Information Systems and Ethics

By Dr Danielle McConville, Queen's University Belfast, Examiner for F2 Information Systems

As accountants, our professional ethics should influence all of our day-to-day behaviours and interactions. This is equally the case when we are thinking about engagement with matters relating to information systems as when we are auditing, preparing financial statements or computing/advising on tax.

This article gives some examples of how the ethical principles relate to Information Systems. It brings together some past questions in the area from F2 Information Systems with some guidance on how to approach an ethical issue and/or an exam question on this topic.

Ethical principles

Our ethical principles are contained within the *Code of Ethics for all members* (CPA Ireland, 2019a, para 110):

All members shall comply with the five fundamental principle of ethics;

a) Integrity A member shall be straightforward and honest in all professional and business relationships.

b) Objectivity A member shall not allow bias, conflict of interest or undue influence of others to compromise professional or business judgments.

c) Professional Competence and Due Care A member shall attain and maintain professional knowledge and skill at the level required to ensure that a client or employer receives competent professional service based on current technical developments in practice, relevant legislation and techniques. A member shall act diligently and in accordance with applicable technical and professional standards when providing professional services.

d) Confidentiality A member shall respect the confidentiality of information acquired as a result of professional and business relationships and shall not disclose any such information to third parties without proper and specific authority unless there is a legal or professional right or duty to disclose. Confidential information acquired as a result of professional and business relationships shall not be used for the personal advantage of the member or third parties.

e) Professional Behaviour A member shall comply with relevant laws and regulations and shall avoid any conduct that the member knows or should know might discredit the profession.

Ethics and Information Systems: syllabus requirements

Learning Outcomes for F2 Information Systems (CPA Ireland, 2019b) highlight that students should be able to:

- Recognise and discuss ethical, social, and legal issues in the design and use of information systems including:
    - Ethical, social, and political issues of information systems'
    - The impact of contemporary information systems and the Internet on the protection of individual privacy and intellectual property.

It might also be considered that ethical issues should also be considered under key learning outcomes including:

- Discuss the role of information systems in today's competitive business environment.
- Appraise and discuss the major management challenges to building and using information systems in organisations.
- Analyse and discuss the challenges posed by strategic information systems and management solutions.
- Critically analyse Information Technology-based case studies, thus incorporating their strategic and practical knowledge of Information Systems to real-life business situations.

This article highlights some past paper questions on this area, in two broad categories: how to consider an ethical dilemma, and specific ethical dilemmas.

How to consider an ethical dilemma?

The question below presents a useful framework to consider an ethical dilemma alongside consideration of the concerns that arise in a specific scenario:

<u>April 2015 Question 5c</u>

Explain the process by which you might consider the possible ethical implications of storing and analysing customer data, giving relevant examples. (6 marks)

The solution begins by highlighting the nature of the conflict or dilemma:

Legal concerns: to what extent is the storage and analysis of the data legal with reference to data protection legislation? If not, should it be reported?

Privacy concerns: to what extent is the storage and analysis of the data a breach of the individual's right to privacy, if not illegal? Could harm be caused to that individual by storing that data? A particular concern exists in applying analysis which brings together data from a range of sources to provide highly detailed information on an individual, their interests and past misdemeanours (for example non-obvious relationship awareness (NORA) data analysis).

Security concerns: Are proper procedures in place to secure the data, such as access controls, encryption in transmission? Are proper procedures in place to ensure that the data held on an individual is accurate and up to date (consider the implications of wrong information on, for example, a credit application).

And continues by setting out a process through which these can be considered:
These might be analysed by following a five-step process:

1. Identify and describe the facts clearly: in this case, intention to store and analyse data
2. Define the conflict or the dilemma and identify the principles under threat involved: integrity, confidentiality, possibly also due competence and professional behaviour.
3. Identify the stakeholders: individual involved, the organisation, relevant data protection regulators and other regulatory bodies, the justice system. Is there anyone you can consult (while considering confidentiality)?
4. Identify the options that can reasonably be taken: a range of options from no storage and analysis to storage of information for which permission has not been given and analysis which could cause harm to the individual
5. Identify the potential consequences of your options: harm to the individual, penalties for the organisation and persons responsible, reputational effects.

Specific ethical dilemmas
The process above can be usefully applied in answering questions on specific ethical dilemmas: some examples are below:

<u>April 2019 Question 3c</u>
Analyse the ethical issues arising from storing customers' personal data in cloud environments. (6 marks)

<u>April 2018 Question 1c</u>
Discuss the ethical issues that arise from engaging in social commerce/social marketing, and storing and analysing gathered data. (5 marks)

<u>April 2017 Question 6c</u>
Outline three possible ethical dilemmas arising from organisations' use of social media. (6 marks)

<u>April 2016 Question 6c</u>
Analyse the ethical issues arising from two contemporary information technology trends. (6 marks)

Solutions to these questions are already available to you. Some relevant points to consider are:

- In this specific example, what is at issue? Common issues here include the storage and use of potentially valuable data
- Consider the ethical principles in turn, how might these be impacted upon, e.g.
    - Integrity – are we considering something that might not be considered straightforward and honest, e.g. using data for purposes other than it was given, misleading stakeholders, regulators or others?
    - Objectivity – is there bias in our assessment? Are we under undue pressure to do something?
    - Professional competence and due care – are we acting outside our expertise or knowledge? Is there a risk that we make an error/fail to build in controls or otherwise cause some harm because we are doing something we don't know enough about? E.g. are we taking reasonable steps to protect data?
    - Confidentiality- is there a risk of confidentiality being breached for example in the storage or transmission of data?

    - Professional behaviour – are we in compliance with relevant laws and regulations (e.g. Data Protection Act/General Data Protection Regulations (GDPR))
- Highlight relevant stakeholders – e.g. customers, suppliers, public, regulators
- Suggest options if appropriate

It's particularly important to note that the ethical considerations go beyond what is legally permitted. A baseline for ethical behaviour is that we are aware of and comply with relevant laws and regulations, but we should also be alert for situations where something might be legally permitted, but may not be in line with our ethical principles. Taking examples from above, something that might not be contrary to GDPR might still be unethical if it was a threat to integrity or confidentiality.

References:

CPA Ireland (2019) CPA Syllabus 2020: Information Systems. Available at: https://www.cpaireland.ie/CPAIreland/media/Education-Training/Syllabus%202019/F2-Info-Systems.pdf

CPA Ireland (2019) Code of Ethics for all members. Available at: https://www.cpaireland.ie/CPAIreland/media/Professional-Standards/Technical%20Resources/Ethics/Code-of-Ethics_Effective-23072019.pdf

Further reading:

CGMA (2020) Ethics of New Technology. Available at: https://insights.cgma.org/story/ethics-of-new-technology/

CPA Ireland Ethical Case Studies available at: https://www.cpaireland.ie/Current-Students/Student-Requirements/Professional-Ethics

Dalmia and Shatsky (2020) The rise of data and AI ethics Managing the ethical complexities of the age of big data. Available at: https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html

Drew, Tysiak and Whyte (2018) Ethical Implications of Artificial Intelligence. Available at: https://www.fm-magazine.com/issues/2018/dec/ethical-implications-of-artificial-intelligence.html

IAESB (2018) Information and Communications Technology Literature Review. Available at: https://www.iaesb.org/publications/information-and-communications-technology-literature-review-0

Laudon and Laudon, Management Information Systems: Managing the Digital Firm. Pearson 2018 / ISBN-13: 978-1292211756 15th edition.