

Legal, Social, Ethical and Professional issues

1 Introduction

Relevant legal, social, ethical and professional issues must underpin and guide your practice throughout this project module. This is assessed through engagement with the following learning outcome:

LO10. You should be able to identify and address the legal, social, ethical and professional issues that may arise during the development and use of computing and IT systems.

TMA02 and the EMA explicitly assess the way in which you have addressed LO10, but these issues should also guide your initial choice of project and your project work.

Our goal in this document is to help you anticipate and respond to relevant legal, social, ethical and professional issues that may arise in your project work. This is important because you may be held personally accountable for your actions if they prove injurious in some way to others. This is especially so in respect of your responsibilities towards people or organisations affected by the conduct or outcomes of your project. In addition, it is your responsibility as a member of the Open University community to maintain and enhance the standards and reputation of our University. If you give due consideration to such matters at an early stage of your work, you can avoid any major problems and seek to ameliorate the effects of lesser ones.

It is **not sufficient** to say 'This is only an imaginary project so legal, social, ethical and professional issues don't apply' as they almost certainly do, because very few projects do not potentially impact upon people or wider society. In the unlikely situation where they really do not apply, you still need to discuss the issues explaining *why* they are not relevant.

In your project work you should satisfy the following principles maintained by the OU:

- treat all those associated with your research with respect
- understand and adhere to ethical standards in research as laid down by the University, research councils, Home Office, the National Health Service Central Office for Research Ethics Committees and professional bodies.
- refrain from any research activity that diminishes the reputation of the OU due to its inadequate quality
- ensure validity and accuracy in the collecting and reporting of data
- ensure the safety of all those associated with the research
- ensure that all work presented as your own complies with protocols for acknowledging the contribution of others and acknowledges all source materials.

You should also satisfy the following Ethical Principles for Research Involving Human Participants in Appendix A. You will notice some overlap. However, legal, social, ethical and professional issues apply to all projects, not just those involving human participants.

In addition to considering the reputation of the OU, you should also, of course, consider the reputation of any other person or organisation involved, including your employer if the work involves them in any way.

You are also required to behave in a professional manner. Professionalism in this context is embodied by the BCS Code of Conduct for its members. Please familiarise yourself with this document.

The Autumn 2014 issue of ITNOW, the BCS magazine for IT Professionals, has a special edition on Ethics in IT which you might find helpful and interesting to refer to.

The remainder of this document explains legal, social, ethical and professional issues in more detail finishing with a set of questions to consider both as you choose your project and as you plan and carry out your project work.

2 Working with stakeholders

You are required to behave ethically. Ethical behaviour is 'behaviour that takes account of the legitimate interests of others' (OECD, 2002). The value of this definition is that it focuses attention on three tasks:

- identifying stakeholders (people or organisations) who may be affected in some way by your project
- identifying what their legitimate interests may be
- evaluating those interests and determining whether and how to proceed.

You will find it helpful to carry out these tasks as you choose, plan and carry out your project. It could also contribute to your TMAs and EMA.

Stakeholders

The list of people or organisations affected will include those with direct involvement in the project, either as participants or as project workers themselves, including you, of course. It will also include those affected indirectly, as the outputs of the project are adopted and exploited. These may include users and others who could potentially be disadvantaged by the outputs of your work.

Legitimate interests

The question of what constitutes a 'legitimate interest' is not entirely straightforward. Some interests are established in law; for example, rights under the Data Protection Act 1998 must be considered whenever a project involves recording and storing personal data. Other forms of legitimacy may arise through the existence of 'codes of conduct' adopted by organisations, such as the BCS Code of Conduct for its members.

Legitimacy may also be thought to arise through what might be called 'commonly held values'. Such values might include fairness, equity, equality, and respect for autonomy and dignity.

Many legitimate interests are covered by the notion of 'risk of harm', whether it is material, psychological, or social. Sources of possible harm to project workers and participants may be identified by a risk analysis that complies with health and safety legislation. For participants, there are additional sources of potential harm to consider. If a project involves capturing and storing personal data, especially as defined by the Data Protection Act, then appropriate measures should be used to restrict access to, and the use of, this data. (For help in deciding whether data is personal, see the website of the [UK's Information Commissioner](#):

Some projects may lead to participants discovering or realising something about themselves that they were not aware of previously. This is perhaps especially true of projects in the area of interaction design where, for example, a participant may discover they exhibit a range of conditions. The impact of such knowledge can be significant; a person who discovers, through your research, that they are colour-blind may be employed in work that precludes people with this condition. Participants may also experience social harm – diminution or loss of reputation or 'face'.

Evaluation

Evaluation entails considering the positive and negative impacts of the work on the interests of each individual or organisation. More problematically, it will often involve weighing up the *net* risks and potential impact of the project for each stakeholder, and possibly across all stakeholders. This is a difficult and highly subjective task, especially when performed by any one individual. The difficulty gives rise to the important ethical principle of 'informed consent'. This principle maintains that stakeholders, and especially participants, must be involved in a process leading to a decision to become, and then remain, involved.

3 Working with human participants

In the context of computing, a good test of whether your project involves human participants is to ask yourself whether you are going to collect and process data from, or about, individuals. Collection may be done personally (e.g. through an interview), or impersonally (e.g. via a web questionnaire or any other remote data-recording device).

If you are involving human participants only carry out project work where any reasonable judgment would suggest that no harm could arise to any person, living or dead. In particular you must satisfy the ethical principles listed in Appendix A.

Working with children needs to be approached with particular care. The issue of DBS (Disclosure and Barring Service) checks becomes relevant when working with children. If the research is being done in a friend's home with their children this is not needed, but parents or guardians should still sign consent forms and be present during the study. The child's assent should also be sought and their decision respected if they choose not to take part. Asking intrusive or personal questions is potentially problematic, but asking a willing child to test some software with their parent present is unlikely to cause a problem.

If you want to work with children in a school you will need to ask the permission and advice of the Head Teacher. You should ask for a letter from the Head Teacher agreeing to the research taking place. We suggest you include this in an appendix for TMA02 (if it is available at this point) and also for the EMA. The Head will explain the school's requirements, which may involve you being DBS checked and will almost certainly involve a letter being sent to parents so they have the option of excluding their child from the study. You should ensure you have a teacher or teaching assistant present during the study.

If you are in doubt about these issues, contact your tutor for advice on how to proceed.

4. Asking the right questions

We have divided the following questions into two groups: legal, social or ethical issues, and professional issues. We have done this because the two groups have a different emphasis – the first is about the *project* and the second is about the way *you* should behave. However there is a lot of overlap between the two groups.

These questions relate to several module learning outcomes, so your conclusions should come through in the relevant sections of your TMAs and EMA, as well as when you address LO10 in TMA02 and the EMA.

Legal, social or ethical issues

The following questions will help you reflect upon the impact your project *will* have and the impact it *could* have if developed further and applied to a real world context. You should consider potential issues relating to both the *process* you are going through and the *product* you will be producing.

You will need to tailor the questions to your particular project and some of them may not be applicable. If they are not applicable you should briefly explain why. You may well be able to think of additional relevant questions which are applicable to your particular circumstances.

- What is the *point* of solving this problem? What is the contribution to society? Is any social impact a good or potentially bad thing? How could any bad impacts be avoided?
- Who will use the results of your project and what impact could it have on them and on others?
- Who will be affected when you are solving this problem? (E.g. who will you interview, observe etc). Might their involvement be potentially good or harmful to them (or to the communities/businesses of which they are a member)? How could any harmful impacts be avoided? Might there be any legal issues, perhaps relating to security, confidentiality, health and safety, child protection etc.?

- If your project were to be completed to scale in a real-world context, who would be affected? Might this be potentially good or harmful to these people (or to the communities/businesses of which they are a part)? How could any harmful impacts be avoided? Might there be any legal issues, perhaps relating to security, confidentiality, health and safety, child protection etc.?
- What could happen if the outcome of your project becomes extremely successful/influential? Could it have any impact upon society or the way people work? Would this be a good or potentially bad thing? How could any bad impacts be avoided?
- Could private data be collected? Could this data conceivably be misused in some way? How could this be avoided?
- Could people be tracked? – are there privacy issues? Does this matter? How could this be avoided?
- Could the outcome of your project conceivably be misused in some way, perhaps in conjunction with something else which may not even have been developed yet?
- If you are developing a program and it contains unexpected errors in logic or security holes could this have any bad impacts? What about if it were developed to scale and still contained these?
- Are there legal issues relating to data protection, computer misuse or freedom of information?
- Are there any relevant legal issues not just in the context it is being used now, but if it were to be generalised or re-used in a different context?
- Does your project contribute towards a larger development in technology that leads somewhere you feel may or may not be for the good of society?

Professional issues

You are required to abide by the [BCS Code of Conduct](#) as you complete your project – this is what we mean by being professional. The Code of Conduct governs the behaviour of the *individual* – i.e. you. It might be helpful to think of yourself as a *consultant* working for a client. The client may well be imaginary but you are still expected to behave in a professional manner and behave as though there is one.

Explain any compromises or adjustments you need to make as you carry out your project being honest about the problems you experience and how you address these.

The following questions result from this Code of Conduct. The references in brackets, e.g. (3b), link to the relevant section in the Code. You will need to tailor the questions to your particular project and some of them may not be applicable. If they are not applicable you should briefly explain why. There are many other potential questions relating to the Code. Consider these as well.

- Do you have a conflict of interest (3b)? How will you resolve this conflict? For example, if you were a consultant this might include recommending software you have shares in. This would be a conflict of interest. Also, if you are doing a project based in your workplace, they may have a different timescale and requirements to TM470, which would be a conflict of interest. How will you mitigate these, so you can behave professionally both as an employee and as an OU student?
- Are the project outcomes fit for purpose (4a)? Would they adequately meet the requirements of the client? If not, you need to acknowledge this both in your EMA, and to your client. Being honest is a characteristic of a professional and develops trust.
- Will you use tools and techniques which are appropriate to the context (2c)? For example, using Scratch to develop a safety critical system is unlikely to be the choice of a professional (unless there is an extremely strong justification, such as that you are just developing a rapid prototype for gathering further requirements). Similarly carrying out a survey because you feel confident writing questionnaires, when you need in-depth information about requirements which might be gathered better through interviews and observation is unlikely to be considered professional behaviour.

- Will you be using pirated software or work software you have not been given permission to use? (2d). You must only use software (and other tools) you are entitled to use.
- Do you have the necessary skills (2a and 2b)? We appreciate that you will be learning as you carry out your project work, but you should not make unrealistic claims to your client (or tutor) about your capabilities (this is not good for you either because you will struggle with your project work). So, acknowledge explicitly the limits of your competence. How would other professionals approach your project?
- Will you have adequate resources? Resources include time. Again you should not make unrealistic claims to your client (or tutor) about the available resources.
- How will you take responsibility (3c)? If the project work does not work out as planned, how would you set about completing it after project completion (this is particularly relevant if you have an actual client) or at least producing an acceptable compromise? – you will need a plan for the way forward in your EMA. What are the criteria for success?
- Have you received permission from the client to include data in your TMAs and EMAs (3d)? This would be particularly important if you were working with medical data or for the defence industry but will be true in many situations.

Appendix A Ethical Principles for Research Involving Human Participants.

This appendix presents a summary of The Open University's Ethical Principles for Research Involving Human Participants.

Principle 1: Compliance with protocol

Research with humans conducted by Open University employees and their agents and assignees should comply with an explicit protocol defining how informed consent to participate is sought, gained and recorded, how data is collected, stored and accessed, and how participants are informed of their rights within the study. *The only exception to this requirement shall be where any reasonable judgement would suggest that no harm could possibly arise to any person, living or dead, in connection with the proposed research.*

Formal approval of the protocol shall be gained from the Open University (and, where appropriate, the relevant NHS LREC) before data collection commences.

Please note: In these Principles, the term 'protocol' refers to a filed document which specifies the procedures for recruiting participants and gathering and managing data, with which all research staff agree to comply.

Principle 2: Informed consent

Potential participants should always be informed in advance and in understandable terms of any potential benefits, risks, inconvenience or obligations associated with the research that might reasonably be expected to influence their willingness to participate.

Consent should always be gained in a consistent manner, as specified in the research project's ethical protocol. This should normally involve the use of an information sheet about the research and what participation will involve, and a signed consent form. Sufficient time shall be allowed for a potential participant to consider their decision between the giving of the information sheet and the gaining of consent.

Except in exceptional circumstances, where the nature of the research design requires it, no research shall be conducted without the opt-in informed consent of participants. In the case of children (individuals under 16 years of age) no research shall be conducted without a specified means of gaining their informed consent (or, in the case of young children, their assent) and the consent of their parents or guardians, or persons acting *in loco parentis*.

Where participants are involved in longer-term data collection, the use of procedures for the renewal of consent at appropriate times should be considered.

No inducement to participate should be offered prior to seeking consent, either in the form of payments or of gifts. Reasonable recompense for inconvenience and time contributed to the research and reimbursement of travelling expenses can be offered.

Participants should be informed clearly that they have a right to withdraw their consent at any time, that any data that they have provided will be destroyed if they so request and that there will be no resultant adverse consequences.

Principle 3: Openness and integrity

Researchers should be open and honest about the purpose and content of their research and behave in a professional manner at all times.

Researchers should comply with the University's principles for integrity in the general conduct of research.

Where an essential element of the research design would be compromised by full disclosure to participants, the withholding of information should be specified in the project protocol and explicit procedures stated to obviate any potential harm arising from such withholding.

Deception or covert collection of data should only take place where it is essential to achieve the research results required, where the research objective has strong scientific merit and where there is an appropriate risk management and harm alleviation strategy.

Participants should be given opportunities to access the outcomes of research in which they have participated and debriefed if appropriate after they have provided data.

Principle 4: Protection from harm

Researchers must make every effort to minimise the risks of any harm, either physical or psychological, arising for any participant, researcher, institution, funding body or other person.

Every project should carry out a risk analysis and, where significant risks are identified, should specify a risk management and harm alleviation strategy in the protocol.

Researchers shall comply with the requirements of the UK Data Protection Act 1998, the Freedom of Information Act 2000 and any other relevant legal frameworks governing the management of personal information in the UK or in any other country where the research may be conducted.

Where research involves children or other vulnerable groups, an appropriate level of disclosure should be obtained from the Criminal Records Bureau for all researchers in contact with participants.

Where harm does nevertheless arise in the course of research, researchers should take remedial steps.

Participants should be given information as to whom they may contact in the event of any issues arising in the course of the research that cannot be resolved with members of the project team.

Principle 5: Confidentiality

Except where explicit written consent is given, researchers should respect and preserve the confidentiality of participants' identities and data at all times. The procedures by which this is to be achieved should be specified in the protocol.

Please note: The duty of confidentiality is not absolute in law and may in exceptional circumstances be overridden by more compelling duties such as the duty to protect individuals from harm. Where a significant risk of such issues arising is identified in the risk assessment, specific procedures to be followed should be specified in the protocol.

Principle 6: Professional codes of practice and ethics

Where the subject of a research project falls within the domain of a professional body with a published code of practice and ethical guidelines, researchers should explicitly state their intention to comply with the code and guidelines in the project protocol.

Research within the UK NHS should always be conducted in compliance with an ethical protocol approved by the appropriate NHS Research Ethics Committee.

Human Participants and Materials Ethics Committee (HPMEC)

The Open University

March 2006

References

Organisation for Economic Co-operation and Development (2002) *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD Council Recommendation, 1037th Session, 25 July.