The Internet has provided employees and organisations with many benefits. However, employee misuse of Internet services has also become increasingly common. A solution to combating this problem is the implementation of an Internet Use Policy (IUP) within an organisation. This study developed IUP guidelines that were used to evaluate existing Victorian local government authority (LGA) IUPs. The number of LGAs without policies was then determined in February 2001. The findings revealed 36 per cent of Victorian LGAs did not have an IUP implemented. Fifty-one per cent of rural LGAs were found not to have IUPs. Furthermore, policies when compared with the IUP guidelines revealed deficiencies in many areas. A follow-up review was then conducted in 2004. It revealed that only 6 per cent of LGAs now lacked policies.

The purpose of an Internet Use Policy (IUP) is to inform employees of what constitutes acceptable use of employer provided Internet services. The policy is often referred to as an IUP or an Acceptable Use Policy (AUP). The study by Roman (1996) revealed that even in the early days of the Internet, about 50 per cent of company management were concerned about the issue of unacceptable Internet use. The consequences that may arise from unacceptable use include loss of productivity (‘cyberloafing’), increased service costs, increased risks of litigation and damage or loss of data (Siau 2002; Lim 2002; Han 2000; Buckley and Green 2000; Dunten 1999). Verton (2000) highlights a loss of employee productivity of 30 per cent to 40 per cent due to inappropriate Internet use. A survey of 100 workers in the US revealed that 64 per cent of employees ‘surf’ the Internet for personal reasons during the working day (The Straits Times 2000). Vault.com (1999) suggested that Internet surfing for personal use might be as high as 80 per cent to 90 per cent.

Background

According to Phillips (2001), numerous incidents of inappropriate use of employer email and web use within Australia have been reported. These include:

- March 2000 — six staff were dismissed from Centrelink in Adelaide for distributing sexually explicit material using the Internet.
- July 2000 — employees at Holden were caught sharing sexually explicit material; four were dismissed sparking industrial unrest.
- September 2000 — a similar incident occurred at Toyota, as at Holden, with industrial unrest resulting from the disciplinary action.

The impact of an IUP is one that concerns both employers and employees. Some employees express unease about infringement of privacy or whether it guarantees due process protection in relation to alleged policy breaches (Ginder 1999; Privacy International 1999; Casser 1996; Kadie 1991). Studies such as Schulman (2001) reveal that 35 per cent to 40 per cent of organisations systematically monitor employee use of network services and that monitoring is increasing. The technology used to monitor employee use is becoming very sophisticated (Schulman 2001; Conry-Murray 2001; Berkley 2000). At its simplest, employers have the right to monitor, but employees should be informed of this taking place (Office of the Federal Privacy Commissioner 2000; Cassar 1996).

The issues surrounding Internet use affects all organisations including local government (LG) and their employees. The issue of recreational use of the Internet in the workplace has
been made (Oravec 2002). It is important that local government authorities (LGAs) have an effective policy and one that addresses these concerns. It is recognised that these concerns are not mutually exclusive and ‘trade-offs’ will have to be accommodated when formulating the IUP. One example of a ‘trade-off’ is between employee privacy and monitoring of employee communications to ensure compliance with the policy.

An examination of the literature reveals a paucity of research regarding IUPs and that no study related to LGAs in Australia has been undertaken. The most relevant research was that conducted by Sandy (2000) concerning Acceptable Use Policies of Australian Universities. By conducting this study, it is expected that the findings will assist LGAs in the following ways:

First, this study will raise awareness of the issues and significance of implementing an IUP within LGAs. It will provide LGA representatives with knowledge and a framework to communicate to its representatives, the importance of such a policy. It will also influence standards bodies in developing a model IUP, as currently one is not available.

Second, for LGAs that have implemented policies, this study will provide them with guidelines that can be used when re-examining their own policies. It will also act as a reminder for LGAs to review their existing policies and update any areas if necessary.

Third, for LGAs that have not implemented an IUP, this study will provide reasons to implement a policy and provide them with a model policy. The development of a policy can be complicated. However, by providing a framework, the task of creating an IUP will be simplified.

Finally, the findings will help foster better policy development, ultimately ensuring the issues faced due to inappropriate use of Internet services are minimised in the workforce. The model IUP and guidelines to assist in the preparation of an IUP are available by request from the authors.

Research purpose

The primary aims of this study were to:

- Identify and document IUP guidelines to be used when formulating IUPs for LGAs.
- Obtain IUPs from each Victorian LGA and evaluate each policy against the IUP guidelines.

In addition, the subsidiary aims of this study were to:

- Identify LGAs that lacked a formal IUP.
- Compare the number of policy implementations of metropolitan LGAs with the Rural LGAs.

Research method

All 78 Victorian LGAs were contacted and a copy of their IUP, if it existed, was obtained. In order to obtain policies, the technique selected for the collection of policies was the telephone interview. Based on Jankowicz (1991) findings, telephone interviews enable the capture of personal views and values of the respondent. During telephone conversations conducted with LGA contacts, a series of unstructured questions were asked. For example:

1. Whether the purpose of the IUP was known.
2. Was the policy available for staff to access? If so, was its location known?
3. How was the policy developed and approved?
4. Whether formal policy training had been conducted.

For LGAs that lacked a formal policy, questions were directed towards future intentions of implementing a policy.

Once all available policies were obtained, each IUP was systematically evaluated against the IUP guidelines. Formation of the IUP guidelines was achieved by reviewing literature in relation to IUPs. In addition, organisations closely associated with Victorian LGA, the Municipal Association of Victoria, National Office of Local Government, Australian Local Government Association and Standards Australia were contacted for information on IUPs.

The IUP guidelines provide a framework for the creation of a LGA IUPs and promote the development of a policy that communicates effectively to users. The IUP guidelines used to evaluate the existing IUPs are outlined in Table 1, together with authoritative sources.

Data collection

Internet use policy guidelines

A review of the literature and information from diverse sources, including Internet Magazines,
Table 1 Internet use policy guidelines

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Communication effectiveness. In common with all policy documents, the IUP should satisfy the principles of effective communication. These include that it be written in a positive tone, be unambiguous, minimise redundancy and eliminate extraneous information (Dunten 1999; Sandy 2000).</td>
</tr>
<tr>
<td>2</td>
<td>Version. Each policy must contain version identifiers and authorisation details including the last update (Sandy 2000).</td>
</tr>
<tr>
<td>3</td>
<td>Statement of purpose. A succinct explanation of the purpose of the policy, how the policy was developed and the person(s) responsible for developing and administering the policy (Sandy 2000).</td>
</tr>
<tr>
<td>4</td>
<td>Acceptable use. An unambiguous statement detailing what constitutes acceptable use of Internet services. If conditional personal use is accepted then the conditions should be clearly stated (Electronic Frontier Australia (EFA) 2000; Sandy 2000).</td>
</tr>
<tr>
<td>5</td>
<td>Unacceptable use. An unambiguous statement detailing what constitutes unacceptable use of Internet services. Logically this should not be required in addition to Acceptable Use. However, it can reinforce what is not permitted (Buckley and Green 2000; EFA 2000; Sandy 2000; Woodhead 1999).</td>
</tr>
<tr>
<td>6</td>
<td>Downloading of software. Any employee download rights granted must be explicitly stated and its scope indicated (Buckley and Green 2000; Dunten 1999).</td>
</tr>
<tr>
<td>7</td>
<td>Copyright and trademarks. A statement should stipulate that no employee should copy, retrieve, modify or forward any material that is either copyrighted or trademarked without permission from the holder. Employees breaching copyright or trademark rules will be held directly responsible (Dunten 1999).</td>
</tr>
<tr>
<td>8</td>
<td>Privacy and management of email. A statement should include a reference to the users right to privacy, personal information captured, the lack of Internet security and how employee communications are managed. However, an organisation should have a separate privacy policy (Australian Privacy Commissioner (APC) 2000; Benson 2000; EFA 2000; Sandy 2000; Swarbrick 2000).</td>
</tr>
<tr>
<td>9</td>
<td>Monitoring and enforcement. A statement on the nature and scope of monitoring of employee use of services should be clearly stated. Specifically, employees should be informed if explicit surveillance is operative (APC 2000; EFA 2000; Dunten 1999).</td>
</tr>
<tr>
<td>10</td>
<td>Due process. A clear statement of the process of why, when, where, how and whom disciplinary actions are taken against those breaching the policy. It includes reference to initiation of a breach, hearing the case, penalties imposed, right of appeal and legal aspects (APC 2000; EFA 2000; Sandy 2000).</td>
</tr>
<tr>
<td>11</td>
<td>Policy changes. The policy should be reviewed on a regular basis to ensure that it be kept up-to-date with changes in Internet technology. The policy should also address when policy reviews are conducted, when employees are notified of the modifications, the reason for the modifications, the authorising person and the number days before an updated policy is enacted (APC 2000; EFA 2000; Sandy 2000).</td>
</tr>
<tr>
<td>12</td>
<td>User agreement. Before any employee is permitted use of the Internet, the policy must be issued and explained to the employee requiring Internet access and formally assented to. Once understood, the employee must then sign the policy. The policy must state this and contain a section where employees sign and agree to the terms outlined in the policy. The employee’s manager must also sign the policy. Both parties must sign the policy before Internet access is permitted to the employee (Buckley and Green 2000; Dunten 1999).</td>
</tr>
</tbody>
</table>
Legal Firms and Human Resources Guides were used to document the IUP guidelines. Primary source documents used to document the guidelines include:

- Similar research conducted by Sandy (2000) on Acceptable Use Policies of Australian Universities.
- The Guide on Workforce Email, Web Browsing and Privacy published by the Australian Privacy Commissioner (2000).

Acquisition of LGA IUPs
All 78 LGAs were contacted by telephone and policies were collected from the 15th of November 2000 until the 15th of February 2001. The response rate achieved was 100 per cent. Assurance of confidentiality was the most important determinant of the very successful response rate.

2004 policy review
To establish if LGAs reviewed their policies, follow-up calls were undertaken in January 2004. A sample, of 12 percent of LGAs, was selected to conduct this follow-up. Each LGA in this sample was contacted by telephone and asked the following:

a) Whether their policy had been reviewed since February 2001.
b) If a review has occurred, when was this performed and were there any changes made to the policy?

In addition, LGAs that did not have policies implemented in February 2001 were contacted and asked if they had now implemented an IUP. These newly implemented policies were not obtained and not evaluated against the IUP guidelines.

Data analysis
The information received from each LGA, including their IUP, was analysed using qualitative techniques. The analysis involved the use of simple arithmetic and calculation of percentages. The use of sophisticated quantitative techniques was not required for this study. All policies obtained were systematically reviewed in accordance with the IUP guidelines. In addition, anecdotal information was captured during telephone conversations.

Findings
The major findings of this study are now discussed:

Policy statistics
1. Organisations closely associated with Victorian local government including Municipal Association of Victoria, National Office of Local Government, Australian Local Government Association or Standards Australia did not possess guidelines, models or standards relating to IUP. No legislation existed that required an LGA to implement such a policy.
2. As shown in Table 2, 64 per cent of LGAs had implemented IUPs. Of those that had not implemented a policy, 6 per cent of LGAs indicated implementation of an IUP would occur within the year 2001.

Table 2  LGA policy implementations

<table>
<thead>
<tr>
<th>LGs</th>
<th>Number of LGA</th>
<th>Percentage of LGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Policies</td>
<td>50</td>
<td>64</td>
</tr>
<tr>
<td>Without Policies</td>
<td>28</td>
<td>36</td>
</tr>
<tr>
<td>Total</td>
<td>78</td>
<td>100</td>
</tr>
</tbody>
</table>

3. It can be seen from Table 3, 51 per cent of Rural LGAs lacked an IUP compared with 13 per cent for Metropolitan LGAs.

Anecdotal findings
Telephone conversations undertaken with LGA employees revealed issues in relation to IUPs. The following findings were based on random employee responses. Employee responses originated from various departments being IT, reception, finance, administration and human resource staff.

- Approximately 50 per cent of LGA employees when asked if their organisation had implemented an IUP responded, ‘they were not sure’.
Table 3 Metropolitan vs rural LGA Internet use policy implementations 2001

<table>
<thead>
<tr>
<th>LGs</th>
<th>Number of metropolitan LGAs</th>
<th>Percentage of metropolitan LGAs</th>
<th>Number of rural LGAs</th>
<th>Percentage of rural LGAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Policies</td>
<td>27</td>
<td>87</td>
<td>23</td>
<td>49</td>
</tr>
<tr>
<td>Without Policies</td>
<td>4</td>
<td>13</td>
<td>24</td>
<td>51</td>
</tr>
<tr>
<td>Total</td>
<td>31</td>
<td>100</td>
<td>47</td>
<td>100</td>
</tr>
</tbody>
</table>

- Of LGAs that had implemented policies, approximately 20 per cent of employees contacted were unsure of the location of their policy. Employees had to contact other staff and seek assistance in order to determine the whereabouts of their policy.
- Approximately 40 per cent of employees indicated that no formal training had been conducted in order to educate employees on the policy contents.
- The development and implementation of an IUP within 60 per cent of LGAs was found to be the responsibility of the IT department. The remainder of LGAs believed it was the responsibility of human resources and the department of corporate services.
- Of the employees contacted, 90 per cent indicated that they were familiar with the purpose of an IUP.

Evaluation of Internet use policies
The 50 Victorian LGA IUPs obtained were then evaluated against the IUP guidelines. The policies obtained varied in page length. Policies ranged from half a page to 23 pages. The mean page length of policies equated to five. Although most policies were written in an idiosyncratic manner, many policies were very similar. Some policies also contained identical statements and two documents were found to be virtually identical. The major findings of the policy evaluation were as follows:

1. Communication effectiveness. The communication effectiveness of each IUP involved a judgment made about ‘positive tone’, ‘ambiguity’, ‘redundancy’ and ‘extraneous material’. It was found that 58 per cent of the policies were positive in tone. This was especially evidenced by the introduction of the purpose of the policy, making reference to the benefits of the Internet services and concentrating on the ‘Do’s’ rather than the ‘Don’ts’ in terms of Internet use. Twenty-eight percent of policies frequently used ambiguous terms like ‘frivolous’ and ‘offensive’ or phrases like ‘Messages must not contain any content offensive to the person who is being sent the message’. The use of the term ‘Internet’ in many policies was poor, out of context and lacked a definition and scope. Most policies when stating the term ‘Internet’ used it to describe the World Wide Web (WWW). Technically, this is not correct as the Internet encompasses the WWW and does not simply refer to the WWW. The few policies that did define ‘Internet Use’ stated that the Internet included WWW, email and other Internet services such as file transfer protocol and newsgroups. Also a third of policies contained extraneous material not directly related to acceptable Internet use. Examples include the records management and retention process, Internet access costs and details regarding the anti-virus software used. The evaluation also revealed other areas of concern. For example, many policies had a tendency to scatter statements in relation to one area over a number of different pages and sections, making it difficult and confusing to read. Many policies also contained contradictory statements.

2. Version. Sixty per cent of policies failed to include both the version details of the policy and the authoriser of the policy. When evaluating the method used to display the policy version, it was found that either a
An Evaluation of Internet Use Policies of Victorian Local Government

version number or date was used, the latter being the preferred option. An analysis was also conducted to determine when the policies were created. It was identified that 29 policies contained a version date. The years in which the policies were developed is outlined in Table 4.

Table 4 Year of policy development

<table>
<thead>
<tr>
<th>Year policy developed</th>
<th>Percentage of policies developed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>58</td>
</tr>
<tr>
<td>1999</td>
<td>35</td>
</tr>
<tr>
<td>1998</td>
<td>7</td>
</tr>
</tbody>
</table>

3. Statement of purpose. The majority of policies contained a statement of purpose. Few indicated who was responsible for the policy and even less made reference to how it was developed or updated. Table 5 details the results of the evaluation. These results are also mutually exclusive of one another:

Table 5 Statement of purpose results

<table>
<thead>
<tr>
<th>Statement of purpose</th>
<th>Percentage of policies addressing area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of policy</td>
<td>88</td>
</tr>
<tr>
<td>How policy was developed</td>
<td>4</td>
</tr>
<tr>
<td>Members responsible</td>
<td>22</td>
</tr>
</tbody>
</table>

Not all LGA IUPs covered all areas of Internet use. The evaluation found that only 54 per cent of policies addressed both email and WWW use. Some LGA policies contained statements regarding the use of email and the WWW in separate documents. These documents also contained duplicate data that could have been encapsulated into one policy. The types of policies reviewed are illustrated in Table 6.

Table 6 Types of LGA Internet use policies

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Percentage of policies addressing area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>14</td>
</tr>
<tr>
<td>WWW</td>
<td>2</td>
</tr>
<tr>
<td>Email and WWW</td>
<td>54</td>
</tr>
<tr>
<td>Email and intranet</td>
<td>2</td>
</tr>
<tr>
<td>Email, WWW, IT telephones</td>
<td>14</td>
</tr>
<tr>
<td>Separate email and WWW policies</td>
<td>14</td>
</tr>
</tbody>
</table>

4. Acceptable use. Acceptable use should be explicitly stated in unambiguous terms. In evaluating the IUPs, 48 per cent of policies contained ambiguous statements about acceptable use. For example, ‘Internet access is provided for supporting and conducting Council business. In relation to acceptable personal use, 78 per cent stated that personal use was permitted under certain conditions. However, these conditions were often undefined.

5. Unacceptable use. Areas of unacceptable use, displayed in Table 7, highlights the frequency of reference in each IUP to unacceptable behaviour. Comments relating to socially belligerent or objectionable use were most often noted.

6. Downloading of software. Most policies permitted the downloading of files from the Internet but did not prohibit the downloading of software. Policies simply warned users to be cautious when downloading files due to the risk of computer viruses and insisted that users check all files downloaded with a virus scanner before use.

7. Copyright and trademarks. The evaluation of LGA IUPs revealed that most policies did not address both copyright and trademarked material as per the IUP guidelines. The evaluation identified the following: 58 per cent discussed copyright whereas 6 per cent discussed both copyright and trademarks.
Policies that did discuss copyright and trademarks did so while listing actions considered unacceptable. Statements made were usually simplistic such as, ‘Infringement of copyright laws is prohibited’. Most policies did not direct users to obtain permission from the holder of the copyright or trademark and did not state that employees would be held directly responsible for copyright breaches.

8. **Privacy and management of email.** Based on the guidelines, the evaluation of policies revealed that 12 per cent of LGA IUPs did not address privacy. Of the policies that did address privacy, only few covered all privacy areas. Table 8 outlines the results of the privacy evaluation.

9. **Monitoring and enforcement.** Most policies indicated that all material created, acquired or maintained within their organisation was the property of the organisation. Furthermore, most IUPs indicated that network communications were not private and could be accessed by the employer. A few policies were specific about what could be accessed and under what circumstances. Three quarters of the LGAs stated that employee Internet use was monitored and for most, this was a condition of signing the policy. The main reason for monitoring was to enforce compliance. However, other reasons included cost analysis, security, technical maintenance or problem resolution.

10. **Due process.** Most policies did not address the issue of due process for non-compliance when evaluated against the IUP guidelines. Most simply stated that a policy breach would result in disciplinary action. Only 30 per cent of IUPs referred to how breaches were initiated and how a hearing into an alleged breach would be conducted. No IUPs referred to a right of appeal. However, some IUPs cross-referenced to other policy documents that detailed due process for policy breaches. The most common type of penalties referred to were written warnings, counselling or removal of Internet privileges. Few policies attempted to match the type of breach with the severity of the discipline.

11. **Policy changes.** Policies were grossly inadequate in this area, as 85 per cent of policies did not discuss policy reviews. Many policies stated that amendments would not be communicated to employees before implementation. Of the policies that did record review details, the following time frames were identified: six-monthly, annually, within two years or within five years. Though review times were included, not all policies adhered to these. One policy noted that reviews would be conducted annually. However, the policy had not been reviewed or updated in over three years.
12. **User Agreement.** The evaluation of the LGA IUPs indicated that 40 per cent of policies did not require employees to sign the policy and to obtain authorisation before being granted Internet access. Instead, employees were automatically provided Internet access without having to read and agree to the terms and conditions stipulated in the IUP. Policies that did not contain a formal user agreement form simply stated that it would be the responsibility of the organisation to make all employees aware of the policy and any modifications. It would also be the responsibility of all employees to comply with the policy.

**Discussion**

The study of Victorian LGAs IUPs revealed a number of important policy deficiencies when evaluated against the IUP guidelines. The IUP guidelines discussed in this study together with the findings provide a means by which these deficiencies may be rectified for each LGA. This study also confirms the choice of personal contact through the telephone as an effective technique to gather the relevant information.

It was alarming that 28 LGAs (36 per cent) should lack a formal IUP given the ubiquity of the Internet and the importance of email to public and private sector organisations. Somewhat less surprising was that most lacking a policy were Rural LGAs, many of which had only recently provided the services of the Internet to their employees. All LGAs lacking a policy should rectify this situation immediately and prepare one in accordance with the IUP guidelines. Implementing the policy will minimise the effect of cyber bludging and the exposure to lawsuits. Furthermore, the implementation of an IUP will minimise the threat of copyright-infringement suits to the LGA from unacceptable downloads of files by employees.

Although 64 per cent of all Victorian LGAs had implemented policies, anecdotal evidence raised two significant concerns. First, 50 per cent of employees interviewed were unsure as to whether their organisation had implemented a policy. Second, 40 per cent of employees stated that they had not received any formal training regarding their IUP.

There are significant legal ramifications that may arise as a result of insufficient training. Failure to communicate and educate a policy to employees could render a policy useless and fail to protect an organisation from litigation. Organisations attempting to dismiss an employee for breach of policy could potentially be defeated in court due to the policy not being adequately communicated or explained to staff. Furthermore, organisations attempting to dismiss an employee for distributing offensive material may not always be protected by their policies in an unfair dismissal case. As described by Norington (2002), two police officers were reinstated after Justice Roger Boland, of the NSW Industrial Relations Commission, ruled it was unreasonable to sack the officers. It was found that others did not regard the pornographic material distributed by the officers as unwelcomed or offensive.

It follows from the findings of the study that LGAs with existing policies should undertake a review of their policies, in accordance with the policy guidelines, and make amendments where necessary. Specifically, the findings suggest the following:

- Policies should be rewritten in a positive tone and should minimise the use of ‘do not’ statements. Understanding of the policy and minimising the possibility of misinterpretation is also promoted by eliminating ambiguity, repetitive and extraneous material.
- Most policies failed to include a policy version number. Failure to add a version number could result in users inadvertently viewing superseded policy versions.
- Most policies failed to address both email and WWW use within a single document. By addressing both email and WWW use within the one umbrella document, the possibility of duplication, confusion, redundancy and incomplete policy documents is minimised. Furthermore, there is no need for separate documents for email and WWW use.
- Many policies contained download statements but did not prohibit the downloading of software. Permitting such practice could subject the organisation to licensing violations or network disruptions.
- If acceptable use is identified and clearly defined then a discussion of unacceptable use is superfluous. However, it is recognised that identifying and clearly defining the most serious use of services for non-business
purposes may assist with user understanding of their rights and responsibilities when using the Internet services.

- Policies need to clearly define what constitutes acceptable use of all Internet services. For instance, limited personal use should be permitted but what constitutes ‘limited’ must be unambiguously defined.
- Copyright and trademarks must be addressed within policies. For example, policies should state that employees should not copy, retrieve, modify or forward copyrighted materials unless permission is granted. Failure to do so could result in LGAs being directly responsible for breach of copyright or trademark.
- Legal precedents worldwide suggest that employers have greater success in disciplining an employee for unacceptable Internet use if they possess an IUP. If the employer has explicitly informed staff that authorised monitoring was conducted to detect policy breaches, action can be taken against the offending employee. More attention should be given to resolving this issue by the LGAs.
- Policies should address in detail the due process that should follow an alleged breach of policy. The essence should be contained in the IUP document but be cross-referenced to a document setting out due process in detail. The detailed document, given its nature, would have to withstand a legal challenge. To put all the detail in the IUP would be counter productive. This also applies to government legislation. The IUP should only cross reference to the relevant legislation such as the Classification, Copyright, Discrimination, Freedom of Information and Privacy Acts.
- No employee should be authorised to access any Internet services until they have explicitly assented to the IUP and have been given ‘training’ in its use.
- Failure to notify employees of policy changes could potentially result in LGAs not having sufficient grounds to dismiss an employee. Policies are not static documents. They require periodic revision to accommodate changes in technology and legislation.

2004 Policy review update

An update to this study was conducted in January 2004 to specifically look at LGAs that previously lacked a policy and to determine the frequency of policy reviews. This study when initially conducted in 2001 revealed that 36 per cent of Victorian LGAs lacked an IUP. In order to determine if these LGAs still lacked policies, each were contacted again in January 2004 and asked if they had a policy. The findings revealed a significant decrease in the number of LGAs without policies. Since February 2001, 30 per cent of LGAs implemented an IUP. However, 6 per cent of LGA’s still lacked IUPs. Table 9 outlines the findings.

<table>
<thead>
<tr>
<th>Table 9 2004 LGA policy implementations</th>
</tr>
</thead>
<tbody>
<tr>
<td>LGs</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>With policies 2001</td>
</tr>
<tr>
<td>Without policies (excluding drafts) 2001</td>
</tr>
<tr>
<td>With policies 2004</td>
</tr>
<tr>
<td>Without policies (excluding drafts) 2004</td>
</tr>
</tbody>
</table>

These findings were analysed further to determine the number of metropolitan versus rural LGA implementations taking into consideration draft policies. As per the findings in 2001, rural LGAs still accounted for the greatest percentage of LGAs without policies (refer to Table 10). Two LGAs stated that they had not implemented an IUP but had developed draft policies. These drafts were pending final approval by council.

The evaluation of LGA IUPs conducted in 2001 exposed deficiencies that existed with implemented policies. To determine if LGAs reviewed their policies, a sample was selected that consisted of 9 LGAs representing both rural and metropolitan LGAs. This group was contacted and the findings detailed in Table 11.

It was found that 67 per cent of the sample group had not reviewed their policies since February 2001. Of these, one LGA had a policy
that dated back to August 1999, but did affirm that it would review its policy in three months time. Two LGAs that reviewed their policies indicated that annual policy reviews were conducted. The other LGA had last reviewed their policy in July 2001. When asked if any changes were made to their policy, two responded ‘yes’, with one stating that a change was made in relation to viruses.

**Conclusion**

Based on the findings of this study, it is strongly recommended that all Victorian LGAs undertake a review of their policies in terms of the IUP guidelines. Policies should be revised with full involvement of all relevant stakeholders in line with the IUP guidelines. For LGAs lacking a policy, action should be taken immediately to develop and implement a policy, using the IUP guidelines as a framework for the creation of an IUP.

**Table 11 Sample policy reviews**

<table>
<thead>
<tr>
<th>Sample review status</th>
<th>Number within sample</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not reviewed since 2001</td>
<td>6</td>
<td>67</td>
</tr>
<tr>
<td>Reviewed since 2001</td>
<td>3</td>
<td>33</td>
</tr>
</tbody>
</table>

**References**


Berkley, T 2000 ‘Peeping tools: Nine tools that can snoop on your employees’, Network World, 10 July.


Han, H 2000 ‘Email not so business-critical’, Network World Today, 26 June.


Lim, V, T Teo & G Loo 2002 ‘How do I loaf here?: Let me count the ways’, Communications of the ACM,


The Straits Times 2002 Cyberslackers at Work, 28 April.

