



SWANSEA METROPOLITAN UNIVERSITY

PRIFYSGOL FETROPOLITAN ABERTAWE

Swansea Business School, Swansea Metropolitan University

Codes of Ethics

Tutors:

Steve Griffiths

steve.griffiths@smu.ac.uk

Caroline Jawad

caroline.jawad@smu.ac.uk

Assignment Title:	Cyber ethics	Management	Assignment No (x of x):	1 of 1
-------------------	-----------------	------------	-------------------------	--------

Code of Conducts:

A formal code of conduct is a common CSR tool employed by companies to establish and communicate responsible business practices and an ethical organizational culture (Erwin, 2011). These codes are perceived as fundamental to the establishment of CSR policies within an organization and essential to creating and sustaining an ethical organizational culture (Collins, 2004). Rezaee et al (2001) state that corporations perceive the establishment of corporate codes of conduct as achieving the following goals:

1. Fostering their corporate moral principles and values
2. Communicating and monitoring their ethical expectations to employees
3. Demonstrating their commitment to ethical values
4. Providing legitimacy for possible legal actions
5. Helping individuals resolve ethical dilemmas

The codes of conduct and administrative procedures are the first line of damage control as litigation experts will focus on them right away (Agatiello, 2008). Somers' (2001) research supports the proposition that employees in organisations that had adopted corporate codes of ethics were significantly less aware of wrongdoing than the employees in organisations without codes of ethical conduct, and that ethical codes implemented by work organisations serve to set guidelines for individual behaviour in organisations, thereby inhibiting wrongdoing.

Recent corporate scandals such as Enron and Parmalat have brought to the forefront the importance of having strict conflict of interest standards in place (Hurst, 2004). New employees should fully understand the conduct and behaviour that the employer expects from the outset. Communicating appropriate policies and procedures can help eliminate unacceptable behaviour and work habits, and may be helpful if it becomes necessary to dismiss employees who cannot meet minimum standards (Hurst, 2004).

However Small (2001) argues that “by defining moral obligations in a formal fashion, they give the impression that these may be satisfied by a single procedure of compliance, rather than through a continuing process of considering the ethical aspects of one’s actions. As Homan (1992) puts it, “Statements of ethics invite the individual to surrender the moral conscience to a professional consensus”.

State/Government Regulation:

Campbell (2007) proposes that “corporations are more likely to behave socially responsible if strong and well-enforced state regulations are in place to ensure such behaviour”. The likelihood of this is enhanced if regulations and enforcement capacities are based on negotiation and consensus among corporations, government and other relevant stakeholders (Campbell, 2007; 955). According to Eriksen (2009), “regulations can take place at both national and international level, but it is argued that due to changes brought on by globalization it is becoming more difficult for regulatory authorities to set the ‘rules of the game’”.

Polishchuk (2009) explains “the effectiveness of government regulation depends on the complexity and scale of the tasks that are being implemented and the ability of regulatory authorities to perform their functions effectively. The more complex and numerous the tasks requiring regulation and the greater the doubts regarding the government’s ability to accomplish them, the more grounds there are for relying on CSR”. Government regulation often fails to keep pace with changes in economic and social needs. These shortcomings could become the basis for turning to alternative tools, including CSR (Husted & Salazar, 2006)

Governments at different levels can regulate the behaviour or practices of businesses by defining minimum standards for business performance embedded within the legal framework; establishing targets for business to achieve; setting up enforcers and inspectorates to oversee business conduct; promulgating codes or laws to confine undesirable business conduct; or imposing license of operation or mandatory environmental friendly industrial systems. Examples of this include

establishing a minimum age for labour forces, emission limit values for particular categories of industrial productions, or requirements for companies to publicize corporate social responsibility reports (Kitthananan, 2010).

The argument that regulation would hinder voluntary efforts on the part of the company to improve their behaviour has been readily accepted by a government keen to avoid its regulatory duties when it comes to curbing corporate power. Regulation, including rules on: how corporations can be structured, as well as on the impacts they can have on the environment and society, and their dealings with their workforce and other stakeholders, is the only way that a democratic society can control what is acceptable and unacceptable in corporate behaviour. If the corporation is left to regulate itself then far from curbing it, the corporation gains power (Corporate Watch, 2006).

Industry/Self-Regulation:

Self-regulation means that corporations voluntarily adopt rules and standards that exceed the requirements of public regulation (Neergaard & Perdersen, 2003, p.44). Campbell (2007) state that "corporations are more likely to behave socially responsible if there is a system of well-organized and effective industrial self-regulation in place to ensure such behaviour". Self-regulation is argued to offer a win-win-win situation for corporations, regulatory authorities and society (Eriksen, 2009). For corporations the advantage of self-regulation is that it protects them from public regulation and external stakeholder pressures; for regulative authorities the advantage is the reduced need to implement unpopular and costly command-and-control policies and. In addition, society sees an advantage in self-regulation because CSR related standards outdo governmental regulative requirements (Neergaard & Perdersen, 2003, p.48) . The General Accounting Office (2011) state that "the justification for relying on industry self-regulation is that firms have more information, expertise and resources than government regulators".

According to Sacconi (2004), “self-regulation is nothing other than self-discipline whereby the firm does not behave in a manner such to abuse the trust that stakeholders have placed in it”. Compliance with the norms creates reputation; reputation induces a cooperative response from the stakeholders; those who abide by the norms are thus offered a benefit; and this benefit acts as an incentive for complying with the norms (Sacconi, 2004). This suggests that some businesses are only implementing self-regulation for their self-interests and to satisfy the stakeholders.

KPMG (2006) outline and explained the advantages and disadvantages of self-regulation:

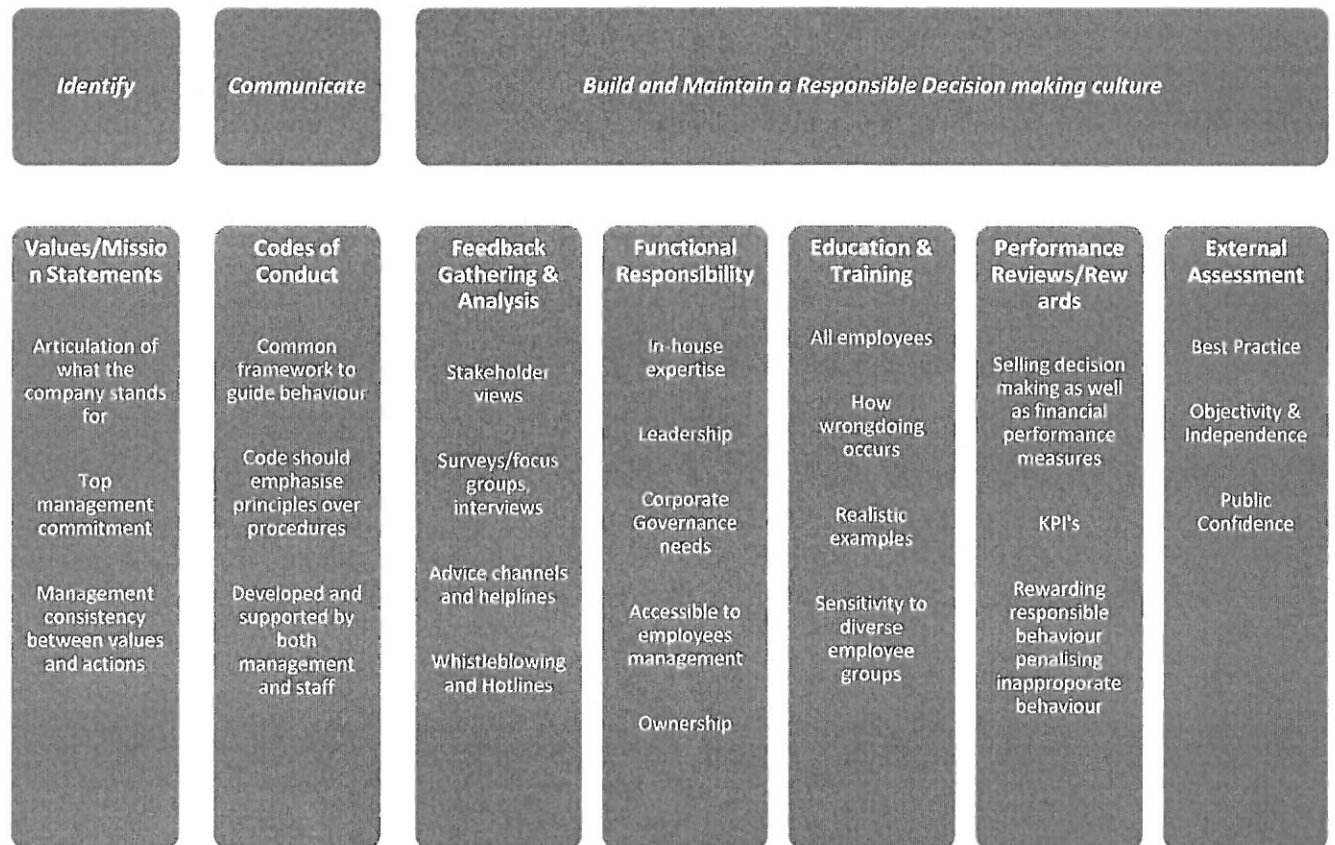
Table 1 – Advantages and Disadvantages of self-regulation (KPMG, 2006)

<u>Advantages</u>	<u>Disadvantages</u>
Proximity Self-regulatory organisations are generally rooted in the industry being regulated, enabling access to more detailed and current industry information which can be especially helpful in rapidly changing sectors. By comparison, government regulators are often playing “catch up.” Being closer to the action, self-regulators are better situated to identify potential problems.	Conflicts of Interest The same proximity that can help the self-regulator acquire useful information can be a disadvantage because of conflicts of interest. Knowing an industry better does not mean that a self-regulator will necessarily have the proper incentives to regulate it more effectively.
Flexibility Self-regulatory organisations can act with greater flexibility than government regulators: they are not subject to the same procedural and due process hurdles or political constraints as	Inadequate Sanctions The greater flexibility afforded to self regulatory organisations also means they may have the discretion to administer only modest sanctions against serious violators.

government. Governmental regulators are often not inclined to deal with politically unpopular or highly complex issues, so these issues may be more suitably delegated to self-regulatory bodies. Compliance Self-regulation may generate a higher level of compliance.	Under-enforcement
	Global Competition In a global marketplace, an industry's collective interest may be defined by competition with foreign markets. If foreign markets are not equally burdened with regulation, then aggressive self-regulation could disadvantage domestic firms. This provides yet another reason to question whether self regulators will make decisions that will benefit society.

Figure 2 shows key elements of an ethical programme within a business conducted from a survey by Arthur Andersen (2000). The survey shows that the desire to protect or improve reputation is the most common factor influencing the development of business ethics activities among major UK companies and that such activity is more common among "heavily branded" companies (Gordon, 2000).

Figure 2- Cornerstones of a Business Ethics Programme (Andersen, 2000)



Porter and Kramer (2006) stated, when done strategically and deliberately, CSR "can be much more than a cost, a constraint, or a charitable deed—it can be a source of opportunity, innovation and competitive advantage". For example, products that are partial damaged and not fit for selling can be donated to charities free-of-charge instead of disposing them. It will save the business cost of disposal and increased the business reputation for doing CSR for charities.

Home > Tools > Samples > Code of Business Conduct - Sample

TOPICS

Audit Committee & Board
Business Continuity Management
Control Self Assessment
Corporate Governance
COSO
Enterprise Risk Management
Fraud & Ethics
IFRS
Internal Audit
IT Audit
IT Governance
Sarbanes-Oxley
All Topics

TOOLS

Work Programs
Audit Reports
Charters
Checklists & Questionnaires
Guides
Job Descriptions
Methodologies & Models
Policies & Procedures
Process Flows
Samples
All Tools

April 25, 2011

Code of Business Conduct - Sample

 Add to my favorites

Prepared By:	
Approved By:	
Revision Date:	
Effective Date:	

INTRODUCTION:

This Code of Business Conduct covers a wide range of business practices and procedures. It does not cover every issue that may arise, but it sets out basic principles to guide all employees and officers of the Company (Company includes Company A and all its subsidiaries). All of our employees and officers must conduct themselves accordingly and seek to avoid even the appearance of improper behavior. The code should also be provided to and followed by the Company's agents and representatives. In addition, Company policies apply to various Company operations and you need to know and follow those policies that apply to your Company work.

If a law conflicts with a policy in this code, you must comply with the law. Alternatively, if a local custom or policy conflicts with this code, you must comply with the code. If you have any questions about these conflicts, you should ask your supervisor how to handle the situation. Employees and officers are responsible for understanding the legal and policy requirements that apply to their jobs and reporting any suspected violations of law, this code, or Company policy.

Those who violate the standards in this code will be subject to disciplinary action, including possible dismissal. Furthermore, violations of this code may also be violations of the law and may result in civil or criminal penalties for you, your supervisors and/or the Company. If you are in a situation which you believe may violate or lead to a violation of this code, follow the procedures set out in Section 19 of this code.

The basic principles discussed in this code are subject to any Company policies covering the same issues.

1. COMPLIANCE WITH LAWS, RULES AND REGULATIONS

Obeying the law, both in letter and in spirit, is the foundation on which this Company's ethical standards are built. All employees and officers must respect and obey the laws, rules, and regulations of the cities, states, and countries in which we operate. Although employees and officers are not expected to know the details of each of these laws, rules and regulations, it is important to know enough to determine when to seek advice from supervisors, managers or other appropriate personnel.

2. CONFLICTS OF INTEREST

A "conflict of interest" exists when a person's private interest interferes in any way, or even appears to interfere, with the interests of the Company. A conflict situation can arise when an employee or officer takes actions or has interests that may make it difficult to perform his or her Company work objectively and effectively. Conflicts of interest may also arise when an employee or officer (or a member of his or her family) receives improper personal benefits as a result of his or her position in the Company. Loans to, or guarantees of obligations to, employees and officers and their family members by the Company may create conflicts of interest and in certain instances are prohibited by law.

It is a conflict of interest for a Company employee or officer to work for a competitor, customer or supplier. You should avoid any direct or indirect business connection with our customers, suppliers or competitors; except as required on our behalf.

Conflicts of interest are prohibited as a matter of Company policy, except as approved by the board of directors. Conflicts of interest may not always be clear-cut, so if you have a question, you should consult with your supervisor or follow the procedures set out in Section 19. Any employee or officer who becomes aware of a conflict or potential conflict should bring it to the attention of a supervisor, manager, or other appropriate personnel or consult the procedures provided in Section 19 of this code.

3. INSIDER TRADING

All non-public information about the Company should be considered confidential information. Employees and officers who have access to confidential information about the Company or any other entity are not permitted to use or share that information for trading purposes in Company A, the other entity's securities, or for any other purpose except for the conduct of the Company's business. To use non-public information for personal financial benefit or to "tip" others who might make an investment decision on the basis of this information is not only unethical, but also illegal. If you have any questions, please consult the Company's Guidelines for Trading Company Stock.

4. CORPORATE OPPORTUNITIES

Employees and officers are prohibited from taking opportunities that are discovered through the use of corporate property, information or position for themselves without the consent of the board of directors. No employee or officer may use corporate property, information or position for personal gain and no employee or officer may compete with the Company directly or indirectly. Employees and officers owe a duty to the Company to advance the Company's interests when the opportunity to do so arises.

5. COMPETITION AND FAIR DEALING

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information that was obtained without the owner's consent, or inducing such disclosures by past or present employees of other companies is prohibited. Each employee and officer should endeavor to respect the rights of and deal fairly with the Company's customers, suppliers, competitors and employees. No employee or officer should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other illegal trade practice.

No employee or officer is permitted to engage in price fixing, bid rigging, allocation of markets or

SIGN UP FOR A 30-DAY FREE TRIAL

We invite you to use the tools and resources within KnowledgeLeader for free for 30 days so you can discover for yourself how this service will improve your internal audit and risk management capabilities.

Your free trial will expire automatically. There is no obligation to purchase a subscription.

Start Trial

Start Group Trial

LEARN MORE

- > Prices and Ordering
- > KnowledgeLeader Value Proposition
- > KnowledgeLeader Content
- > About KLplus
- > Take a Tour
- > What Our Customers Say
- > KnowledgeLeader University Program
- > About Protiviti

customers, or similar illegal activities.

To maintain the Company's valuable reputation, compliance with our quality processes and safety requirements is essential. All inspection and testing documents must be handled in accordance with all applicable specifications and requirements.

The purpose of business entertainment and gifts in a commercial setting is to create goodwill and sound working relationships, not to gain unfair advantage with customers. No gift or entertainment should ever be offered, given, provided or accepted by any Company employee or officer, family member of an employee or officer, or agent unless it: (1) is not a cash gift, (2) is consistent with customary business practices, (3) is reasonable in value, (4) cannot be construed as a bribe or payoff and (5) does not violate any laws, regulations or applicable policies of the other party's organization. Please discuss with your supervisor any gifts or proposed gifts that you are not certain are appropriate.

6. POLITICAL CONTRIBUTIONS

Except as approved in advance by the chief executive officer or chief financial officer, the Company prohibits political contributions (directly or through trade associations) by the Company or its business units. This includes: (a) any contributions of Company funds or other assets for political purposes; (b) encouraging individual employees to make any such contribution; or (c) reimbursing an employee for any contribution.

Individual employees are free to make personal political contributions as they see fit.

7. DISCRIMINATION AND HARASSMENT

The diversity of the Company's employees is a tremendous asset. We are firmly committed to providing equal opportunity in all aspects of employment and will not tolerate any illegal discrimination or harassment based on race, color, religion, sex, national origin or any other protected class. For further information, consult the appropriate Company policy.

8. HEALTH AND SAFETY

The Company strives to provide each employee and officer with a safe and healthy work environment. Each employee and officer has the responsibility for maintaining a safe and healthy workplace for all employees and officers by following environmental, safety, and health rules and practices and by reporting accidents, injuries and unsafe equipment, practices or conditions. Violence and threatening behavior are not permitted.

Employees and officers are expected to perform their Company related work in a safe manner, free of the influences of alcohol, illegal drugs or controlled substances. The use of illegal drugs in the workplace will not be tolerated.

9. ENVIRONMENTAL

The Company expects its employees and officers to follow all applicable environmental laws and regulations. If you are uncertain about your responsibility or obligation, you should check with your supervisor, unit manager or the Corporate Vice President - Administration for guidance.

10. RECORD-KEEPING, FINANCIAL CONTROLS AND DISCLOSURES

The Company requires honest, accurate and timely recording and reporting of information in order to make responsible business decisions.

All business expense accounts must be documented and recorded accurately in a timely manner. If you are not sure whether a certain expense is legitimate, ask your controller. Policy guidelines are available from your controller.

All of the Company's books, records, accounts and financial statements must be maintained in reasonable detail; must appropriately reflect the Company's transactions; must be promptly disclosed in accordance with any applicable laws or regulations; and must conform both to applicable legal requirements and to the Company's system of internal controls.

Business records and communications often become public and we should avoid exaggeration, derogatory remarks, guesswork or inappropriate characterizations of people and companies that may be misunderstood. This applies equally to e-mail, internal memos and formal reports. Records should always be retained or destroyed according to the Company's record retention policies. In accordance with those policies, in the event of litigation or governmental investigation, please consult the Corporate Vice President - Administration.

11. CONFIDENTIALITY

Employees and officers must maintain the confidentiality of proprietary information entrusted to them by the Company or its customers or suppliers, except when disclosure is authorized in writing by the chief financial officer or required by laws or regulations. Proprietary information includes all non-public information that might be of use to competitors or harmful to the Company or its customers or suppliers if disclosed. It includes information that suppliers and customers have entrusted to us. The obligation to preserve proprietary information continues even after employment ends.

12. PROTECTION AND PROPER USE OF COMPANY ASSETS

All employees and officers should protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. All Company assets are to be used for legitimate Company purposes. Any suspected incident of fraud or theft should be immediately reported for investigation. Company assets should not be used for non-Company business.

The obligation of employees and officers to protect the Company's assets includes the Company's proprietary information. Proprietary information includes intellectual property such as trade secrets, patents, trademarks and copyrights, as well as business, marketing and service plans, engineering and manufacturing ideas, designs, databases, records, salary information, and any unpublished financial data and reports. Unauthorized use or distribution of this information is a violation of Company policy. It could also be illegal and result in civil or criminal penalties.

13. PAYMENTS TO GOVERNMENT PERSONNEL

The U.S. Foreign Corrupt Practices Act (FCPA) prohibits giving anything of value (directly or indirectly) to officials of foreign governments or foreign political candidates in order to obtain or retain business. While the FCPA does, in certain limited circumstances, allow nominal "facilitating payments" to be made, any such payment must be discussed with local management and the Corporate Vice President - Administration before any such payment can be made.

In addition, the U.S. government has a number of laws and regulations regarding business gratuities, which may be accepted by U.S. government personnel. The promise, offer or delivery to an official or employee of the U.S. government of a gift, favor or other gratuity in violation of these rules would not only violate Company policy but will also commit a civil or criminal offense. State and local governments, as well as foreign governments, often have similar rules.

14. TRADE ISSUES

From time to time, the United States, foreign governments, and the United Nations have imposed boycotts and trading sanctions against various governments and regions, which must be obeyed. Advice regarding the current status of these matters must be obtained from the chief financial officer.

15. WAIVERS OF THE CODE OF BUSINESS CONDUCT AND ETHICS

Any waiver of this code for executive officers or directors may be made only by the board of directors and will be promptly disclosed as required by law or regulation.

16. REPORTING ANY ILLEGAL OR UNETHICAL BEHAVIOR

Employees are encouraged to talk to supervisors, managers or other appropriate personnel about observed behavior that they believe may be illegal or a violation of this Code of Conduct or Company policy or when in doubt about the best course of action in a particular situation. It is the policy of the Company not to allow retaliation for reports made in good faith by employees of misconduct by others. Employees are expected to cooperate in internal investigations of misconduct.

17. IMPROPER INFLUENCE ON CONDUCT OF AUDITORS

It is prohibited to directly or indirectly take any action to coerce, manipulate, mislead or fraudulently influence the Company's independent auditors for the purpose of rendering the financial statements of the Company materially misleading. Prohibited actions include, but are not limited to, those actions taken to coerce, manipulate, mislead or fraudulently influence an auditor: (1) to issue or reissue a report on the Company's financial statements that is not warranted in the circumstances (due to material violations of generally accepted accounting principles, generally accepted auditing standards, or other professional or regulatory standards); (2) not to perform an audit, review or other procedures required by generally accepted auditing standards or other professional standards; (3) not to withdraw an issued report; or (4) not to communicate matters to the Company's audit committee.

18. FINANCIAL REPORTING

As a public company, it is necessary that the Company's filings with the U.S. Securities and Exchange Commission be accurate and timely. The Company expects employees and officers to take this responsibility very seriously and provide prompt and accurate answers to inquiries related to the Company's public disclosure requirements.

The Company's policy is to comply with all financial reporting and accounting regulations applicable to the Company. If any employee or officer has concerns or complaints regarding accounting or auditing matters of the Company, then he or she is encouraged to submit those concerns by one of the methods described in Section 19.

19. COMPLIANCE PROCEDURES

We must all work to ensure prompt and consistent action against violations of this code. However, in some situations it is difficult to know right from wrong. Since we cannot anticipate every situation that will arise, it is important that we have a way to approach a new question or problem. These are the steps to keep in mind:

(a) Make sure you have all the facts. In order to reach the right solutions, we must be as fully informed as possible.

(b) Ask yourself: What specifically am I being asked to do? Does it seem unethical or improper? This will enable you to focus on the specific question you are faced with and the alternatives you have. Use your judgment and common sense; if something seems unethical or improper, it probably is.

(c) Discuss the problem with your supervisor. This is the basic guidance for all situations. In many cases, your supervisor will be more knowledgeable about the question and will appreciate being brought into the decision-making process. Remember that it is your supervisor's responsibility to help solve problems. If you are uncomfortable discussing the problem with your supervisor, you can talk to your general manager or human resources manager.

(d) Seek help from Company resources. In a case where it may not be appropriate to discuss an issue with your supervisor or local management, call XXX-XXX-XXXX which will put you in direct contact with the Vice President - Administration at Company headquarters. If you prefer to write, address your concerns to the Vice President - Administration or the audit committee of the board of directors. Anonymous reports can be made through the internet to www.CompanyA.com or for calls originating in the United States X-XXX-XXX-XXXX, for calls originating from foreign countries follow the normal collect call procedures for your country and ask to be connected to XXX-XXX-XXXX.

(e) You may report violations in confidence and without fear of retaliation. If your situation requires that your identity be kept secret, your anonymity will be protected. The Company does not permit retaliation of any kind against employees or officers for good faith reports of suspected violations.

(f) Always ask first, act later: If you are unsure of what to do in any situation, seek guidance before you act.

(g) All employees and officers are subject to the Company's code, which describes procedures for the internal reporting of violations of the code. All employees and officers must comply with those reporting requirements and promote compliance with them by others. Failure to adhere to this code by any employee or officer will result in disciplinary action up to and including termination.

20. ANNUAL ACKNOWLEDGEMENT

To help ensure compliance with this Code of Business Conduct, the Company requires that all exempt salaried employees and officers review the Code of Business Conduct and acknowledge their understanding and adherence in writing on an annual basis on the attached form.

Download the sample:



Code of Business Conduct - Sample.doc

Criteria for evaluation of a Professional Code

You will be looking at a specific problem but I would like to get a digital copy of your assignment to try to do a comparison

Generic Criteria	BCS	HSBC	Australian Computing society	IEEE	
Accessibility- Drill downs or access to paper document					
Length of code-Pages					
Quality of code-general ethical content-accessibility of language					
Quality of code-general ethical content-% in relation to other non ethical material					
Training to implement the code					
Assignment of responsibility for ethical management e.g. Ethics committee					
Sanctions for unethical behaviour					
Senior Management or Committee support for code					
Target areas of ethical risk					
Links to other organisations for support					

Date the document was written or updated					
--	--	--	--	--	--

Problem specific criteria

Reference to the problem					
Examples to aid understanding of and resolve the problem					
Ease of understanding					
Specific sanctions					
Offers of help					
Whistle blowing policy					

You will effectively be using CONTENT ANALYSIS. We need to discuss the problems of coming to a verdict "Good" or Bad" code. If possible everyone should agree on how to make a judgement as we discussed when looking at the Portuguese Computing Society code.

The code may be good generally but not for the issue you are concerned with and vice versa

You can use the general stuff to analyse the code in general see code articles and my notes

The specifics which justify what you put in the table need to be analysed

e.g. I felt it was accessible because there were clear links from the home page, see screen grab

e.g. the language was accessible as the vocabulary was not too difficult or there was a link to a user friendly manual

e.g. despite the BCS listing training courses these tended to be annual and largely based in London, a problem for Computer Professionals in the provinces

Ethical aspects of e-business: the use of codes of conduct

Mike Healy and Jennifer Iles

Introduction

Confidence and trust have long been seen as key elements in helping an organisation establish an ongoing relationship with customers, clients and other organisations, depending on the specific nature of the business activity. Whereas in the past such relationships were built upon either personal contact or organisation reputation, relationships mediated through the use of information communication technology create a range of possible barriers to the development of these elements. Organisations therefore have to prove their online reliability.

The expansion both in depth and breadth of e-business creates a number of problems for those responsible for the management of the process and the people involved. This paper looks at one aspect of this process, namely the extent and use of codes of conduct governing the application of Internet technology within organisations, and forms part of an ongoing study concerned with ethical issues in this area. The need for codes of conduct for information systems professionals is well established (Hoffman and Moore 1992). Now that regular computer use by non-IS professionals is the norm, and given the nature, quality and quantity of electronic information available today and the ease with which it can be accessed, it is pertinent to question whether codes covering computer use by all employees should also be instituted.

Evidence from a variety of Internet industry analysts such as MediaCast and the International Data Corporation (IDC) indicates that business to consumer e-commerce (B2C) is expanding at

a rapid rate. IDC predicts that "revenues from e-commerce in Europe will total €124 billion (US\$118.6 billion) by 2003 up from €10.3 billion (US\$9.85 billion) in 1999."¹ Based on data from a survey of 332 UK firms, MediaCast predicts that during the next two years the number of firms generating 40% plus of their sales through Internet trading will increase from 6% to 25%.² However, while there continues to be a significant growth in B2C e-commerce, there is evidence that consumers have serious misgivings about buying online. Research undertaken by MORI for the UK National Consumer Council found that 35% of British consumers agreed with the statement: "The Internet is the most insecure place to conduct a transaction."³ Furthermore, some 55% of UK Internet users believed that buying online is a risky exercise.

As the histories of the dot.com companies show, e-commerce is an intensely competitive environment, and not even well established retailers such as C&A are immune from crisis. There is strong evidence to suggest that successful e-commerce organisations appear to be evolving towards a convergence of models where traditional retail firms lock into an Internet strategy based on alliances or partnerships with existing dot.com companies. For example, Dixons embraces what it calls the 'Martini approach' while others refer to it as a 'multi-channel retailing environment'. The Kingfisher group has invested £3 million in a 7.5% stake in ThinkNatural.com, the online healthcare products company, and Marks and Spencer has invested in Talkcast, a digital publishing group, as well as developing close working links with Splendour.com, an online lingerie business.

If e-commerce is growing, e-business is booming. Internet research organisations such as Jupiter Communications⁴ estimate that in the US alone e-business revenues are likely to increase from US\$336 billion this year to US\$6.3 trillion by 2005. Research from the Boston Group⁵ supports the magnitude of this estimate. The Gartner Group⁶ believes that global B2B transactions will increase from US\$154 billion in 1999 to US\$7.29 trillion in 2004, accounting for some 7% of all global business sales transactions. As with e-commerce, such expansion will lead to the development of complex business partnerships using an Internet infrastructure. Hence, for example, AOL has linked up with a provider of a business exchange platform provider called PurchasePro.com to provide a tailor-made environment for small businesses, thereby allowing these businesses to source and negotiate prices as well as to buy and sell products.

A key aspect of all these developments centres around how much mutual trust will exist between the organisations who form online partnerships and alliances, since such relationships inevitably lead to the sharing of online space, commercially sensitive data, and common procedures based on the application of Internet technology. These circumstances point to a configuration of organisational relationships based on a close identity of aims and objectives. Under these conditions non-technical factors, such as confidence and trust, are just as important as the development of a technically secure working environment.

The application of Internet technology to business activities creates a number of problems that generate a sense of unease among customers of various types. It is generally assumed that organisations seeking to develop an online presence would want to promote the idea that any information about customers or clients would be secure. However, existing research seems to indicate that there is a problem here. In 2000, the Unisys Annual Fraud Survey of 1,166 financial services organisations such as building societies revealed that although 56% of such institutions knew they were vulnerable to online fraud, 95% of board members did not receive any fraud awareness training. Clearly the majority of firms in the finance sector have not implemented any practical

measures to counter the potential threat arising from electronic fraud. That survey also found that 85% of companies had not adapted their 'know your customer' identification procedures to the Internet. This finding is of some significance given that in the UK it is a legal requirement that financial institutions know the true identity of every customer. The Unisys research indicates that the vast majority of such institutions have no robust procedures for establishing such an identity online. Evidence such as this actively discourages client confidence and trust in a range of organisations. The cases of Powergen, Egg, and Barclays in the UK all underline the enormous damage that an Internet information systems failure can inflict on businesses seeking to utilise Internet technology.

At the same time that there has been a growth in the use of Internet technology within businesses, between businesses, and between businesses and consumers, there has also been an increasing sensitivity to what might be broadly defined as ethical issues. The UK election result of 1997, the horror over the response to the Paddington rail crash, and changing attitudes to GMO foods – all are examples of a growing concern with ethics in business. A recent MORI poll undertaken on behalf of the Co-operative Bank indicates that 25% of the British public have "actively sought information on a company's ethical practices and policies" in the last twelve months.⁷ Research by the Institute of Business Ethics⁸ indicates that there has been an increase in the number of firms adopting a code of ethics covering business activities. Part of this expansion has been the introduction of codes of conduct geared towards the actions of employees using information technology. It is these codes that form the basis of this study.

Methodology

Our survey was conducted among part-time postgraduate students of the Westminster Business School at the University of Westminster. It was decided to target part-time students since these were currently employed within a variety of

commercial and other organisations. It was also decided to focus on the students in one particular course, the Diploma in Personnel Management, since students on this course invariably come from a human resources background and should therefore be aware of the ethical issues the survey sought to address. The objectives of the exercise were to determine the extent to which codes of conduct specifically tailored to information technology existed within organisations dependent on Internet technology, to measure awareness of both the scope and authorship of such codes, and to ascertain if disciplinary action had been taken against employees who breached such codes.

A questionnaire was developed comprising 25 multiple-choice questions, all of which required tick box responses, and in some cases a brief written answer if a box such as 'Other – please specify' was ticked. It was decided that the questionnaire should be anonymous to encourage an honest response to all the questions. Questions 1 to 4 were concerned with organisational profile, 5 to 12 were intended to determine both the degree and function of information technology within organisations, 13 to 17 attempted to assess the use of Internet technology within organisations, 18 and 19 looked at the way in which the Internet is used by employees, 20 to 24 sought to determine the scope, authorship, current responsibility for,

and distribution of codes of conduct covering the use of information technology, and questions 24 and 25 were intended to measure the number of and reasons for disciplinary action arising from breaches of the codes.

One hundred and twenty questionnaires were distributed in paper form to students at the start of their evening class and were collected during the first break. This method had two strengths; it resulted in a high response rate with 80 papers returned, and it ensured that students on the targeted course, the Diploma in Personnel Management, were encouraged to complete and return the questionnaire. A possible weakness was that it allowed students working for the same organisation to each submit a questionnaire. However, it was felt that since such duplication was likely to be minimal and the quality of response would be high, this weakness would not ultimately undermine the collection of the data.

Results

The first part of this section seeks to establish the profile of the survey group with respect to the access and use of information technology. As can be seen from Figure 1 below, there was a good spread of organisation type represented in the

Figure 1. Types of organisation

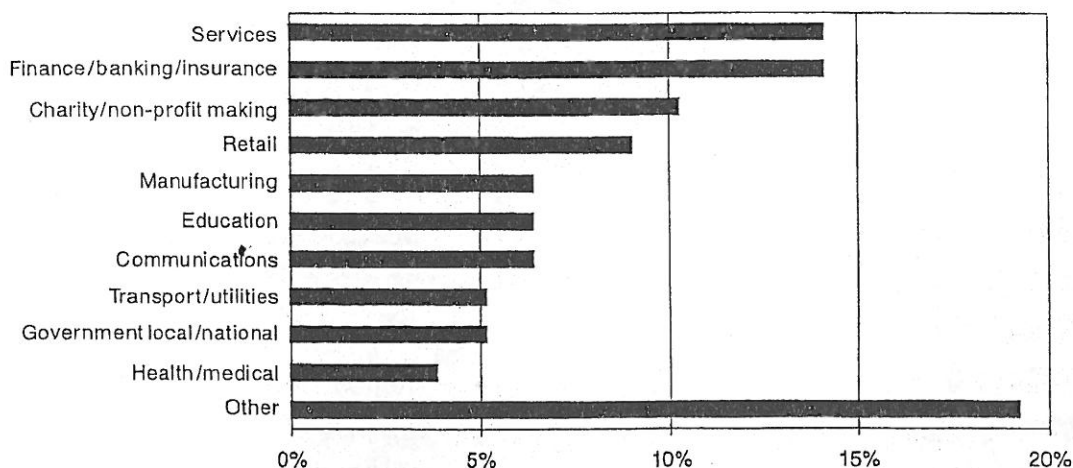
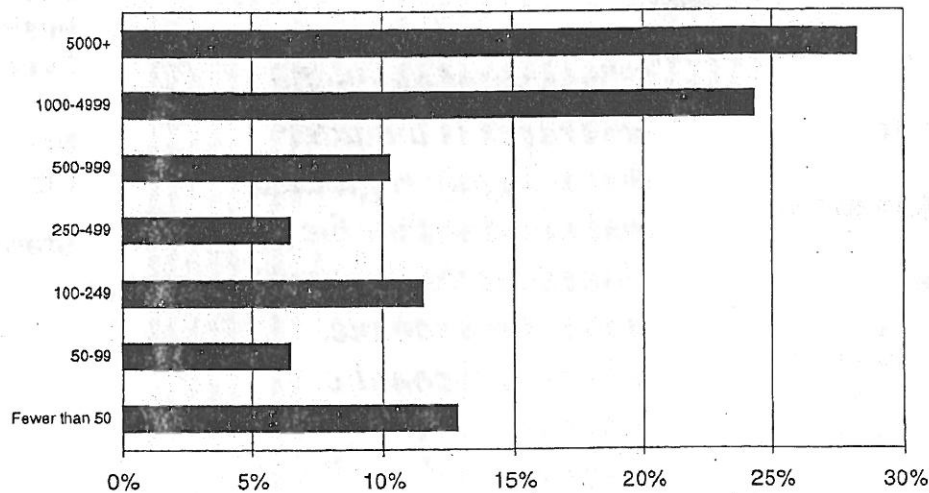


Figure 2. Number of employees



survey. It was expected that there would be a greater response from the finance/banking and services sectors, since students from these sectors are attracted to the post-graduate courses running at the Westminster Business School. However, the survey revealed that a significant number, approximately 15%, worked in the public sector (education, government, and health).

Figure 2 shows that although there was a spread of organisation by size in the survey there was a greater representation from organisations with more employees.

The results from Figures 1 and 2 indicate that the survey covered a range of organisation by type, size and extent of use of information technology which was acceptable for research of this kind. The next section looks at the utilisation of a number of key Internet technologies by the organisations.

Respondents were asked to say how long their organisation had been connected to the Internet. The response to this question shows that while only 4.5% of organisations were not connected to the Internet, 15% had been online for more than five years. Since this survey was undertaken towards the end of 1999, it is likely that this percentage will by now have increased. The bulk of organisations covered, some 55%, had been online between one and four years. Perhaps an

interesting result from this question is that every one of the respondents knew of the online status of their organisations.

The survey also sought to measure the extent of e-mail use within the surveyed group: it revealed that the vast majority, almost 85%, of the organisations covered, make use of e-mail for both internal and external communications. This is a significant finding since the abuse of e-mail, both internally and externally, is increasingly seen as a major problem facing managers working in an environment committed to the use of Internet technology. The concern within commercial organisations in the UK about employee misuse of e-mail and Internet facilities has led to legislation being passed which allows them, from October 2000, to monitor employees' e-mail, phone calls and Internet use.⁹

Respondents were also asked to indicate the extent to which intranets and extranets are used within their organisations. Results here show that approximately 68% of organisations covered have an intranet in place: this provides further evidence that the organisations covered routinely use a range of Internet technologies to store, retrieve, interrogate and communicate data and information. The results of a question concerned with extranet use show that only 19% make use of this facility. This result says something about the

perceptions of the novel and perhaps uncertain nature of extranets. However, it is still the case that almost a fifth of respondents indicated that their organisations have an extranet in place, and it can be reasonably anticipated that the proportion of organisations using this facility will grow in the medium term.

The next part of the paper looks at codes of conduct governing the use of information technology. Replies to the questionnaire show that almost 59% of those surveyed indicated that their organisations had a written code of conduct. This finding is not entirely unexpected since research undertaken by the Institute of Business Ethics in the UK (LeJeune and Webley 1998) revealed that over 60% of the organisations they contacted had such codes. Given the profile of the group surveyed – part-time students with a human resource background – it is perhaps surprising that 21% of respondents did not know if their organisations had a code. (It could be argued that lack of employee awareness of a code effectively equates to not having a code.) The survey also revealed a degree of unevenness between sectors in respect of codes of conduct covering the use of information technology. For example, whilst 70% of financial/banking/insurance organisations, 75% of local/national government organisations, and 63% of charitable organisations had codes of conduct in place, only 20% of educational institutions represented in the sample had an appropriate code of conduct governing the use of information technology.

The survey also sought to establish whether the type or size of organisation as well as length of time on the Internet and/or the use of information technology had any influence on the existence and nature of codes of conduct. All types of organisation, apart from transport, indicated that they had a code of some kind in place. In terms of organisation type, the questionnaire revealed that 63% of those in the charity/non-profit making sector had a written code compared with 33% in the health/medical sector. The survey shows that the service and financial sectors, which have been at the sharp end of developments in information technology, both have a relatively high number of organisations, some 63%, with a written code. However, it was the government national/local

sector that showed the highest proportion, some 75%, of organisations with a code. This contrasts dramatically with the education sector where only 20% of organisations were found to have a code.

An examination of the relationship between the size of organisation and code of conduct indicates there is no firm evidence linking size to code. While the survey shows that 64% of organisations with more than 5000 employees have a code, compared to 40% of those with fewer than 50 employees, it also indicates that the category of organisation with the highest proportion of codes (78%) was that with between 100 and 249 employees.

Looking at computer density as a factor influencing the existence of codes of conduct, the survey found that of those organisations with over 75% of staff using personal computers, the percentage using a code was 66%. This compares with 55% for organisations with less than 25% of staff using computers. For the rest of the organisations with other rates of computer density, the figure was 50%. The survey also indicates that there is no strong correlation between the length of time an organisation has been online and the existence of a code. The survey confirmed the view that e-mail use is prevalent across a wide range of organisations. However, the survey also revealed that only 62% of organisations using e-mail have a written code determining the use and abuse of this facility.

The paper will now consider those areas of Internet technology covered by codes of conduct. Sending e-mail (78%), receiving e-mail (74%), visiting Internet sites (74%), downloading files (70%), and virus control (65%), all figured prominently as issues identified as needing to be regulated by respondents whose organisations had a code of conduct in place. Only 22% of organisations have any regulations covering access to online shopping sites while at work. This issue, which has featured significantly in press reports covering the abuse of the Internet at work, does not at present appear to be seen as a major problem. Of more importance were moving equipment and the storage of information about individuals. The survey revealed that 40% of organisations had codes covering both of these issues.

The data relating to the safeguarding of information is significant. The survey evidence shows that 60% of organisations with codes do not include in these appropriate reference to measures designed to safeguard data about individuals. That figure rises to 78% for all responses. Given that information is often considered to be a key element within businesses using information technology, it is surprising to note that only 33% of organisations with codes made any reference to the need to back up data. If applied to all cases, with or without a code, this finding indicates that in 80% of the surveyed group no codified directive exists to highlight the importance of backing up data.

The survey also sought to investigate the ownership of codes by looking at the management levels responsible for initiating and enforcing them. Results showed that the chief executive officer and the human resources department were the most frequent initiators, with 35% and 30% respectively. In only 15% of cases did the information systems/technology department decide on the need for a code of conduct. However, the IS/IT department was cited in 24% of instances as being primarily responsible for *enforcing* the code, and in a further 28% of cases as being partially responsible for enforcing the code. The human resources department was mentioned as being solely responsible in 20% of cases. As might be expected, the results indicate that there is a significant degree of joint responsibility for ensuring adherence to codes, with 35% of cases reporting that code enforcement was the responsibility of more than one department. In 15% of cases, both the IT and the HR departments had joint responsibility for monitoring the code. In only 2% of cases were line managers considered solely responsible for ensuring that employees followed provisions laid down by codes of conduct.

The survey revealed that 40% of organisations with codes had taken disciplinary action arising from employee breaches in such codes. Sending unofficial e-mail and visiting Internet sites were found to be the most significant offences, with 25% and 17% of organisations respectively indicating that disciplinary action had been taken

in such cases. Other offences, such as purchasing online, not applying appropriate virus protection measures, unauthorised storage of data on individuals, and installing unauthorised software, had a very low profile.

Discussion

The evidence obtained from this survey supports other research findings that indicate a growth in the number of organisations introducing codes of conduct covering the use of information technology. The results also show that organisational type and function rather than size seem to be the most influential factors in determining the introduction of codes of conduct. A high proportion of national and local government institutions have codes in place, as have a significant number of those in the service and financial sectors.

The evidence obtained from this survey implies that over 65% of institutions in the medical/health sector and 80% of organisations concerned with education do not have codes in place. This is an important finding, given that institutions in these sectors hold a wide range of confidential data on most of the population in the UK. The results of this survey in this specific area also indicate that further research should be carried out that is more tightly focused on the education and health sectors. Should further research support the findings presented here, it would prompt wider concerns about the commitment of senior managers in these institutions to the protection of private personal data.

The examination of those areas covered by codes of conduct shows a preoccupation with the use of e-mail, visiting websites, downloading unauthorised files, and virus control. These measures are essentially concerned with the efficient functioning of a web-based information system. Other issues more concerned with the safeguarding of data on individuals do not appear to figure prominently in codes of conduct, nor do references to backing-up data.

The findings indicate that whilst information systems/technology departments have a major responsibility for policing codes of conduct, these

departments often do not have ownership of the codes. This is believed to be a significant finding since it highlights a possible weakness in implementing codes due to separation between those who champion the introduction of codes of conduct and those given the responsibility of enforcing them. There are also questions to be raised where code enforcement is a joint responsibility. How closely, for example, do the departments work together? What protocols are in place to ensure consistency in monitoring the use of IT? A further significant finding is that in only 2% of cases were line managers charged with enforcing the code. It is felt that further research is needed into the processes involved in implementing codes of conduct to see if the findings presented here are replicated in other institutions.

The survey findings indicate that a large minority of institutions, some 40%, are prepared to discipline employees who breach codes of conduct concerned with information technology. Further research is required here to establish whether this is a growing trend. And finally, the above findings demonstrate that a significant number of institutions responsible for holding data about individuals have yet to establish effective codes of conduct, and that where such codes do exist they are directed at the efficient functioning of management information systems rather than at the protection of personal data. The practical implications of these findings are that managers in organisations without codes need to review their policies, and managers in organisations which do have codes should review the scope and effectiveness of their codes. Failure to do so could result in a loss of trust with consequent adverse effects on the growth and development of e-business.

Notes

1. <http://www.nua-surveys/> as at 10/04/2000
2. <http://www.nua-surveys/> as at 23/06/2000
3. <http://www.ncc.org.uk/pubs/pdf/ecommerce.pdf> as at 26/10/2000
4. <http://jup.com/company/> as at 27/10/2000
5. <http://www.nua.ie/surveys> as at 08/09/2000
6. <http://www.nua.ie/surveys> as at 21/02/2000
7. MORI: *Ethical Consumerism Research*, <http://www.mori.com/polls/2000/coop-csr.htm>, accessed 27/10/2000
8. Reported in 'Jobs with added value', *The Guardian*, 11/09/2000
9. *Financial Times*, 4/10/2000

References

- Baase, S. 1997. *The Gift of Fire: Social, Legal and Ethical Issues in Computing*. Englewood Cliffs, NJ: Prentice Hall.
- Bynum, T.W. 1998. *Information Ethics: An Introduction*. Cambridge, MA: Blackwell.
- Hoffman, W. M. and Moore, J. M. (Eds.) 1992. *Ethics and the Management of Computer Technology*. Cambridge, MA: Oelgeschlager, Gunn and Hain.
- Kizza, J. M. 1998. *Ethical and Social Issues in the Information Age*. New York: Springer-Verlag.
- Le Jeune, M. and Webley, S. 1998. *Company Use of Codes of Business Conduct*. London: Institute of Business Ethics.
- Spinello, R. A. 1997. *Case Studies in Information Ethics*. Englewood Cliffs, NJ: Prentice Hall.
- Unisys Annual Fraud Survey 2000. Detroit: Unisys Corporation.
- Wagner, I. 1996. 'Confronting Ethical Issues of Systems Design in a Web of Social Relationships'. In Kling, R. *Computerization and Controversy*. New York: Academic Press Inc.

Potential Conflicting Pressures on Managers

- **Personal Contract**
- **Company Code**
- **Industry Code**
- **Functional Code**
- **Professional Codes**
- **Personal Morality**
- **Religion**
- **Social/Cultural Environment**
- **Legal Environment**
- **Enforcement- likelihood & nature of punishment/reward**
- **Country of location**

Which code do I obey?