authority to the Disciplinary Action-Policy and Procedures document. Mr Motet covered the process of the review of internet use including his examination of a number of the websites listed in the IURs. He says, *due to the sheer volume, it was not possible for me to examine every single site that was listed as adult/sexually explicit*. He then provided the Authority with a range of sites he sampled from each of the applicants' IUR.

[85] An issue which arose in the course of the investigation meeting was which of the respondent's representatives took the leading role in the investigation and disciplinary meetings. The applicants took the firm view that Mr Motet was in fact controlling the meetings and that Mr Mangos was working under his instructions. Mr Bisson says that following the introduction to his meeting on 28 October 2004, Mr Motet took over running the meeting. Mr King gave evidence which also indicates that at his meeting on 29 October 2004, Mr Motet was the predominant participant for the respondent after Mr Mangos had introduced the meeting and issued the warning about serious misconduct and the possibility of dismissal. The evidence of Mr Cameron is similar.

[86] In his written evidence, Mr Motet says in relation to Mr Bisson that he did not consider he took over the running of the meeting but that he went through the various policies. In response to Mr King's evidence, Mr Motet said he was unsure what policy Mr King believes he *rushed over* and says that he did not deliberately seek to downplay any aspects of the policy but simply highlighting what he thought were the most relevant areas for the matter in hand.

[87] In the course of the investigation, the notes taken by Mr King's representatives at the meeting of 26 November 2004 were put before the Authority. These notes are of interest in that they indicate that the meeting was largely conducted by Mr Motet and that it was he who refused to consider new information prior to Mr King's dismissal. I set them out below:

26-11-04 9:45

ANZES MEETING *Terry Mangos*
Richard Motet
John (delegate)
Martin King
Nicky Young

NY *Has Martin been informed that this is an investigatory or disciplinary meeting?*

RM *Lance has been informed that this is a disciplinary process.*

NY *We believe that we have more information to offer. Gabrielle [Moore] can offer intimate [sic] information on Monday.*

RM *We have been over this matter at last meeting.*

NY *No we haven't. This is new meeting, this is not John Bisson, this is Martin King. Separate meeting. Would continue to raise these issues.*

RM *Indicates to TM to begin.*

TM *Starts reading reports/decision in front of him. Concludes that nature and use of internet inappropriate serious misconduct, summary dismissal today will be followed up in writing.*

NY *Would like to raise some concerns that we have.*

RM *Covered that. Put your concerns in writing.*

NY Don't believe we have – did Air NZ have software in place to prevent inappropriate use?

RM Super scout software.

NY How were these sites accessed if software installed?

RM Raise that concern in writing. It is disadvantageous for your member now and we don't wish to discuss it. We have reached a conclusion.

NY We believe we have information further to this investigation. We would expect a fair and reasonable employer to adjourn to consider this.

RM Put it in writing.

** Fire alarm sounds. Discussion on whether to evacuate, just about to leave room and it stopped.*

RM Use your organisation to gather this information. I am not your secretary.

NY For the sake of our members and yourselves I need to highlight to you our areas of concern, offer further information and ask for clarification. Irresponsible not to.

RM Meeting is closed.

John (delegate) requests notes and asks was the decision to dismiss Terry's.

RM Yes. Meeting closed.

NY Offer of industrial chaplain extended to Martin?

Martin No thank you.

RM Wait for Murray downstairs who will handle it from here.

[88] For the sake of the record it needs to be acknowledged that the company says that it never received any further information.

[89] Two other matters which emerged in the course of the investigation meeting are significant. When the Authority put to Mr Mangos the proposition that there was inconsistency of expression in the policy documents relating to internet and webmail use, the witness agrees that this was so.

[90] The second matter relates to the evidence of Mr Motet in relation to the minutes of the Martin King dismissal meeting taken by Nicky Young. Mr Motet, under questioning, said in respect of the adjournment requested by Nicky – he had no reason to adjourn and recommended to Mr Mangos that they proceed. The other is in relation to the dismissal procedures set out in the company's policy document which requires the company's representatives to consider all alternatives short of dismissal. When asked what alternatives had been considered, Mr Motet said *the misconduct was so severe they could not go back to the workplace*.

[91] Another issue firmly presented by Mr Motet in his evidence was that examination of the individual IURs established a pattern for each applicant in terms of specific taste in material.

Discussion and analysis

[92] The kernel of this case is the respondent's finding that each applicant breached the company's policies so seriously that the company had no alternative but to dismiss them.

[93] In defending its decision, the respondent faces some significant difficulties. One is its failure to fully investigate the extent to which sharing of log ons and passwords or the leaving work stations open prevailed in this workplace at the time. The Authority accepts Mr Mangos' evidence that the practice is not condoned, but faces the difficulty that evidence of the local logistics manager giving his own access details to Mr King when he rejoined the company was not contradicted at any

stage. All four applicants, in the course of the respondent's investigation meetings, clearly stated that they had given others their passwords for operational reasons and several indicated that at various stages they had been instructed to share this information with others in the workplace.

[94] Each applicant denied personally accessing the adult/sexually explicit sites and made it clear that in the course of the respondent's investigation that the practice of sharing access information was widespread. In this set of circumstances, there can be no certainty that each applicant personally accessed all or any of the explicit sites found on their IURs. I accept Mr Mangos' evidence that he found the explanations proffered by each of the applicants to be incredible however, had he and Mr Motet fully probed the extent of log on and password disclosure, I think it fair to say he may have found the applicants' defence more believable.

[95] To be clear, the Authority is in no better position than the respondent to determine whICH sites were personally accessed by the applicants and which were accessed by others. It is clear from the evidence of Mr Bisson, that at least 24 people had access at some time to his log on details.

[96] The Authority accepts the accuracy of the IURs linking the applicants' access details to the sites visited and but for the widespread dissemination of those details, would find each applicant had personally visited the listed sites. In this instance, it is simply unsafe to conclude that each site listed on the individual IUR was in fact accessed by the applicant in question.

[97] The Authority accepts that at the time and on the face of the evidence provided by the IURs Mr Mangos found the explanations proffered by the four applicants as *not credible*. That judgement could have been made only after fully investigating the information provided by the applicants in respect of access misuse and verification, or otherwise, of each applicant's claim that he had seen for the first time the documents explained by Mr Motet at the first formal meetings.

[98] The respondent's disciplinary policy is clear, setting out the process to be followed and all the matters needed to be taken into consideration in a disciplinary setting. The Authority has no criticism of this policy. What is of concern is the admitted failure to consider alternatives to summary dismissal. On p.11 of the company's document *Disciplinary Action – Policy and Procedures*, the document outlines a range of questions the respondent's decision-maker needs to take into account. Among those are:

- What explanation was given by the employee? Was it reasonable?
- Has the employee committed similar or other offences previously, and been warned?
- What are the employee's length of service and previous work and behaviour records? Have there previously been negative reports? Have there been positive reports?
- Has this type of incident happened elsewhere in the company? How was it handled? What was the outcome and penalty?
- Is the proposal disciplinary action excessive in the particular circumstances?

[99] In the same document, under the heading *Levels of Disciplinary Action*, the policy covers dismissal. That subsection reads:

> *This sanction the strongest available to the company, should be used only after very careful consideration of alternatives.*

[100] A further difficulty the respondent faces is its failure to ensure, in accordance with its policies, that those granted access to webmail and internet on its IT system are provided with the terms of such access prior to it being granted to them.

[101] At no time during the Authority's investigation did the respondent produce evidence that the applicants were fully appraised of their responsibilities prior to access being granted. That is a significant matter since the company states in its webmail policy that *these terms and conditions are a **contract** between you and Air New Zealand Limited* (emphasis is mine). The questions posed are simply, how can one become a party to a contract when one is not given the terms of the contract, and how can one be punished for failure to adhere to unknown terms of a contract?

[102] The Authority commends the company for establishing appropriate policies and protocols in respect of its email and internet facilities. Such policies and protocols are essential to maintain the system's integrity and the good name of the airline.

[103] In its defence, the respondent asserted in evidence that it sent regular reminders to staff about their obligations when using the company's IT systems. The Authority accepts that evidence, but notes that a number of updates preceded the applicants' access to the full IT system and may well have been dismissed by the applicants as irrelevant to them at that time. The reminders posted on the company's Korunet were cited in evidence. However, Mr Mangos conceded that at the relevant time the link to this reminder was indirect but had been upgraded to a direct link following the incident involving the applicants. The Authority also accepts the evidence of the respondent that at various times notices were posted on staff noticeboards. Again, the risk is that not all staff read staff noticeboards. In short, neither method of communication is guaranteed to find every employee. There is no substitute for a full and unequivocal induction process which leaves no room for any doubt in any employee's mind.

[104] Following the release of two personal grievance actions investigated in the Auckland office of the Employment Relations Authority (*Cliff v. Air New Zealand Ltd* AA1A/05 and *Groom v. Air New Zealand Ltd* AA1B/05), counsel for the respondent forwarded copies of these determinations to the Authority member. Having studied those determinations, the Authority finds that they are clearly distinguishable on the facts. Mr Groom accepted that he was aware of the company's IT policy, while Mr Cliff accepted he was aware of the prohibition on accessing sexually explicit sites. The issue of shared access information featured in neither case.

[105] In the course of the Authority's investigation of these matters, the applicants alleged that they were significantly offended by a small piece on the front page of the *Christchurch Press* shortly after the dismissal of the applicants. They felt aggrieved with what they believed were unnecessary comments made by the airline's Chief Executive which would have led to a reasonable suspicion about the reasons why the applicants had been dismissed and that this put them in an unfair situation. The respondent replied that the article did not name the division in question nor did it personally identify any of the applicants. Further, it produced a union document which it said had been posted on staff noticeboards at the Christchurch site identifying the four applicants by name. The Authority, having considered this matter, is of the view that both may have been injudicious. The Authority believes that the action of Mr Mangos advising all other warehouse employees in Christchurch of the applicants' identity and the reasons for their dismissal was an action open to him as he appears to have been reporting only on a series of facts.

Legal principles

[106] The test for justification of the dismissals is as set out in *W&H Newspapers Ltd v. Oram* [2002] 2 ERNZ 448. The question essentially posed is, was the decision to dismiss the applicants

one which in all the circumstances a reasonable and fair employer could have taken? The Authority must also bear in mind that the employer's conduct of the disciplinary process is not to be put under a microscope nor subjected to pedantic scrutiny, nor an unreasonably stringent procedural requirement to be imposed. The approach is as set out in *New Zealand (with exceptions) Food Processing etc IUOW v. Unilever New Zealand Ltd* [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 overly indulgent person.*

The determination

[107] Having carefully and at length considered the evidence before the Authority, I find that given the extensive misuse of computer access, it was unsafe for the respondent to reach the conclusions it did in respect of the applicants.

[108] I find the failure of the respondent to adhere to its own well-designed procedures in regard to internet access and in particular its insistence that access to its IT systems formed a contract with the applicants, failed because the respondent granted IT access without advising the applicants of their obligations under the so-called *contract*.

[109] I find that the respondent failed to further investigate the claim of all four applicants that the sharing of system access data was very widespread and that had it done so it would, on the balance of probabilities, found it credible that persons other than the applicants had accessed the sites the respondent found to be in breach of its policies. In the light of this and the overall evidence before the Authority the respondent's reference to its loss of trust and confidence in the applicants cannot fly when the fundamental breach was on the part of the respondent.

[110] I find that the respondent failed, particularly in respect of Mr Bisson, to take into account not only his long, committed service, but also the commendation he received in respect of his contribution to the SAFE project in early 2004.

[111] I find that the respondent, in refusing an application to adjourn the final meeting with Mr King pending receipt of further information, prejudiced Mr King and on the balance of probabilities the other applicants. I can understand how the company representatives would be irked by extending its process. However, the provision of the extensive evidence in respect of log on and password sharing later produced by the Union may have had a very significant effect on the respondent's deliberations and view of the matter.

[112] Having made these findings, I want to record the Authority's clear understanding of the respondent's honest commitment to deal with its investigation in a correct and timely manner. The task of investigating the alleged breaches was inevitably protracted and involved significant time and expense for the company. The Authority accepts the earnest and honest attempts of Air New Zealand to fulfil its obligations.

[113] I find each of the applicants was unjustifiably dismissed.

Remedies

[114] Having found that each applicant has been unjustifiably dismissed I must now turn my mind to remedies. In respect of the applicants' claims for lost remuneration, the Authority received evidence from each applicant detailing his loss of remuneration between the time of dismissal and the order for interim reinstatement. I am satisfied that each has advised the Authority of income earned from other employment in the period in question, and I have taken account of those earnings.

Mr Bisson

[115] Mr Bisson is to be reinstated to his former position with no loss of seniority or benefits. The respondent is to pay Mr Bisson the sum of $23,040 in respect of wages lost as a result of his personal grievance.

[116] The respondent is to pay Mr Bisson the sum of $7,000 without deduction as compensation under s.123(1)(c).

Mr Gardner, Mr Cameron and Mr King

[117] These three applicants are to be reinstated to their former positions, or to positions no less advantageous with no loss of seniority or benefits.

[118] The respondent is to pay Mr Gardner the sum of $13,768 gross in respect of wages lost as a result of his personal grievance.

[119] The respondent is to pay Mr Gardner the sum of $3,000 as compensation pursuant to s.123(1)(c).

[120] The respondent is to pay Mr Cameron the sum of $17,134 in respect of lost wages resulting from his personal grievance.

[121] The respondent is to pay Mr Cameron the sum of $3,000 as compensation pursuant to s.123(1)(c).

[122] The respondent is to pay Mr King the sum of $6,753.75 gross in respect of wages lost as a result of his personal grievance.

[123] The respondent is to pay Mr King the sum of $3,000 as compensation pursuant to s.123(1)(c).

Costs

[124] Costs are reserved. The parties are to attempt to resolve the question of costs between them. However, if they are unable to do so, Mr Little is to lodge and serve his submissions on or before 1 August 2006. Mr Kiely is to file his memorandum on or before 15 August 2006.

Paul Montgomery
Member of Employment Relations Authority