Acceptable Use Policies for Networked Services: Australian Universities

Geoffrey A Sandy

School of Information Systems
Victoria University of Technology
Melbourne, Australia
Email: Geoff.Sandy@vu.edu.au

Abstract

Organisations, including Universities, develop policy to manage the use of their network services. It describes what is acceptable and what is unacceptable behaviour of the network users. The policy may be referred to as "Acceptable Use Policy" (AUP). Network users express concerns about how these policies may affect them. In particular, there is a concern about infringement of privacy and lack of due-process protection in hearings for alleged non-compliance. Academic staff and students of a University are also concerned about the possible violation of academic freedom. This work describes how the AUPs of Australian Universities are evaluated against "Best Practice" principles. The findings demonstrate that users concerns are well founded. The majority of AUPs are seriously deficient when evaluated against these "Principles" and should be extensively amended so that they are in accord with them.

Keywords

BD0104 Ethical Issues BD0105 Privacy BD0106 Discrimination DA 09 Organizational Procedures

INTRODUCTION

Organisations develop policy to manage the use of their network services. It is referred to as an Acceptable Use Policy (AUP) or similar wording. Its main purpose is to describe what is permitted and what is not permitted in use of the network. This paper adopts the term AUP.

An important employer concern is the consequences that can arise from unacceptable behaviour by employees using networked services. Unacceptable behaviour may be unlawful, unethical or incompetent for instance. It can result in a loss of productivity, increased costs of service provision, increased risk of litigation, and damage or loss of data and systems. University management shares this concern and also develop policy to manage the use of the network by staff and students.

Employees have concerns about the policy itself and how it may affect them. Specifically, whether an AUP infringes privacy or whether due-process protection is provided in relation to hearings on alleged non-compliance. University staff and students also share these concerns but are also concerned about infringement of "academic freedom". An AUP may compromise this freedom through censorship and impose penalties for behaviour that should be "acceptable" for a University. If a University is to function as such then academic freedom must be guaranteed and not compromised by an AUP. Academic freedom makes a University "different" from other organizations (Merel 1996; Yee; AAUP 1992).

RESEARCH PURPOSE

The primary purpose of this research is to evaluate Australian University AUPs against "Best Practice" principles. These principles reflect a network user's perspective. Specifically, that of academic staff and students. These principles are also relevant for university management and information technology services (ITS). The latter have the responsibility to implement the policy.

RESEARCH HYPOTHESIS

The research hypothesis is that the AUPs are not in accord with these principles. The consequences of this are that users may be adversely affected. This includes the violation of academic freedom and infringement of privacy. It may also result in the denial of natural justice through a lack of due process protection on hearings for alleged breaches of policy, and from policy ambiguity. The penalties for breaches of policy by users are serious and include dismissal from employment or exclusion from a course or subject, litigation to recover losses and fines. Users (and management) therefore should be concerned that an AUP be in accord with the "Best Practice" principles.

This paper reports on an analysis of Australian University AUPs and an evaluation against "Best Practice" principles. This work has not been undertaken before. First, the research process adopted is described. Then the principle are identified and discussed. Next, the AUPs are analysed and evaluated against these principles. Finally, the major conclusions of the research are discussed.

To improve readability two citation conventions for the AUPs are adopted. First, each University is referred to by an abbreviated name. These are found in Appendix 1 *Australian Universities Acceptable Use* Policies. Second, when reference is made to "most AUPs" or similar wording four citations are given as illustrative from a larger number.

RESEARCH PROCESS

The research process consisting of five main activities is now described together with the results of each.

Literature Review

First, a review of AUPs, policies relating to AUPs and other related literature is undertaken. It includes American Universities, a few key British Universities, and other institutions. The policies of the following organizations are sought because they are likely to express a user perspective in relation to acceptable network use. The organizations are the National Tertiary Education Union (NTEU), National Union of Students (NUS), Council of Australian University Information Technology Directors (CAUDIT), Australian Library Information Association (ALIA), Internet Industry Association of Australia (IIAA), Australian Computer Society (ACS), American Association of College Professors (AACP) and the American Library Association (ALA).

The review reveals that the AUPs of American Universities and policies of relevant American organisations, like the AACP and ALA are easily accessible. Less accessible are AUPs and policies from Britain and Australia. The peak body representing academic staff (NTEU) and that for students (NUS) do not have a formal policy on acceptable use. The NTEU (1988) does have a policy on privacy of electronic communications. The NUS in their Education

Policy (1999) refers to academic freedom, students' rights and privacy of personal information but without explicit reference to computer networks.

Access Australian University AUPs

An attempt is made via their website to access the AUPs for each Australian University, except the Australian Defence Force Academy, Bond University, Australian Maritime College, and Avondale College, listed on the Australian Vice Chancellor's Committee [AVCC] "Australian Universities WWW Servers". An alternative website, the Council of Australian University Directors of IT [CAUDIT] is not current and is incomplete.

Twenty-nine of the possible thirty-seven sites were successfully accessed and these are listed as *Appendix 1 Australian Universities Acceptable Use Policies*. Some AUPs were not accessible. These are the University of Ballarat, Central Queensland University, Northern Territory University, University of Southern Queensland and University of Technology, Sydney. The University of Melbourne, Monash University and Southern Cross University prohibit access to the policy by someone external.

Preliminary Analysis of the AUPs

A preliminary analysis of the AUPs is undertaken to identify their purpose and scope. In particular, it concentrates on identifying acceptable and unacceptable behaviour, the due process associated with breaches of policy, and policy data that includes author, last update, authorization and user involvement. These aspects are documented under appropriate headings.

Generate "Best Practice" Principles

"Best Practice" principles are generated from the literature and from the preliminary analysis of the AUPs. Of prime importance are the CAUDIT, IIAA, EFA and EFF sites, and ALIA(a), ALIA(b), AAUP (1992) ALA (1996). The principles are used to evaluate each AUP. They proved easy to discern and each is described in the section titled "Best Practice" principles.

Evaluation of Australian University AUPs

Each AUP is evaluated against the "Best Practice" principles. The findings are discussed in the section "Evaluation of AUPs".

BEST PRACTICE PRINCIPLES

The "Best Practice" principles are now described.

Unambiguous Statement about what is Acceptable Use

If a network is to be used, only for "approved university purposes" then this must be explicitly stated and its scope described. Reference must be to material that can be read, prepared, copied, communicated and stored, Reference must also be made to "acceptable" practices that promote efficient, effective, ethical and competent use of the network. Again, if "personal use" is permitted, and it should be, then this must be explicitly stated and its scope described.

Unambiguous Statement about what is Unacceptable Use

If acceptable use has been explicitly defined then logically, anything outside its scope must be unacceptable. Therefore, any description of what constitutes unacceptable use is redundant. Despite this, an AUP should contain an unambiguous statement about unacceptable use. This makes “doubly certain” the user understands what is and what is not permitted. It may also serve to educate users to adopt better work practices. This should not be viewed as a substitute for user training programmes in the competent use of network services.

Sandy (2000) suggests a useful classification of unacceptable activities that distinguishes between illegal, socially aggressive, socially objectionable, academic transgression, economically inefficient, unethical, incompetent and lack of etiquette. All types of unacceptable behaviour identified in an AUP listed in Appendix 1 can be classified using this system.

1 Illegal behaviour is that proscribed by federal or state legislation. The latter includes University Statutes and Regulations. Examples are intentional damage of facilities, theft of supplies, unauthorised access and slander of another person.

2 Socially Aggressive behaviour is that which is aggressive towards another user but is not regarded as illegal. Examples are to harass another person, abuse another person, intentionally offend another person and intentionally discriminate against another person. What is socially objectionable behaviour becomes socially aggressive when "offence" or "discrimination" towards another person is done intentionally and probably repeatedly against the wishes of the other person.

3 Socially objectionable behaviour is that which is likely to be found objectionable based on the test of the "reasonable adult". This includes reading, preparing, copying, communicating and storing legal material that is obscene, lewd, lascivious, indecent or profane.

4 Academic transgression is behaviour that involves the use of the network for collusion and/ or plagiarism and other behaviour that is directly related to academic pursuits, for example unauthorised use of university logos or intentionally misrepresenting the University.

5 Economically inefficient behaviour is inefficient use of scarce network resources whether intentional or not. This includes failure to delete excess mail, use of resource intensive internet features or home page design that is resource intensive.

6 Unethical behaviour is that which offends against professional standards of conduct. This includes holding up printer queues, commercial use and denying access to other authorised users.

7 Incompetent behaviour is incompetence in the professional use of the network. This includes unintentional damage of facilities, failure to choose a secure password or failure to report a breach of policy.

8 Lack of Etiquette is behaviour that whilst not unethical or incompetent breaches “good manners” in the use of network facilities and services, and in relation to other users. This includes eating and drinking in a shared work area and behaving in a noisy manner.

An AUP should have a complete list of all the relevant Federal and State legislation concerning “illegal” use of the network. It should not selectively quote or interpret some of the legislation. There is a possibility that this may expose the University to litigation because the advice is selective or a misinterpretation. Examples of likely offences should be given but it must be clearly stated they are illustrative only.

An AUP is premised on the assumption that the users understand the legislation. The reality is that they are ignorant of much of it, and will remain so unless they are willing to embark on an intensive study of it. Ignorance of the law is no excuse for any breach. An AUP must attempt to unambiguously state what constitutes illegal use.

Guarantees Academic Freedom

An AUP must explicitly state that the academic freedom of its users is guaranteed. It must accept that the individual user makes decisions about what is read, prepared, copied, communicated or stored. Accordingly, it is the responsibility of the user to apply the same ethical, privacy and educational considerations to the use of the network as with other communications.

Academic freedom demands that "on a campus that is free and open no idea can be banned or forbidden. No viewpoint or message may be deemed so hateful or disturbing that it may not be expressed" [AAUP 1992]. It is this freedom that more than anything else defines a University and distinguishes it from other types of organisations.

An AUP should take this as its basic premise and the policy should aim to develop knowledge and competencies of network users for a "robust" exchange of ideas. An acknowledged constraint is illegal use of the network. What should be permitted is criticism of any law including advocacy to disregard any law that is unjust. Freedom of speech is the foundation of all democratic freedoms and is intrinsic to the nature of a University.

Guarantees the Right to Privacy

The right to privacy by network users is necessary to guarantee academic freedom. Users must be confident that the University does not routinely monitor the material they read, prepare, copy, communicate and store. An AUP must state that such monitoring does not occur. It should clearly state under what circumstances material is examined, and who will authorise and conduct the examination. Any complaints of unacceptable behaviour that violates the privacy of another user should be initiated by that user and not be part of routine monitoring. The use of technology to filter selected material or identify users with such material is an infringement of privacy rights. This is censorship imposed on the user. It means that some other party, often an outside vendor, imposes their views on University staff and students.

Equal Access

All of a particular user group must be guaranteed equal access to the network according to their needs. This must be explicitly stated by the AUP. Access is not a privilege but a right.

Due Process Protection

University management has a right to impose a penalty for a specific breach of acceptable use. Users have the right to "due process protection". An AUP must clearly describe the following or explicitly cross reference to another document that does:

- What specific penalty attaches to each breach of acceptable use? – each type of unacceptable use must have a matching penalty.
- Who initiates an alleged breach? - given an absence of routine monitoring.
- Who conducts the hearing and by what authority – the person (or persons) who conduct the hearing and authorise it must be indicated.
- Who imposes the penalty and by what authority? – the person (or persons) who impose the penalty and authorise it must be indicated.
- What are the rights of all parties concerned? – the process and rights of all parties must be described. No disciplinary action must be taken before a breach is confirmed.
- How may a user appeal a decision? – the process of appeal must be described. The right of appeal must be stated.

Users fully informed of policy before use of network facilities and service

An AUP must be distributed and its contents explained to every new user before beginning use of the network. Whenever an AUP is amended, all users must be advised of the change, the reason for the change and who authorised it. The document should contain a statement to this effect.

Users informed of how the policy was developed, why it was developed and who authorised it

An AUP must indicate how the policy was developed, why it was developed and who has authorised its implementation. It must refer to the nature and extent of user involvement in policy formulation. It must indicate the author(s) and when it was last updated.

Communication effectiveness

An AUP is a written policy document and to maximise its communication effectiveness it should:

- contain a clear statement of its purpose
- avoid ambiguous terms
- be positive in tone
- minimise redundancy and eliminate extraneous material

EVALUATION OF THE AUPs

The findings of the evaluation of the AUPs against the "Best Practice" principles are now described.

Acceptable and Unacceptable Use

The AUPs describe acceptable behaviour as that being for "approved university activities" or some similar statement [VUT, LTrobe, QLD, ECowan]. This is not usually defined comprehensively. The University of South Australia is a rare example that attempts a more comprehensive definition. RMIT University is a rare example where it's AUP does not even state what constitutes acceptable use.

The overwhelming majority of AUPs explicitly do not permit personal use. Logically it makes much of the content of these AUPs redundant. This is because they describe, often in great detail "unacceptable use" that is obviously proscribed because it is personal use.

Four AUPs [LTrobe, TAS, Deakin(a), QUT] permit limited personal use of the network. They indicate that personal use must not interfere with “official” university work. Anecdotal evidence suggests that most Universities "accept" some limited personal use of the network just as the do for the telephone and photocopier. A problem for users is that enforcement of the policy can be capricious. It is akin to car "roadworthiness". If the police wish to "book" you virtually any car can be found to be unroadworthy. Such ambiguity and capricious behaviour may result in a denial of natural justice.

The content of an AUP is primarily about "unacceptable" use rather than "acceptable” use. There are dozens of different examples of unacceptable behaviour when all AUPs are considered. Great diversity exists among universities as to what constitutes unacceptable behaviour. Most AUPs are ambiguous when describing this type of behaviour. This is especially so concerning socially objectionable behaviour. The usual test of what is objectionable or offensive or obscene is to invoke that of the "reasonable adult" or "community standard". One problem is that what one person finds objectionable another does not. Sexually explicit images, for instance, may be regarded by one person as pornographic but erotic by another. There is no one identifiable community standard but many. Indeed, for a country like Australia, there is pride in its multi-culturalism. Another problem is that policies tend to adopt a conservative approach and reflects the "lowest common denominator". This is partly because university management is concerned about possible litigation from an offended user. This also is inimical to a "robust" exchange of ideas that should characterise a University.

Academic Freedom

Most AUPs [WA, Woll, Macq, Griffith] do not explicitly refer to academic freedom and how this is guaranteed for network users. The focus is on controlling the environment rather than providing users with knowledge and skills appropriate to their network needs. Universities make use of technology to filter internet sites. This can compromise academic freedom and infringe the users right to privacy. This problem is aggravated because filter technology is a "blunt" instrument and can unintentionally block many sites useful to the user.

Three AUPs refer to academic freedom. Catholic University’s AUP refers to “obligations of academic freedom” but does not expand on what this means. The University of Adelaide’s AUP contains a statement on software and intellectual rights distributed by EDUCOM a non-profit consortium of American higher educational institutions. It reads in part “Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy and right to determine the form, manner, and terms of publication and distribution”. The AUP of Swinburne University states that “the rules governing academic freedom at the University will apply to the use of the communications networks, where the objective is the transmission and pursuit of knowledge”.

Privacy

Most AUPs [VUT, USA, Murd(a), Sydney] implicitly acknowledge a users right to privacy. Victoria University's AUP states that "In certain cases the University may intercept user files and communications and provide evidence of misuse to the appropriate authority". AUPs from other universities make scant reference to this matter. Some examples are "monitor" [Woll], "take actions if necessary" [Macq] and "monitoring usage and inspect user data" (NewE). No reference is made to monitoring at all in some AUPs [LTrobe, RMIT, Flind, WA].

A better statement on privacy is from Griffith University which states "The University will not make any effort to routinely monitor the content of electronic communications or stored information (including web pages), authorised staff have every right to do so when investigating properly identified allegations of misuse and to verify compliance with applicable University regulations and State and Federal laws".

Two other points of interest are to mention again that the University of Adelaide subscribes to the EDUCOM statement on software and intellectual rights, and to note that Murdoch University's AUP [Murd(a)] has a section on OECD Information Privacy Principles.

Equal Access

Two AUPs [RMIT, Cath] explicitly refer to equality of access to the network by users. The best statement is from RMIT "these rules have been drawn up so all users can have equal access to the resources provided by RMIT ITS…". Many AUPs [JCook(a), Murd(a), Flind, LTrobe] state that the University has the right to withhold use of facilities or remove materials under certain circumstances, for instance, excessive use of bandwidth. The AUP for James Cook University [JCook(a)] states that "Nothing in these conditions shall prevent the Council of the University from withholding use of the facilities from any person for any period, for any reason or without stating a reason". Other AUPs [Ade, Curtin, Griff, Cath] refer to access to the network as a privilege not a right. The AUP of Griffith University contains the statement "Usage is a privilege, not a right" as a major heading of the document.

Due Process

Some AUPs [VUT, QLD, Sydney, ECowan] do not address due process for non-compliance beyond stating that sanctions will apply. The AUP of the University of Tasmania and the University of Western Australia make no mention of sanctions. The latter appears to have been prepared by a lawyer and is very legalistic in tone. Victoria University's AUP explicitly state that the scope of non-compliance extends beyond failure to comply with the policy to disobeying lawful instructions by authorised staff. This is implicit in other AUPs, for instance "observed actions" [RMIT], "responsible officer detects misuse" [Flind], "user must notify the Director ITS of a breach or suspected breach" [Syd]. An interesting question regarding the latter is whether the failure to do so is also a breach of policy.

Some AUPs indicate who initiates alleged non-compliance hearings. It is, for instance, the "Systems Administrator" or "Senior ITS Manager" [RMIT], "Supervisor", "Chairman Local Management Group", "Director Computing services" [Ade], "director ITS" [Sydney, NewE]. Charles Sturt University's AUP mentions "a confidential report to Computer Centre Manager or Executive Director Division of IT". The University of Newcastle's AUP is vague when it states that users are to "inform the University" of a breach.

Some AUPs indicate who conducts the hearing into alleged non-compliance and who is authorised to impose penalties for "proven" non-compliance. It is, for instance, the "Director" or "Vice Chancellor [JCook(a), Murd(a), Curtin] or the "Director or nominee' [NewE], "Heads of Schools, Centres and Offices" [Macq] or "Heads of Department or Senior Officials for staff and students…Director of Information Technology…for other users" [LTrobe].

Few AUPs attempt to match the specific act of non-compliance with a particular penalty. None succeed in a comprehensive way. The better examples are [Ade, Murd(a) and RMIT]. Victoria University's AUP makes a general statement that the penalty depends on "the severity of the breach" The AUP of the University of Western Sydney explicitly states that "students have already been suspended for the offence of hacking".

The most common penalties referred to in the AUPs are a suspension of account, loss of an account, warning or caution, or referral to the relevant authority for legal or criminal prosecution. Dismissal from employment which is applicable to staff is also mentioned. There are other penalties that are less common or are specific to a University. These include a fine, and the recovery of loss or damage from the user. The AUP of the University of New South Wales contains a schedule of fines. Another penalty is dismissal of a student from a class, for instance, at the University of Adelaide the "Chairman of a Department excludes a student from any class for any cause he or she deem sufficient". Other penalties include charging for use at commercial rates [Woll], "expelled for a period of at least two years without the automatic right of re-enrolment" [CSturt] or "Given a combination of the above penalties" [CSturt]. Some AUPs [VUT, Ade, Griffith, NSW] simply state that disciplinary action will be taken in accordance with University Statutes or Regulations. The AUP for the University of Wollongong and Catholic University are vague and refer to breaches being dealt with in the same manner as violations of other University rules.

Apart from the few AUPs that explicitly cross reference to relevant University Statutes and Regulations there is no description of the rights of both parties in the case of an alleged breach. Only a few AUPs [RMIT, Swin(a), NewE, QUT] state that there is a right of appeal against the decision of the hearing.

Users Informed of Policy

The AUPs do not state that each user is provided with the AUP and that it must be read before beginning use the network. However, Sydney University requires a signature of assent. Other Universities may also require this but is not referred too in their AUP. Anecdotal evidence suggests that many users are unaware or have never read their University's policy.

User Involvement in Policy formulation

Most AUPs do not discuss how the policy was developed. Some specify an author [LTrobe, Murd(a), USA, Sydney] others do not [VUT, Woll, TAS, Ade]. Most fail to state who authorised the policy. Better examples in this regard are Queensland University of Technology and Curtin University. Few AUPs makes reference to any user involvement in policy development. Again, anecdotal evidence suggest that ITS, without serious user involvement, prepare most policies. Many AUPs lack a last update [Can, JCook(a), RMIT, WA]. Again, anecdotal evidence suggests that university management request user involvement only after the current policy has been seriously tested and found grossly deficient.

Communication Effectiveness

Many AUP's are deficient in their ability to communicate effectively. The major factors contributing to this are lack of a clear statement of purpose, ambiguous terms, negative tone and redundancy and extraneous material. It is suspected that many would not withstand a challenge in a court of law.

No purpose is included in many of the AUPs [Murd(a) NewE, TAS, WA]. Canberra University's and Catholic University's AUP include the guiding principles on which the policy is based. Most AUPs describe the purpose in one sentence [RMIT, Flind, NSW, LTrobe]. Three examples follow. One, "This document provides guidance of acceptable behaviour expected of users and intending users of these facilities" [NewE]. Most of this document discusses "unacceptable behaviour". Two, "This code of conduct is to facilitate the efficient effective responsible and lawful use of the University's electronic facilities, thereby safeguarding the interests of all users and of the University" [CSturt]. Three, "This code of practice sets out responsibilities when using University computing and networking facilities" [Griff].

The AUPs abound in the use of ambiguous terms and vagueness. Terms like "bother", "annoy", "lascivious" and "lewd" are never defined. Other examples are phrases like "whatever the University has stated is inappropriate" [TAS], "don't snoop" [Griff], "The Director may prohibit any practice detrimental to the interests of the University…" [JCook(a)], and a sanction will be imposed on a user "responsible for inappropriate use of the facilities" [Curtin]. The latter is a "catch-all" as it comes after a list of specific unacceptable behaviour. At the Australian National University [ANU(a)] it is an "offence to display pictures…with sexual connotation in a work or study environment within the University in circumstances in which another person *reasonably* feels offended, humiliated or intimidated".

Many of the AUPs lack a positive tone. The emphasis is on describing unacceptable behaviour and the penalties that will be applied for non-compliance. Some documents [VUT, Griffith, UWS, TAS] place this description very early in the document. The AUPs of the University of Sydney and the University of Western Australia have a very negative tone. The AUP of the University of South Australia has a long section on Federal and State laws and the gaol terms that can be given for an offence. The AUP for RMIT University immediately refers to "what you are restricted from doing" but makes no mention of "acceptable use". On a more positive note the AUP of Queensland University of Technology describes both the positive and negative user responsibilities.

Redundant and extraneous material abound in the AUPs. This may result from a failure to keep the policy current. Some examples are "smoking in a computer laboratory" [VUT], smoking has been banned in any building for some time, a large section on Do's and Dont's of password selection [Ade], a large section on the South Australian Criminal Law Consolidation Act, Crimes Act and Copyright Act [USA], a large section on AARNET, that has been incorporated into a number of AUPs [Flind], job descriptions of computing staff [Curtin] and standards for material placed on the University server [QUT]. Some AUPs are written in an idiosyncratic manner [Can, TAS, RMIT]. By way of contrast the AUP for the University of the Sunshine Coast is the shortest document of all AUPs, being barely a page in length.

DISCUSSION AND CONCLUSION

There are two major concerns that are likely to be held by users about Australian University AUPs. First, is whether an AUP violates academic freedom and infringes individual privacy through censorship of material that is read, prepared, copied, communicated and stored by network users. Second, whether an AUP ensures “due process protection” for alleged non-compliance with the policy. The evaluation of AUPs against “Best Practice” principles demonstrates that these concerns are well founded. Many policies are seriously deficient. They should be extensively revised with full involvement of all the relevant stakeholders so that they are in accord with these principles.

Just how concerned users should be depends on how the policy is implemented. What is stated as policy may not be fully implemented in practice. The AUPs of all but four Universities state that network facilities and services must only be used for approved activities. Anecdotal evidence suggests that a “blind eye is turned” to personal use. University staff and students should be permitted and encouraged to read, prepare, copy, communicate and store material from a diverse range of sources and expound a diverse range of views. This includes material that is viewed by university management as not being directly related to the teaching, research or study of the user. This includes legal material that is referred to as “socially objectionable”.

Censorship has no place in a University. Of course, university management may confine use of the network to material directly related to “approved” activities on economic grounds. It may be argued that network resources are scarce resources and so must be rationed on an equitable basis. The risk is that those who would wish to censor may invoke the economic argument to justify it rather than admit to the “real” reason.

University management is also concerned about the risks of litigation and so favours a conservative policy in relation to network use in order to minimise these risks. An important concern is in relation to “obscene” or “offensive” material. This usually means material of a sexually explicit nature. Their concern is that such material, especially in shared work areas, may constitute sexual harassment as defined in Government legislation. There is no justification in a University for censoring “sexually explicit” material that is legal. If a student accesses this material in class instead of undertaking the allocated task, a staff member may be justified in imposing some sanction for this misdemeanour. Accessing the AFL or ARL or any other site should attract the same sanction. Accessing legal sexually explicit sites or the AFL or ARL site or any other site outside of class is a different matter.

The second major concern is about “due process protection”. As indicated earlier what is stated as policy may not necessarily be fully implemented in practice. Anecdotal evidence suggests that this applies to imposing sanctions for non-compliance. University management tends to be reluctant to apply sanctions unless a serious breach of policy occurs. One reason is that they fear the “bad” publicity and potential loss through litigation. On those occasions when action has been taken against a user and this becomes public, it is a reminder of the need for “due process protection”. This is in the interests of both staff and students, and university management. The American work by Kors and Silvergate [1999] and The Shadow University Web Site Links it inspired is recommended reading for anyone interested in how university management can fail to exercise due process. It also shows how University management and others can fail to understand the "true" nature of a University.

FURTHER RESEARCH

The analysis of the policy documents of Australian Universities concerning acceptable and unacceptable use of network services is reported here. Reference has been made to anecdotal evidence and a likely "gap" between the documented policy and how it is implemented in practice. Further research focuses on implementation of the policy. This includes an investigation of:

- the use of software to monitor network usage, especially the employment of logging and filtering software
- the most common types of breaches by users and their frequency
- how hearings of alleged breaches of policy are undertaken including the appeals process and the sanctions employed
- how policy is formulated and authorised, including the extent of user involvement

A survey of CAUDIT members on these implementation issues has been undertaken and the responses are currently being analysed.

REFERENCES

American Association of University Professors, (AAUP) (1992) *On Freedom of Expression and Campus Speech Codes*,
http://www.eff.org/pub/Censorship/…edu/CAF/academic/speech-codes.aaup, date accessed 25/5/00

Australian Library and Information Association (ALIAa), *Statement on Freedom to Read*, http://www.alia.org.au/policies/freedom.to.read.html, date accessed 8/5/00

Australian Library and Information Association (ALIAb), *Statement on professional Ethics*, http://www.alia.org.au/policies/profesional.ethics.html, date accessed 8/5/00

Australian Vice Chancellor's Committee, *Australian Universities WWW Servers*, http://www.avcc.edu.au/avcc/uniwebs.html

American Library Association (ALA) (1996) *Library Bill of Rights*, http://www.ala.org/work/freedom/lbr.html, date accessed 25/5/00

Council of the Australian University Directors of Information Technology (CAUDIT), http://www.caudit.edu.au/caudit/codes

Kors A. C. and Silvergate H.A. (1998) *The Shadow University: The Betrayal of Liberty on Americas Campuses"*, Harper.

The Electronic Frontier Foundation (EFF), http://www.eff.org/pub/CAF/policies

The Shadow University Web Site Links, http://www..shadowuniv.com/links.html

Merel P (1996) *A Bill of Electronic Rights and Ethics*, http://www.efa.org.au/Publish/ere.html, date accessed 31/5/00.

National Tertiary Education Union (NTEU), *Privacy of Electronic Communications"*, facsimile copy 29/5/00.

National Union of Students (NUS) (1999) *Education Policy*, email attachment 5/9/00

Sandy G (2000) The Classification of Unacceptable Use of Network Services: Australian Universities, *Working Paper Number 5*, School of Information Systems, Victoria University of Technology.

Yee D *Draft Proposal: A Code of Practice Regarding Content That May Infringe Censorship Laws*, http://danny.oz.au/freedom/Ccalternative.html, date accessed 8/5/00

NOTE: A comprehensive reference list is available on request to the author.

APPENDIX 1 AUSTRALIAN UNIVERSITY ACCEPTABLE USE POLICIES

NOTE: The abbreviation for each University cited in the paper is in **bold**.

[Ade] The University of Adelaide (1996) *Computer Network Access and Usage Policy.* 6 February, 2000, http://www.adelaide.edu.au/ITS/pol-pracs/access.html

[ANU (a)] *Information Technology Service Rules: Part 1 – Preliminary*. 26 July 2000, http://www.anu.edu.au/cabs/rules/its.htm

[ANU (b)] *Discipline Rules*. 26 July 2000. http://www.au.edu.au/cabs/rules/discipline.htm

[Cath] The Australian Catholic University (1998) *Computer and Internet Acceptable Policy.* 7 February, 2000, http://www.acu.edu.au/its/nsw/policy/acceptableuse.html

[Can] University of Canberra (1999) *Network Access and Use - Responsibilities and Obligations.* 5 February, 2000, http://www.canberra.edu.au/uc/policies/it/nap.html

[**CSturt]** Charles Sturt University (1997) *Code of Conduct for Users of Electronic Facilities.* 7 February, 2000, http://www.csu.edu.au/acadman/o3m.htm

[Curtin] Curtin University (1997) *Information Technology Use.* 5 February 2000,

[Deakin(a)] Deakin University (1999) *Guidelines on the Use of the Internet*. 25 January 2000, http://www.deakin.edu.au/div_its/corporateinfo/policies/internetguidelines.html

[Deakin(b)] Deakin University (1999) *Conditions of IT Use*. 25 January 2000, http://www.deakin.edu.au/div_its/corporateinfo/policies/conditions.html

[ECowan] Edith Cowan University (1999) *Computing Facilities - Conditions of Use.* 6 February, 2000, http://www.cowan.edu.au/secretariat/policy/it/it008.html

[Flind] Flinders University *Student Related Policies and Procedures Manual: Section D - Computing.* 6 February, 2000, http://adminwww.flinders.edu.au/Calendar/Vol3/SecD.htm

[Griff] Griffith University *Use of Computing and Networking Resources - Code of Practice.* 6 February, 2000, http://gu.edu.au/ins/its/govern/coc.html

[JCook(a)] James Cook University (1999) *Conditions for Use of University Computing and Communication Facilities.* 7 February, 2000, http://www.jcu.edu.au/office/itr/policies/condts_use_univ_facilts.shtml

[JCook(b)] James Cook University (1999) *Usage Guidelines and Penalties.* 7 February, 2000, http://www.jcu.edu.au/office/itr/policies/comp_use_gdlins.shtml

[LTrobe] La Trobe University (1997) *Internet Code of Practice*. 25 January, 2000, http://www.latrobe.edu.au/comp/code_of_prac.html

[Macq] Macquarie University (1998) *Security Policy and Rules Governing the Use of the Computing and Communications Facilities at Macquarie University*. 7 February, 2000, http://www.ois.mq.edu.au/policy/mqrules.html

[Murd(a)] Murdoch University *Standards and Guidelines for all users of University Computing and Network Facilities: Version 1.0.* 6 February, 2000, http://wwwits2.murdoch.edu.au/security/sg_users.html

[Murd(b)] Murdoch University (1999) *Student Network Conditions of Use.* 6 February, 2000, http://wwwstudent.murdoch.edu.au/policy/conditions-of-use.html

[NewE] The University of New England (1999) *Rules for the Use of University of New England Computing and Communication Facilities.* 7 February, 2000, http://www.une.edu.au/its/ccfrules.htm

[NSW] The University of New South Wales (1998) *Rules Relating to Student Use of Computing and Electronic Communications Facilities.* 5 February, 2000, http://www.infonet.unsw.edu.au/poldoc/rulcomp.htm

[NewC] The University of Newcastle (1999) *Use of Computing and Communications Facilities.* 5 February, 2000, http://www.newcastle.edu.au/services/iesd/policies/conds_use.html
[QLD] The University of Queensland (1999) *Internet Code of Practice.* 7 February, 2000, http://www.uq.edu.au/itspp/CodeF.html
[QUT] Queensland University of Technology *Information Technology Rules.* 12 May, 2000,
[RMIT] RMIT University (1997) *Conditions of Use of ITS Facilities.* 25 January, 2000, http://www/rmit.edu.au/rules/
[USA] University of South Australia (1997) *Use of University Information Technology Facilities.* 7 February, 2000, http://www.unisa.edu.au/adminfo/policies/corp/c22.htm
[UWS] University of Western Sydney (Nepean) (1994) *Rules and Guidelines on the use of Computing and Network Facilities At UWS Nepean.* 26 July 2000, http://www.nepean.uws.edu.au/ccd/guide/rules.htm
[Swin (a)] Swinburne University (1993) *Network Access and Code of Practice Policy*. 26 July, 2000, http://www.swin.edu.au/csit/comms/cofprac.htm
[Swin (b)] Swinburne University (1994) *Student Disciplinary Code.* 26 July, 2000, http://www.swin.edu.au/csit/comms/discp.htm
[Sydney] The University of Sydney (1999) *Conditions of Use.* 5 February, 2000, http://helpdesk.usyd.edu.au/condUse.html
[Tasmania]University of Tasmania *Computer Usage Guidelines.* 6 February, 2000, http://www.its.utas.edu.au/client_services/labg.html
[VUT] Victoria University of Technology (1998) *Policy on the Use of the University's Computing Facilities.* 25 January, 2000, http://www.vu.edu.au/it/central/compuse.htm
[WA] The University of Western Australia (1994) *Computer and Software Use Regulations.* 3 May, 2000, http://uniwa.edu.au:70/1s/compnet/legal/regulations
[Woll] University of Wollongong *Rules Governing the Use of University Computer Facilities.* 7 February, 2000, http://www.uow.edu.au/its/userguide/staff.html
[SCoast] University of the Sunshine Coast *Conditions Governing the Use of Computing and Networking services.* 3 May, 2000, email: hgorden@usc.edu.au

COPYRIGHT