Published on *Jisc community* (https://community.jisc.ac.uk)

Computers and the Law

PB/INFO/005

Please note that this factsheet is written with no legal expertise and that no-one should take any action based solely on its content. In particular, readers outside England and Wales may be subject to different legal systems.

Most people who work with computers will have at least heard of the *Computer Misuse Act* and the *Data Protection Act*: from their titles alone it is clear that these apply to computers. However there are a number of other, less obvious, Acts of Parliament (see below) which may well apply to you, especially if you are involved in operating or managing computer systems or networks. While none of them can be recommended as light reading, it is worth having some idea of how they may affect you.

Of course there are also a very large number of 'real world' crimes that can be committed with the assistance of a computer. These range from defamation and violation of copyright through blackmail and harassment to pornography. Contrary to popular opinion the Internet is not 'lawless' and the fact that an offence is committed through electronic means does not make it any less of an offence, nor is it likely to mitigate the punishment.

Public Acts of Parliament are now available online at www.legislation.gov.uk [1]

Definitive copies of all Acts can be purchased as paper documents from the Office of Public Sector Information (formerly HMSO) or their agents, and may also be available in libraries.

The Joint Information Services Committee (JISC) funds a service providing information on the legal implications of Information Technology [2]

We recommend that organisations should establish contact with their local police force before they have problems. Such relationships can be highly beneficial to both sides. All police forces now have designated officers who specialise in computer crime. If you do not know who to talk to in your area, Janet CSIRT (Computer Security Incident Response Team) has contacts in several forces and may therefore be able to help: irt@csirt.ja.net [3]

Regulation of Investigatory Powers Act 2000 [4]

This Act defines rules for interception of traffic on all postal and telecommunications networks. It applies to all users and operators of networks, whether local or wide area, and to any action which may cause the content of a message to become known to people other than the sender and recipient. The Act and its supporting regulations only authorise certain groups to examine

traffic on networks and restrict the purposes for which monitoring and recording can be used.

Monitoring for business purposes, such as ensuring compliance with acceptable use policies, is only permitted after users have been informed. This is the subject of a separate statutory instrument [5] (S.I. 2000 No. 2699)

The Act also gives powers to the police and other authorities to require disclosure of information that organisations keep about the use of their computers and networks. More details are available in the Janet Guidance Note on Logfiles [6]

The Information Commissioner's Employment Practices Codes [7] advise how to comply with the Regulation of Investigatory Powers and Data Protection Acts. The Codes are available from the Commissioner's website.

Malicious Communications Act 1988 [8]

This Act makes it an offence in England and Wales to send a message intending to cause distress or anxiety, whether this takes the form of threat, offensive material or false statements. The offence would be dealt with in Scotland as a breach of the peace and in Northern Ireland by a separate order. Such messages will also contravene the Acceptable Use Policies of most computer networks, including Janet.

Computer Misuse Act 1990 [9]

This Act deals with unauthorised access to, or modification of, computer material. Its scope is remarkably wide, including almost any attempt to modify or impair the function or reliability of any computer, program or data without authority to do so. The offender must be aware at the time that their action is unauthorised; for this reason it is recommended that login and other banners be displayed wherever possible.

Sections 35 to 38 of the Police and Justice Act 2006 [10] amend the *Computer Misuse Act 1990* to cover denial of service attacks as well as the creation, supply and obtaining of tools for committing offences. Guidance on these new offences is available from the Crown Prosecution Service [11].

Data Protection Act 1998 [12]

This Act, and related European Union legislation, controls the collection, processing, use and disclosure of information about identifiable individuals. The Act covers information held in both electronic and paper form. Information about the Act and advice on complying with it are available from the Office of the Information Commissioner [13]

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/computers-and-law

Links
[1] http://www.legislation.gov.uk
[2] http://www.jisclegal.ac.uk/

[3] mailto:irt@csirt.ja.net
[4] http://www.legislation.gov.uk/ukpga/2000/23/contents
[5] http://www.legislation.gov.uk/uksi/2000/2699/contents/made
[6] https://community.ja.net/library/janet-services-documentation/logfiles-technical-guide
[7] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx
[8] http://www.legislation.gov.uk/ukpga/1988/27/contents
[9] http://www.legislation.gov.uk/ukpga/1990/18/contents
[10] http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse
[11] http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/
[12] http://www.legislation.gov.uk/ukpga/1998/29/contents
[13] http://www.ico.gov.uk/