Crafting a Code of Ethical Conduct

Kate Lance
Department of Computer Science
The University of Newcastle
Callaghan NSW 2308
clance@cs.newcastle.edu.au

1 Why Did SAGE-AU Want a Code of Ethics?

Most professional associations have some sort of code of ethics, conduct, or responsibility. The form of expression and the reasons for these codes are enormously varied. Some are short, "motherhood-and-apple-pie" statements of good intention, some are more promising of punishment than illustrative of good behaviour, some have strong opinions on their members' moral activities even outside their professional roles, some contain reams of explanation and examples, and some are more like business documents. They aren't, on the whole, meant to remain without revision for long periods.

For instance, you might imagine that the Australian Medical Association Code of Ethics is something like the single paragraph of high ideals of the Hippocratic Oath you would recall from old Hollywood movies: in fact it contains sixty items under twelve subheadings, with discussions of responsibility to patients, to clinical research trials, to other doctors; it talks about terms of contracts, advertising, organ transplants, and social obligations—and even contains a definition of brain death.

At the other extreme, the Journalists' Code of Ethics is ten short points (many of which are blithely ignored, without penalty, by the less scrupulous media). The Institute of Electrical and Electronics Engineers get by with a page and a half of crisp statements, while the Data Processing Management Association has a code with two pages of professional guidelines and over *six* describing disciplinary procedures.

Before the Temporary Working Group on Ethics could define a code appropriate for SAGE-AU, we had to first decide just why we wanted a code, what we wanted to express with it, and whether or not it was really ethics we were considering.

1.1 Possible Reasons to Set Up a Professional Code

- to **inspire** members to be more ethical in their conduct
- to alert professionals to the **moral** aspects of their work that they might have overlooked
- to be a **disciplinary** code to enforce rules in order to protect professional standards
- to offer **advice** in cases of moral perplexity
- to alert employers and clients to what is proper **conduct** by a member of the profession
- to enhance the **image** of the professional in the public eye
- as one of the **credentials** of upgrading the status of a profession
- to protect the **monopoly** of the profession (which historically has been the major aim of most codes of ethics)

1.2 Definitions of Ethics

Oxford Dictionary:
1. moral philosophy
2. moral principles; rules of conduct
3. set of these

Webster's Dictionary:
1. the discipline dealing with what is good and bad and with moral duty and obligation
2. a set of moral principles or values
3. a theory or system of moral values
4. the principles of conduct governing an individual or group

1.3 Ethics and Codes

Ladd (1980) argues that in fact, professional codes of ethics have very little to do with the philosophical discipline of Ethics. He says:

- Ethics is an open-ended, critical intellectual activity, whose principles are established by exploring, deliberating and arguing about issues. It's *not* something that can be settled by fiat or authority—which is really law-making or policy-making. So ethical principles can't be established by an organisation: codifying ethics is like trying to codify medicine or architecture.
- Even if you could agree on some ethical principles, to *impose* them on others contradicts the notion of ethics itself, which presumes that people are autonomous moral agents. Ethics must be self-directed, not defined by others.
- Being a professional does not automatically make someone an expert in ethics, even in the ethics of one's own particular profession. There are no experts in ethics—everyone is capable of being "a teacher of virtue".
- Professionals are not, just because they are professionals, *exempt* from the common obligations and duties binding on other people. These are "micro-ethical issues" regarding personal relationships between individuals, which simply involve the application of ordinary notions of decency, civility, humanity, respect and responsibility.
- While ethics *can* be used to criticise or evaluate a code of conduct or a professional code, it's not the same thing, it's the process you use to validate the code, not the end product.

1.4 What's Special About System Administration?

Rob Kolstad: *"System administration, as a field, is unique. I can think of no other field that shares even a majority of its qualities (and I've asked the question of dozens of other technical and non-technical types). The field is incredibly broad and deals with systems in timeframes from milliseconds through months. It deals with components whose size is measured in bits through components whose aggregate is measured in gigabytes (or even terabytes). It deals with cold, calculating machines and warm, human people. It sometimes deals with life and death; it deals with the background color of the someone's screen. It is a discipline which, when performed best, is virtually unobservable."*

- System administration has been a profession for much less time than traditional ones like medicine and law—it has fundamental differences from any profession that has ever before existed in human history.
- It involves the management of resources whose utility, power and importance in human affairs is increasing without apparent limit.
- Those resources in themselves demand entirely new ways of dealing socially and legally with issues as wide-ranging as privacy, security, and intellectual property.
- The profession has so recently emerged that most people have very little understanding of its demands, its powers, and even its potential abuses.
- The essential relationship in most professions is between clients and practitioners, such as patients and doctors. But the relationship between users and system administrators involves a third party, the system itself—there simply is no way for service to be provided unless a viable system exists.
- Because of this, the very nature of the work system administrators do demands that they aspire to certain qualities, such as:
  - a commitment to technical integrity—because systems are unforgiving of incompleteness or negligence.
  - a commitment to cooperation and communication—attitudes that are fundamental to the existence and viability of network resources.
  - a recognition of the responsibility owed to the people who trust computer systems to manage their years of research data, their medical records, their tax returns, their love letters, and sometimes their very lives.

1.5 The Reasons We Finally Agreed On

After much discussion based on the above points we agreed upon the following items as the rationale for our code:

- To indicate to employers that we are a professional body that takes a serious view of our responsibilities.
- While not being a job description, to delineate the extent of our powers and responsibilities for people unfamiliar with the scope of our activities.
- To indicate to users, colleagues and employers that we will act in good faith, and, as much as possible, in their best interests.
- To protect ourselves should unethical behaviour be demanded of us.
- To explore what ethics might have to offer *us*, to find out for ourselves where our ethical boundaries and obligations really lie.

2 How Other Groups Have Done It

2.1 Privilege, Confidentiality and Privacy

One of the first things we looked at was the protection given to various professions which deal with privileged, confidential information, to see how that might relate to our profession.

- **Lawyers** are protected under Common Law, in civil and criminal cases, from having to reveal lawyer-client communications to do with advice or existing or anticipated litigation.
- **Journalists** have no Common Law or statute protection in Australia (although in England there is statutory privilege protecting them from having to reveal their sources of information).
- **Clergy** have no Common Law privilege, but there are statutes in some states protecting them from having to reveal the contents of a confession. The relevant professional bodies do not permit disclosure: Catholic Canon law imposes immediate excommunication from the Church, and the penalties imposed by other churches for breaking confessional privacy range from excommunication to disciplinary action.
- **Doctors** have no protection under Common Law, but there are statutes in some states protecting them in civil proceedings from revealing confidential information. Doctors revealing confidential information may be censured or even deregistered by their professional association. The Australian Medical Association permits disclosure only in cases when:
  - the patient gives consent
  - it's undesirable to seek consent on medical grounds
  - the doctor has an overriding duty to society
  - for certain medical research
  - it's required by the legal profession

2.2 Privacy Act (1988) Information Privacy Principles

The Federal government requires all of its departments and agencies to comply with the Information Privacy Principles. They govern the keeping of personal information records: methods of collection, storage and security, access, accuracy, completeness, usage, and disclosure to other people.

A copy of the Information Privacy Principles is available by anonymous ftp from **ftp.mel.dit.csiro.au** as **pub/SAGE-AU/Ethics/IPP** and all members of SAGE-AU are urged to read them. (The OECD Guidelines to Computer Privacy and Security are also available there.) Even if you are not associated with any Federal government activity, similar principles are soon to be introduced at some State levels, and may eventually apply much more widely. Extracts from several of the IPPs with system administration relevance are listed below:

Principle 4: storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure: that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse.

Principle 9: personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 11: limits on disclosure of personal information

A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

- the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

- the individual concerned has consented to the disclosure;
- the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life and health of the individual concerned or of another person;
- the disclosure is required or authorised by or under law; or
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2.3 Codes from Other Computing Organisations

Here are some examples of codes from other computing groups. While the following one is short and readable, it doesn't address the specific concerns of *computing* professionals, but only professionals in general.

The Australian Computer Society Code of Ethics

I must act with professional responsibility and integrity in my dealings with clients, employers, employees, students, and the community generally. By this I mean:

PRIORITIES: I must service the Interests of my clients and employers, my employees and students, and the community generally, as matters of no less priority than the interests of myself and my colleagues.

COMPETENCE: I must work competently and diligently for my clients and employers.

HONESTY: I must be honest In my representation of skills, knowledge, services and products.

SOCIAL IMPLICATIONS: I must strive to enhance the quality of life of those affected by my work.

PROFESSIONAL DEVELOPMENT: I must enhance my own professional knowledge and skills and those of my colleagues, employees and students.

COMPUTING PROFESSION: I must enhance the Integrity of the Computer Profession and the respect of its members for each other.

The following code had almost a half a page of explanation and examples for each item. While it is certainly comprehensive, it's also repetitive and too long, and probably would never be read through to the end by many members. (These are just the item headings!)

The Association for Computing Machinery—Code of Professional Conduct

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patents.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.
2.1 Strive to achieve the highest quality in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.
3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information systems that enhance the quality, effectiveness and dignity of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
3.4 Ensure that users and those who will be affected by a computing system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and other affected by a computing system.
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

Some Points Coverered by Other Codes

As well as the two codes above, we also looked at the codes for the Institute of Electrical and Electronics Engineers, the British Computer Society, the Data Processing Management Association, and the Institute for Certification of Computer Professionals. Most of the points in the above ACM list appeared in the other lists, but they were generally not so comprehensive. Some interesting additions to the above list:

ICCP: ...one is expected to apply the same high standards of behaviour in one's personal life as are demanded in one's professional activities.

IEEE: Advance the integrity and prestige of the profession by practicing in a dignified manner and for adequate compensation.

BCS: Actively seek opportunities for increasing efficiency and effectiveness to the benefit of the user and of the ultimate recipient.

DPMA: Use my skill and knowledge to inform the public in all areas of my expertise.

3 Diversion: An Ideal System

As we were trying to identify the essential points from other codes, taking account of additional issues that seemed important, and trying to apply them to as wide a variety of system work as possible, it became clear that we just didn't know enough about the different jobs that SAGE-AU members were doing—what range of activities they actually deal with, whether or not they had the freedom or the opportunity to to live up to the items we were considering, and, for comparison, just what they would consider the ideal system setup.

So a questionaire went out to the Ethics group, asking people to rate the levels of importance, low to high, allocated in their organisation to aspects of system work, such as backups, applying patches, access to the Internet, conditions for users, etc. We received ratings on 30 past and present jobs, and 10 descriptions of the Ideal System.

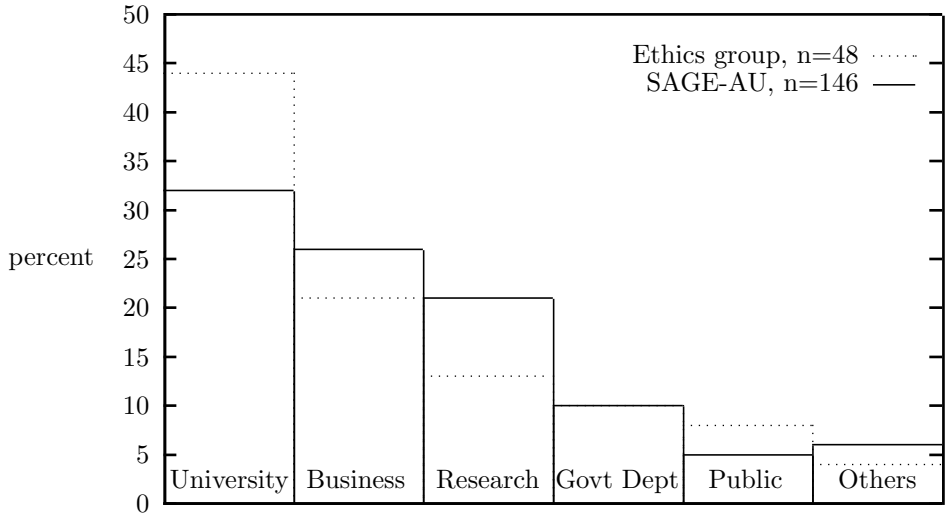

Figure 1: Distribution of organisations in SAGE-AU and the Ethics group

3.1 Did the Ethics Working Group Represent the SAGE-AU Members?

From people's email addresses it was fairly easy to see what type of organisation they posted from—university, business, government research, government department, public access account, and a few which couldn't be identified. I compared the distribution of those in the whole SAGE-AU mailing list with those on the Ethics list (Figure 1).

It was clear that on the Ethics list there were a higher proportion of university sysadmins, and a lower proportion of government research organisation sysadmins, than in SAGE-AU overall. Maybe university sysadmins have to deal more often with ethical dilemmas (from student activity?) than do research organisations.

3.2 Real Systems vs an Ideal One

The questionaire asked people to state the level of importance the following categories of system work were given in their organisation, from 1 (minimum importance) to 5 (maximum importance); and, given an ideal system, what level they themselves would rank these categories:

1) Frequent backups
2) Applying patches
3) Performance monitoring
4) Security monitoring
5) Disaster recovery planning
6) Privacy of email
7) Privacy of accounts
8) Access to internet
9) Safe user environment
10) Comfortable user environment
11) Self-education
12) User-education
13) Updating hardware
14) supply of consumables

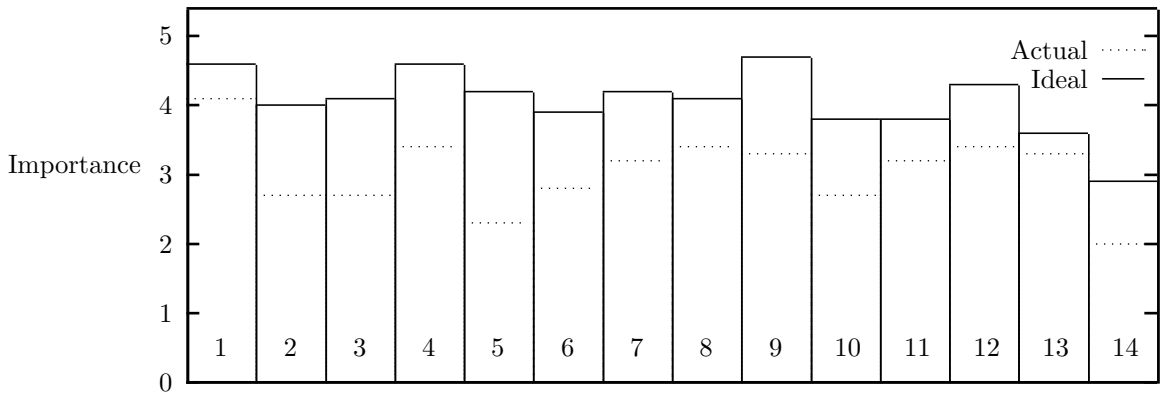

Figure 2: Actual vs ideal systems

The numbers against the categories are the ones plotted on Figure 2, which compares the mean of the replies from different organisations to the mean of the ideal system replies.

The mean of the replies from all the organisations was used, as the total numbers per organisation were too low for separate reliability. However, there were suggestions in the separate results that university sysadmins were more concerned than others about applying patches and security monitoring; while research organisations were less concerned with performance monitoring, but rated email and account privacy very highly.

Both universities and research sites gave access to the Internet an importance more than twice that currently given it by businesses and government departments—but the system administrators of those businesses and government departments gave it just as much importance as the others in their ideal system.

All groups were in agreement that backups are important as an ideal, *and* they get them done as well; however, everyone also think disaster recovery planning is a great idea—but it looks like it's not getting very high priority in real life.

4 What We Ended Up With, And Why

The preamble tries to summarise as many of the points discussed above as possible. The overall aim was to express, to others as well as to ourselves, recognition of our ethical duties as professionals.

When writing the items we found that lists of "job descriptions" were a difficulty: if there was too little detail, the code ran the risk of blandness and irrelevance to real-life situations; but too much detail might make it date too quickly, and be too specific to particular areas of system administration. Detailed lists also run the risk of appearing to be exhaustive, when they may only have been offered as examples.

Another difficulty was making it general enough to apply not just to administrators of Unix systems or those with access to the Net, but to apply to all kinds of installations, with their vast array of different system duties. The problem also arose concerning just what the people involved at all levels with systems should be called—the list of users, clients, employers, employees, colleagues, peers, subordinates, and other administrators, was eventually collapsed just to "users".

"Informing" users of things they need to know was also a discussed point. At one stage we were just

going to strive to do it, but finally, it seemed better to affirm that we would indeed *inform*, we would make information available, then it was up to others to utilise it.

Similarly for the items that relate to our own continuing education, both technical and social—we affirm our duty to actually do it, not just wish to do it, because in this rapidly-changing field we need to emphasise that further education is essential, it's not really a luxury or a choice.

SAGE-AU Code of Ethical Conduct

In a very short period of time computers have become fundamental to the organisation of societies world-wide; they are now entrenched at every level of human communication from goverment to the most personal. Computer systems today are not simply constructions of hardware—rather, they are generated out of an intricate interrelationship between administrators, users, employers, other network sites, and the providers of software, hardware, and national and international communication networks.

The demands upon the people who administer these complex systems are wide-ranging. As members of that community of computer managers, and of the System Administrators' Guild of Australia (SAGE-AU), we have compiled a set of principles to clarify some of the ethical obligations and responsibilities undertaken by practitioners of this newly emergent profession.

We intend that this code will emphasise, both to others and to ourselves, that we are professionals who are resolved to uphold our ethical ideals and obligations. We are committed to maintaining the confidentiality and integrity of the computer systems we manage, for the benefit of all of those involved with them.

No single set of rules could apply to the enormous variety of situations and responsibilities that exist: while system administrators must always be guided by their own professional judgement, we hope that consideration of this code will help when difficulties arise.

(In this document, the term "users" refers to all people with authorised access to a computer system, including those such as employers, clients, and system staff.)

As a member of SAGE-AU I will be guided by the following principles:

1. Fair Treatment

I will treat everyone fairly. I will not discriminate against anyone on grounds such as age, disability, gender, sexual preference, religion, race, or national origin.

This was an item in the ACM code which we though was important. There was some argument about whether or not the list was essential: but it was decided it might be helpful given the diversity of people in places like universities and research organisations.

2. Privacy

I will access private information on computer systems only when it is necessary in the course of my duties. I will maintain the confidentiality of any information to which I may have access. I acknowledge statutory laws governing data privacy such as the Commonwealth Information Privacy Principles.

At one stage we had "information that belongs to others" rather than "private information", which brought up problems with defining who actually owns the files on a computer—the owner as defined by the operating system, or the owner of the hardware? We also tried to avoid emotive terms like "infringing privacy" or "system privileges".

3. Communication

I will keep users informed about computing matters that may affect them—such as conditions of acceptable use, sharing of common resources, maintenance of security, occurrence of system monitoring, limitations of electronic media, and any relevant legal obligations.

Issues here were whether or not you can get people to actually take in the information that you present to them, whether or not most sites actually had defined Conditions of Use, and how much job description was necessary.

4. System Integrity

I will strive to ensure the integrity of the systems for which I have responsibility, using all appropriate means—such as regularly maintaining software and hardware; analysing levels of system performance and activity; and, as far as possible, preventing unauthorised use or access.

Here we argued about mentioning anything to do with current technology (such as disk backups) and again, how much detail should go into this without it becoming a job description.

5. Cooperation

I will cooperate with and support my fellow computing professionals. I acknowledge the community responsibility that is fundamental to the integrity of local, national, and international network resources.

This was one of the hardest to define, because it refers to Net access, which some sites don't have; but in this form, even if people aren't on the Net, they can still acknowledge its importance. An early draft mentioned keeping in touch with " organisations that coordinate security efforts on behalf of network users", but these organisations are also examples of community cooperation.

6. Honesty

I will be honest about my competence and will seek help when necessary. When my professional advice is sought, I will be impartial. I will avoid conflicts of interest; if they do arise I will declare them.

This was the least revised item!

7. Education

I will continue to update and enhance my technical knowledge and management skills by training, study, and the sharing of information and experiences with my fellow professionals.

This had " attend professional conferences" in one draft, but sadly, we decided to be less specific.

8. Social Responsibility

I will continue to enlarge my understanding of the social and legal issues that arise in computing environments, and I will communicate that understanding to others when appropriate. I will strive to ensure that policies and laws about computer systems are consistent with my ethical principles.

Initially there was a list here of issues such as " privacy, confidentiality, academic freedom, copyright, intellectual property, illegal access and computer crime", but again, in the interests of greater applicability, it was put more generally.

9. Workplace Quality

I will strive to achieve and maintain a safe, healthy, productive workplace for all users.

Too-specific lists again: " fundamental health and safety procedures, appropriate ergonomic furniture, and adequate space and lighting" was discarded for greater generality.

5 Future Work

The Ethics working group will convene again in a year's time to consider any revisions to this code that may then be necessary.

One additional point of discussion was, just what do we do if someone in SAGE-AU *doesn't* respect this code when doing system administration. Some other codes had substantial sections on disciplinary procedures. We decided that any such activity would have to be looked at by a different working group, one with more legal expertise than this one, to consider what mechanisms should be in place:

- to give support to sysadmins who might feel their personal ethics are being compromised
- to deal with complaints if others think that a sysadmin is compromising the code of ethical conduct
- to discuss, defend, decide about the complaint
- to enforce a judgement if the complaint is upheld

6 Acknowledgements

Almost half of all the people on the Ethics group mailing-list took some part in the discussion over the last six months, but I am particularly grateful for the substantial contributions of Janet Jackson, Chris Deeble, Glenn Huxtable, Douglas Ray, Shane Youl and Hal Miller.

Thanks also to Diet Ostry for proof-reading this paper, and to John McPhee, of the Faculty of Law, The University of Newcastle, who assisted us with informal opinions and the on-line copies of the Information Privacy Principles and the OECD Guidelines on Privacy and on Security, available by anonymous ftp from **ftp.mel.dit.csiro.au:pub/SAGE-AU/Ethics**.

7 References

Ladd, J., 1980, *The Quest for a Code of Professional Ethics: an Intellectual and Moral Confusion*, in *Ethical Issues in the Use of Computers*, Johnson, D. G., and Snapper, J. W., 1985, Wadsworth Publishing Company, Belmont, California.

Oldroyd, J. R. and Kolstad, R., *Debate: To Certify or Not?*, ;login:, Nov/Dec 1993, Vol 18, No 6, 24.