Codes of Ethics in The IT Industry

The Code of Fair Information Practices (1973)

The Secretary's Advisory Committee on Automated Personal Data Systems for the US Department of Health, Education, and Welfare recommended the adoption of this code to secure the privacy and rights of citizens.

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information is in his or her file and how the information is being used.
- Individuals must be able to correct information in their records.
- Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse.
- Individual must be able to prevent personal information obtained for one purpose from being used for another purpose without their consent.

Internet Activities Board (IAB) (Now the Internet Architecture Board) and RFC 1087 (1989)

The IAB "strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure," which characterized as unethical any activity that purposely

- seeks to gain unauthorized access to the resources of the Internet
- disrupts the intended use of the Internet
- wastes resources (people, capacity, computer) through such actions
- destroys the integrity of computer-based information, or
- compromises the privacy of users

Computer Ethics Institute (CEI) (1992)

- Thou Shalt Not Use a Computer to Harm Other People.
- Thou Shalt Not Interfere with Other People's Computer Work.
- Thou Shalt Not Snoop around in Other People's Computer Files.
- Thou Shalt Not Use a Computer to Steal.
- Thou Shalt Not Use a Computer to Bear False Witness.
- Thou Shalt Not Copy or Use Proprietary Software for Which You Have Not Paid.
- Thou Shalt Not Use Other People's Computer Resources without Authorization or Proper Compensation.
- Thou Shalt Not Appropriate Other People's Intellectual Output.

- Thou Shalt Think about the Social Consequences of the Program You Are Writing or the System You Are Designing.
- Thou Shalt Always Use a Computer in Ways That Insure Consideration and Respect for Your Fellow Humans.

National Conference on Computing and Values (1991)

- Preserve the public trust and confidence in computers.
- Enforce fair information practices.
- Protect the legitimate interests of the constituents of the system.
- Resist fraud, waste, and abuse.

The Working Group on Computer Ethics

In 1991, the Working Group on Computer Ethics created the following End User's Basic Tenets of Responsible Computing:

- I understand that just because something is legal, it isn't necessarily moral or right.
- I understand that people are always the ones ultimately harmed when computers are used unethically. The fact that computers, software, or a communications medium exists between me and those harmed does not in any way change moral responsibility toward my fellow humans.
- I will respect the rights of authors, including authors and publishers of software as well as authors and owners of information. I understand that just because copying programs and data is easy, it is not necessarily right.
- I will not break into or use other people's computers or read or use their information without their consent.
- I will not write or knowingly acquire, distribute, or allow intentional distribution of harmful software like bombs, worms, and computer viruses.

(ISC)2 Code of Ethics

Code of Ethics Preamble

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons

- Protect society, the commonwealth, and the infrastructure.
- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally:

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals:

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and protect the profession:

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.

Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

Bases for Ethical IT Decision Making

Golden rule

Treat others as you wish to be treated. Is your software company itself using unlicensed software?

Kant's categorical imperative

If something isn't right for one person, it isn't right for anyone. Do you tell employees not to use bandwidth for personal use, when you do this yourself?

Descartes' rule of change

If an action isn't right at a particular time, it isn't ever right. Should your website "frame" pages from other websites as if they're your own work?

The Utilitarian principle

Always perform actions which will maximize the good. Should you violate someone's right to privacy by accessing their e-mail account, if you have reason to suspect they may be stealing trade secrets?

Risk aversion principle

When actions will cause harm, choose the action that will do the least damage. If a manager accuses an employee of criticizing the manager in an e-mail, who should search for an read the offending e-mails?

Do no harm

Does your company's privacy policy protect the interests of its customers?

No free lunch rule

Assume all information and property, especially intellectual property, belongs to someone. Does your company use unlicensed software?

Legalism

Moral actions may be illegal, and vice versa. Does your advertising exaggerate the benefits of using your product?

Professionalism

When you explain alternatives to managers who don't really understand them, do you give them all the information they need to make an informed choice?

Evidentiary guidance

If there is data to inform your decisions, you have a responsibility to take it into account. Do you assume you know what's best for employees or do you gather data to find out what they really think?

Client/customer/patient choice

If customers or clients are affected, let them give their input. Do you monitor employees where they assume they have privacy?

Equity

Are those in similar situations provided with the same access to data or systems?

Competition

Consumers can choose between companies offering a service. When you make a proposition to those in management, do they know what risks are involved?

Compassion/last chance

You should refuse to take unfair advantage of those who are vulnerable because of their lack of technical knowledge. Do all employees have the opportunity to benefit from your organization's IT investments?

Impartiality/objectivity

When you make decisions, is there a conflict of interest?

Openness/full disclosure

Are those affected by a system, such as a website's information-gathering application, aware of its existence and what the information will be used for?

Confidentiality

Have you cut no corners in ensuring that information on individuals is secure?

Trustworthiness and honesty

Does the IT Department at your company circulate and fully endorse an ethics code?