Sheffield Hallam University

GUIDELINES ON ETHICAL ASPECTS OF RESEARCH USING INFORMATION AND COMMUNICATION TECHNOLOGY

Contents

1. General

1.1 The professional codes of conduct of both the British Computer Society (UK) and the Association for Computing Machinery (USA) urge consideration of the human consequences of computer systems, supporting, therefore, the ‘Helsinki principle’ of beneficence in research. Computer technology can provide a valuable vehicle for research in many fields and is also a rich area for research in its own right. However, as with any science or technology, care should be taken with the unintended possibility for negative consequences alongside the desire of the researcher to do good.

1.2 The normal University regulations give a good basis for proper and ethical uses of the University’s Information Technology facilities. However, these should be regarded as a ‘floor’ rather than as a ‘ceiling’ for ethical research activity using Information and Communication Technology (ICT).

1.3 The provisions of the Data Protection Act and the Misuse of Computers Act are relevant and not overridden by University regulations.

1.4 In addition, where computer systems are used in research applied to fields such as pharmaceutical studies, then the normal rules applying to such studies (such as those of SHU, RSS) must be observed.

1.5 Students carrying out research have a responsibility to be alert to ethical aspects of their work, and to liaise with their research supervisors over this dimension.

2. Research Using Non-University Facilities

Where the research employs ICT apart from university facilities, then authorisation from the responsible manager or system administrator of these facilities must be obtained.

3. Computer Viruses

3.1 Computer viruses often have unforeseen side effects such as consuming large amounts of system resource, and accidental infection is always a strong possibility. Thus the best (and simplest) approach is to rule out all practical experiments with computer viruses.

3.2 Dissemination of the results of paper based (theoretical) computer virus experiments is a sensitive issue, and must be cleared with the research supervisor.

4. Computer Security

4.1 Attempts to make unauthorised access to telephone systems, computer networks, databases and other forms of ICT are illegal and unethical, regardless of motivation.

4.2 Should a previously undiscovered security weakness be identified, dissemination of this knowledge would have to be treated with caution. In the first instance the research supervisor should be informed of the discovery.

4.3 Practical experiments to breach security should be carried out on designated, ‘standalone’ computers or on designated isolated networks of computers. These experiments should be explicitly authorised by the research supervisor.

4.4 Experiments concerning sensitive aspects of security such as: ‘Identity Theft’; cryptography; use of ICT in terrorism; attempts to bypass payment mechanisms or ‘steal’ resources; these must be cleared with the research supervisor. The University may place safeguards or restrictions upon such work.

5. Intellectual Property Rights

Research that might generate copyright issues, for example involving peer-to-peer networking, or file sharing and distribution, must be cleared through the research supervisor, who may need to take further advice.

6. Identity Hiding

6.1 ICT readily provides the ability to hide or disguise one's identity when communicating with others electronically. This contravenes the usual 'Helsinki' principle concerning openness about the nature and purpose of the research, and should not be done.

6.2 Electronically concealing one's true identity is intrinsically dishonest and can have consequences that can offend or disturb people on whom this impinges.

7. Unsolicited email

7.1 Email can be used as a research tool, typically when conducting surveys. Use of email beyond routine research communication must be cleared with the research supervisor to avoid nuisance to recipients or unduly large demands on system resources.

7.2 Wherever possible a URL should be supplied instead of attachments (which are inevitably larger). This is also a good practice as it promotes transparency monitoring of any web pages that are employed as part of the research.

7.3 Where attachments to email are unavoidable, it is the research student's responsibility to ensure that they do not contain viruses. (The use of Rich Text Format documents as attachments defeats the possibility of 'macro viruses' as well as being smaller than full-scale word processor files). Computer viruses can also be present in spreadsheet, image, and 'PowerPoint' files.

8. On-Line Surveys

Web technologies such as bulletin boards and 'chat rooms' may be utilised in the collection of data in surveys and qualitative research.

Where minors could become the subjects of such on-line research, the provisions of the US Children's Online Privacy Protection Act (COPPA) should provide a baseline. Essentially COPPA enforces positive parental authorisation for on-line divulgence of information by children aged under thirteen years. Several technical means for collecting such authorisation are suggested by the Act.

9. Privacy

Research using ICT that invades the privacy of others (e.g. by monitoring and surveillance) is unethical.

10. Virtual Reality

Some VR environments can give rise to disorientation and nausea in human subjects immersed in them. The subject must be briefed to report any discomfort, and should be monitored periodically for such, in VR research.

11. Differently Abled Subjects

Established ‘good practice’ in human-computer interface design should be followed. Care should be taken not to exclude or disadvantage a research participant where ICT is employed. (For instance, typically 10% of most male populations show non-standard colour vision, and thus have difficulty reading certain visual displays).

12. Experimental Results

Researchers in any discipline must ensure the transparency of data, results, and other material obtained or processed via the use of ICT in order that their legitimacy and correctness may be verified.

13. Approved Variations from Normal Regulations

It may be that research requires the use of ICT to access (by viewing or downloading) information sources that are normally barred by the University’s policy on the use of its ICT resources as offensive, inappropriate or illegal. (An example might be the legitimate need to visit certain Web sites during a study of ‘sex tourism’). Such departures from normal policy must be cleared through the research supervisor, who will liaise with CIS in such cases.

University IT regulations Section 5 (Misuse) require prior approval here.

Author: Andrew Bissett, Faculty of Arts, Computing, Engineering and Sciences