

Cybercrime Overview

1 February 2007

Please note: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

Table of Contents

1. Introduction.....	1
2. Computer Misuse Act 1990	2
3. Other Legislation.....	4
3.1 Pornography	4
3.2 Online Sexual Grooming	6
3.3 Extreme Material.....	6
3.4 Incitement to Racial and Religious Hatred.....	6
3.5 Online Harassment.....	7
3.6 Intellectual Property Offences - Copyright Crime	8
3.7 Online Defamation	9
3.8 Terrorism	9
4. Responsibilities of Institutions	10
5. Conclusion.....	11

1. Introduction

FE and HE institutions are affected by computer crime in many of the same ways as other businesses, organisations and individuals. High up the list of concerns for FE and HE institutions are hacking, fraud and theft, copyright abuse, obscene content (including child pornography) and harassment. Many of these crimes are prosecuted within the existing criminal justice structures just as they are when the offence is committed where no computer is involved. In addition some are classified as crimes under the Computer Misuse Act 1990.

Computer crime may be classified into the following categories:

- Content related crime, for example, child pornography and criminal copyright infringement.
- Traditional crimes committed by means of a computer, for example, harassment, fraud and theft.
- Attacks on computers and computer systems, for example, hacking.

These crimes can also be referred to as cybercrime, e-crime or hi-tech crime.

This overview paper explores the main obligations imposed on institutions concerning the provision and use of IT facilities in terms of cybercrime.

Institutions have a legal duty in terms of Health and Safety legislation to protect staff, students and others from any reasonably foreseeable harm as well as a common law duty of care towards staff, students and others. Further details of the “Duty of Care in the Further and Higher Education Sectors” can be found in the JISC Legal paper online at - <http://www.jisclegal.ac.uk/publications/Dutyofcare.htm>.

2. Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) (and now amended by the Police And Justice Act 2006) was introduced primarily to deal with computer hacking. It contains three main offences to do with unauthorised acts relating to computers:

- Section 1 contains the basic ‘hacking’ offence of gaining unauthorised access to any program or data held in a computer.
- Section 2 makes it an offence to commit a Section 1 offence with a view to commit, or facilitate the commission of, a further offence.
- Section 3 contains the offence of doing any unauthorised act in relation to a computer with intent:
 - to impair the operation of any computer; or
 - to prevent or hinder access to any program or data held in any computer; or
 - to impair the operation of any such program or the reliability of such data;
 - to enable any of the things to be done.

knowing that any modification intended to be caused is unauthorised.

Maximum sentences for these offences range from six months imprisonment and/or a £500 fine to ten years imprisonment and/or an unlimited fine.

Hacking

In terms of external threats FE and HE institutions must adopt technology security appropriate to the current risk level. From an infrastructure perspective this involves well established practice:

- build it secure
- educate users to operate it securely
- and encourage high risk users to invest in matching preventative measures where appropriate

Virtually all hacking activities are offences under the CMA including accessing a computer where this is unauthorised. ‘Hacking’ is a term which was originally used to describe the activities of computer enthusiasts who pitted their skills against the IT systems of governments and big businesses. A variety of motives lie behind hacking attacks and not all hackers pose the same threat. For institutions hacking can cause

serious financial disruption (e.g. through system downtime) and any consequent security breach may expose individual users to further crime.

The Police And Justice Act 2006 expands the CMA provisions on unauthorised modification of computer material to criminalise someone who knowingly does an unauthorised act in relation to a computer with intent:

- to impair the operation of any computer,
- to prevent or hinder access to any program or data held in any computer, or
- to impair the operation of any program or data held in any computer.

The intent need not be directed at any particular computer or any particular program or data.

The UCISA Information Security Toolkit is intended to support UK Further and Higher Education Institutions in producing Information Security policies to address (and to demonstrate that they are addressing) threats to the confidentiality, integrity and availability of information systems for which they are responsible, and to help meet audit requirements. Details of the Toolkit can be found on the UCISA website at - <http://www.ucisa.ac.uk/ist>.

Fraud and Theft

Computer-related fraud can involve:

- altering computer input in an unauthorised way;
- destroying, suppressing, or stealing output;
- making unapproved changes to stored information; or
- amending or misusing programs (excluding virus infections).

In addition to being a crime in terms of existing criminal legislation, such activity is likely to involve "unauthorised access" or "unauthorised modification" as laid out in the CMA 1990 (see above).

Card-Not-Present Fraud

In 2004, card fraud over the Internet cost the UK £117m (Source: Association for Payment Clearing Services – <http://www.apacs.org.uk/>).

This crime usually entails fraudulently obtaining credit or other card details to make a purchase. The vast majority of this type of fraud involves the use of card details that have been dishonestly obtained through methods such as skimming or bin-raiding. The card details are then used to make fraudulent card-not-present transactions, often via the internet. The incidence of computer hackers actually stealing and using cardholder data from organisations computer networks or websites is thought to be very low. However FE and HE institutions staff and student are increasingly vulnerable to these types of card-not-present crimes as more and more payment transactions take place online.

Denial of Service attacks

Usually directed at the institution 'Denial of Service' (DoS) is the name given to attacks involving hackers preventing the normal flow of internet traffic to websites of a college or university. Denial of Service attacks, where hackers overload networks with data in an effort to disable them, have risen 50%, a security report says - <http://news.bbc.co.uk/1/hi/technology/4787474.stm>.

The Police And Justice Act 2006 now makes it an offence to launch a denial of service attack in the UK, punishable by up to ten years in prison. See further details on the OUT-LAW website at - UK bans denial of service attacks - <http://www.out-law.com/page-7462>.

Assistance with handling 'Denial of Service' attacks can be found in 'Guidance Note' on 'Investigating a denial-of-service attack' on the UKERNA JANET website at - <http://www.ja.net/services/publications/technical-guides/index.html>.

3. Other Legislation

3.1 Pornography

The Obscene Publications Act 1959 & 1964 makes it illegal to publish material that tends to deprave and corrupt those viewing it. It is the activities being depicted which are the roots of the obscenity.

The historical focus of UK legislation has been on criminalising distribution of 'obscene' material rather than mere possession in private. However under the 1964 Act it is an offence to possess obscene material with an intention to publish for gain. So strictly, no attempt to publish is required for the crime to have been committed.

All of this then applies equally to the electronic world. The test for what is 'obscene' is set out in the Obscene Publications Acts 1959 and 1964 in s.1(1), and is defined as material which tends to 'deprave and corrupt' those who are likely, having regard to all relevant circumstances, to read, see or hear it. Further, storage and transmission of material which is considered obscene is a criminal offence under s.2(1).

Highly sensitive issues relating to online pornography tend to involve the viewing, possession, making and distribution of indecent images of children or serious stalking or harassment facilitated by communication technologies. Thus, the discovery of obscene materials on an FE or HE institution's computer is likely to be a serious criminal offence. Staff and students may be perpetrators, abettors or even victims of such cybercrime. Although it is the offenders, as individuals, that would face criminal prosecution an institution could suffer reputational damage if it is not seen to be acting responsibly.

Only if an institution's senior office holders knowingly permit the publishing or storage of illegal obscene materials will they be likely to face criminal prosecution.

There may be rare occasions where, for the purposes of research, obscene materials will be stored on computers. Usually institutions will have policies and practices in place to handle such research content. Only with prior approval and under strict senior management supervision should such content be tolerated. It is suggested that if illegal obscene materials are to be retained by an institution for the purposes of academic research then liaison with senior police authorities should take place.

3.1.1 Child pornography

Child pornography is pornography which features the sexual abuse of children. What draws this particular criminalisation is indecency with children i.e. the fact that a young person is involved.

The law's approach to child pornography is that it is so offensive that possession as well as circulation of offending images is criminalised. The primary legislation consists of the Protection of Children Act 1978 (PCA) (which does not apply to Scotland or Northern Ireland) and the Criminal Justice Act 1988 (CJA) 1988. It is an offence to possess indecent images involving children (or convincing depictions thereof). 'Indecent' here means 'sexually explicit' which is a more straightforward test than tending to 'deprave and corrupt'. By virtue of s.160 of the CJA possession of such material is an offence and has a maximum five year penalty. Offences of taking, making and distribution are covered under the PCA and carry a maximum ten year penalty.

Section 45 of the Sexual Offences Act 2003 amends the definition of 'child' - raising the relevant age from under 16 to under 18 years.

Offences are also created by s.2, of the Obscene Publications Act 1959. It is an offence to publish an 'obscene' article whether for gain or not; and this is further extended in the Criminal Justice Public Order Act 1994, ss.84-87 which deals specifically with 'Obscene publications and indecent photographs of children'. There is a defence provided which relates to possession without sufficient knowledge of the material or its nature.

In Scotland, the Civic Government (Scotland) Act 1982 makes it an offence to publish obscene material. Prosecution is the responsibility of the Procurator Fiscal Service (s.52A Possession of indecent photographs of children). The Prevention of Sexual Offences (Scotland) Act 2005 extends these offences to apply to images of children under 18 years.

The Obscene Publications Act 1959 does not extend to Northern Ireland. Obscene material is generally dealt with under the common law offence of publishing an obscene libel.

As well as the negative publicity such an incident will attract to an institution will be the disruption as computers are likely to be confiscated as evidence.

Details of the UK's largest ever police hunt against internet paedophiles - Operation Ore can be read in the 'Guardian report on Operation Ore' online at - http://www.guardian.co.uk/uk_news/story/0,3604,1192073,00.html.

As above if an institution's senior office holders knowingly permit the publishing or storage of illegal child pornography materials they will they be likely to face criminal prosecution.

3.2 Online Sexual Grooming

The Sexual Offences Act 2003 came into force on 1 May 2004 and created an offence of meeting a child following sexual grooming. The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 delivers similar provisions for Scotland. It is now a crime to befriend a child on the internet or by other means and to meet or intend to meet the child with the intention of abusing them. The maximum sentence is 10 years imprisonment. A new civil preventative order, the 'Risk of Sexual harm Order', may be imposed which will prohibit adults from engaging in inappropriate behaviour such as sexual conversations with children online. Any knowledge by an institution of such activity must be reported to the police right away.

3.3 Extreme Material

A proposal to make illegal the possession of a limited range of extreme pornographic material featuring adults is currently being considered by the Home Office. The proposal is to create a new offence of simple possession of pornographic material which is graphic and sexually explicit and which contains actual scenes or realistic depictions of serious violence, bestiality or necrophilia. For further information on this proposal you can access the document "Consultation: On the possession of extreme pornographic material" – online at - news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf.

3.4 Incitement to Racial and Religious Hatred

The problem of illegal, harmful, distasteful or offensive content on FE or HE computer systems or the internet is of course not restricted to pornography.

Internet content exists which contravenes the rules enacted to prevent the making of anti-religious statements (the law of blasphemy), the making of racist or inflammatory statements (incitement to racial hatred or "hate speech" rules - Race Relations Act 1976) and the making of politically subversive or seditious statements.

Incitement to racial hatred is governed by section 21 of the Public Order Act 1986 which states that it is an offence for a person to publish or distribute material which is threatening or abusive or insulting if:

- it is intended thereby to stir up racial hatred, or
- having regard to all the circumstances, racial hatred is likely to be stirred thereby.

The Racial and Religious Hatred Act 2006 gained Royal Assent on 16 February 2006. The Act makes it illegal to threaten people because of their religion, or to stir up hatred against a person because of their faith. It is designed to fill gaps in the

current laws, which makes it illegal to threaten people on the basis of race or ethnic background. This Act extends to England and Wales only.

The Crime and Disorder Act 1998 created new racially aggravated harassment and public order offences and came into force on 30 September 1998. For each of these new offences, the maximum penalty is higher than the maximum for the basic offence without the element of racial aggravation.

What is involved is that either at the time of committing the offence, or immediately before or after doing so, the offender demonstrates towards the victim hostility based on the victim's membership (or presumed membership) of a racial group. Or where the offence is motivated (wholly or partly) by hostility towards members of a racial group based on their membership of that group.

Inciting either racial or religious hatred is therefore a criminal offence. Publishing and disseminating online materials that are likely to incite such hatred is also a criminal offence. Such incidents should be reported to the police.

As corporate entities FE and HE institutions have a responsibility not to publish and disseminate racist materials in any format including electronically. As well as the likely reputational damage, as public authorities, FE and HE institutions have a general statutory duty under The Race Relations Act 1976 (as amended), in carrying out their functions, to consider the need to eliminate unlawful discrimination and to promote equality of opportunity and good relations between people of different racial groups.

3.5 Online Harassment

Harassment by email or online is a serious concern for many people. The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which that person knows, or ought to know, amounts to harassment of another. This includes by email or by other computer related means such as discussion forums, for example. FE and HE institutions must ensure that information technology facilities are not used in such a way.

In England and Wales under s.1 of the Malicious Communications Act 1988 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under s.43 Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent offensive or threatening. Both offences are punishable with up to six months imprisonment and/or a fine. Because the Malicious Communications Offence is wider ranging than the Telecommunications offence it is more likely to be charged by the Police than is the Telecommunications Act offence.

Cases of online intimidation and harassment offence in Scotland are likely to be dealt with as a breach of the peace. Such activity is also likely to contravene the Acceptable Use Policies of most computer networks, including JANET - <http://www.ja.net/services/publications/policy/aup.html>.

There has to be zero tolerance of such harassment and FE and HE institutions are advised to have clear incident handling procedures in place which come into operation when incidents arise.

As employers FE and HE institutions need to take action to prevent harassment, encourage incidents to be reported, respond promptly and ensure policies are followed correctly. Legally, they have a common law duty of care, and responsibilities under health and safety and discrimination legislation.

Further information on the responsibilities owed to students and staff can be found in the paper entitled "Legal Risks and Liabilities for IT Services in Further and Higher Education" by Christine Cooper on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/legalRisks.htm>. Also the duty of care owed to students aged 16-18 is examined in the paper "Duty of Care in the Further and Higher Education Sectors" on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/Dutyofcare.htm>.

3.6 Intellectual Property Offences - Copyright Crime

Copyright law provides for criminal sanction in certain situations. In the UK generally civil remedies provide compensation to wronged intellectual property rights holders and most of the copyright criminal offences, contained in s.107 of the Copyright, Designs and Patents Act 1998 (CDPA), are concerned with commercial activity.

Sections 107, 110 and 198 create criminal offences in relation to the making, distribution, importation, sale or hire of 'infringing copies'.

Specifically, one of the offences covers the act of 'distributing an article otherwise than in the course of business to such an extent as to affect prejudicially the owner of the copyright'. In addition, encouraging the copying of software for sale online could lead to the criminal offence of incitement.

According to s.107 CDPA a criminal offence is committed if a person knowingly sells an infringing copy of a protected work without the permission of the copyright owner. In the UK, criminal penalties for companies and their directors can include unlimited fines and up to two years in prison.

Section 107 has also been amended to create a criminal offence (as well as a civil offence) where a person knowingly infringes copyright in a work by communicating the work to the public in the course of business, or in a way that prejudicially affects the copyright owner.

Further information on intellectual property crime, including counterfeiting and piracy, can be found on the Patent Office website at - <http://www.patent.gov.uk/crime.htm>.

Sharing Music

Music or other file-sharing can be unlawful under the CDPA and students or staff who trade, swap or share music files illegally over the internet open themselves up to the possibility of a civil legal action.

FE and HE institutions are vulnerable to the extent that office holders and those responsible for compliance must not knowingly facilitate the commercial abuse of copyright law.

3.7 Online Defamation

Words are defamatory if they tend to reduce the reputation of an individual in the minds of 'right-thinking members of society'. Although strictly not criminal law, a recent case illustrates the significance of online defamation and libel in an institutional environment. The High Court awarded £10,000 in damages, and over £7,000 in costs against a college lecturer who was found to have committed libel through her postings to an internet message board. Details of the news story can be found on the Guardian Unlimited website at - <http://www.guardian.co.uk/law/story/0,,1737445,00.html>.

FE and HE institutions providing discussion forums, blogs and other similar facilities, should remind participants that the law of defamation applies in the online world. Also, they should ensure that they have well-known take-down procedures in the event of complaints in order to minimise the risk of liability as publisher. However routine monitoring of all information on an institution's systems should be avoided as this is likely to result in the institution being classified as an editor of the material and therefore subject to strict liability for defamation rather than the more lenient, notice-based standard that a distributor is held to in relation to third party provided material. For further information on potential liability in this area please see the separate JISC Legal Overview paper on Internet Service Providers Liability available from the JISC Legal website publications page online at - <http://www.jisclegal.ac.uk/publicationspage.htm>.

3.8 Terrorism

The Terrorism Act 2006 contains a comprehensive package of measures designed to ensure that the police, intelligence agencies and courts have the tools they require to tackle terrorism and bring perpetrators to justice. Although not specifically information technology related, new criminal offences have been created including:

- Acts Preparatory to Terrorism
- Encouragement to Terrorism
- Dissemination of Terrorist Publications
- Terrorist training offences

It is likely that many of these crimes may well be committed or facilitated by computer use and FE and HE institutions should play their part in ensuring that such crimes are not committed or facilitated on their computer systems. Reporting suspicious activity to the police is essential.

Universities and colleges are being urged by the UK government to take seriously the problem of extremism on their campuses. Practical guidance has been issued which points out universities and colleges responsibilities within the law and clarifies the legal position. You can find further details of the guidance (which is particular to

England only) on the Department for Education and Skills website at - http://www.dfes.gov.uk/pns/DisplayPN.cgi?pn_id=2006_0170.

4. Responsibilities of Institutions

Opinions vary on whether uncontrolled internet access from within an organisation represents a significant legal and security risk and to what degree an institution has a legal obligation to protect its staff and students and computer systems from exposure to illegal and inappropriate electronic communications.

In the UK, the Health & Safety at Work etc Act 1974 requires employers to secure the health (including mental health), safety and welfare of employees whilst at work and, amongst other things, provide a safe place of work; ensure safe systems of work and provide information and training. The Act also requires employees to take reasonable care of their own health and safety and that of others and to co-operate with the employer in discharging their duties under the Act.

The extent of the duty of care owed to employees and students is explained in detail in the paper "Duty of Care in the Further and Higher Education Sectors" on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/Dutyofcare.htm>.

Data Retention – Collecting Evidence

There is increasing expectation that institutions will have robust tracking systems which are able to provide detailed evidence of user activity which will stand up to the closest scrutiny. Being able to determine who was responsible for an action is of particular value when crime has occurred and computers have been misused. This misuse may be at a technical level, preventing computer networks from operating correctly, or it may be actual criminal, civil or social abuse.

It is impossible to prevent all misuse, so it must be possible to identify the users whose misuse is a problem, after the fact, so that appropriate action can be taken. Of course, the ability to trace actions back to their source will, in itself, discourage illegal activity.

A 'Good Practice Guide for Computer Based Electronic Evidence' produced by the Association of Chief Police Officers (ACPO) is available online at - http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

Further details of an institution's responsibilities concerning 'Retention of Communications Data' is available in the JISC Legal 'E-Security Overview' paper online at - <http://www.jisclegal.ac.uk/publicationspage.htm>.

5. Conclusion

- Crime on institutions computer systems is wasteful and risks reputational damage.
- As well as traditional crimes being committed by means of computers, the computers and computer systems themselves can be the target of crime.
- In terms of external threats FE and HE institutions must adopt technology security appropriate to the current risk level. Many virus attacks, spam and hacking incidents are directed at the information technology applications themselves. Usually these are most effectively confronted and redressed by technology security matters requiring ongoing sophisticated up to date infrastructure protection systems.
- The day of the vulnerable and naive user of email and the internet should be long gone. However there remains an obligation on an institution to protect and safeguard its users including students, staff and others.
- Many difficulties originating from within an institution can be confronted and avoided by ensuring that students and staff users adhere to strict conditions of use of IT facilities. It is, for example, the responsibility of each FE and HE institution to foster a culture of computer use which complies with the JANET 'Acceptable Use' guidelines.
- Institutions have a right and sometimes a duty to make sure that their computer systems are not being used for illegal purposes. Clearly preventing pornographic images of minors on computer systems is one such responsibility. From a legal standpoint this duty is optimally fulfilled by notice and take-down procedures rather than actively monitoring in general which is likely to draw increased liability upon the institution.
- At the operations level, what is 'acceptable use' should be strictly enforced and a culture of legal use predominant. Even with all the policies and technological solutions in place, there may still be occasions when misuse by individuals of information technology and the internet occur.
- In addition to crime prevention FE and HE institutions are advised to have clear incident handling procedures in place which come into operation when serious crime related incidents arise.

John X Kelly
1 February 2007

Sources used in the compilation of this Overview include:

- The UK E-crime Strategy - <http://www.crimereduction.gov.uk/internet02.htm>
- Guardian Unlimited - <http://www.guardian.co.uk/>
- OUT-LAW - <http://www.out-law.com/>
- JISC Legal E-Security Overview - <http://www.jisclegal.ac.uk/eseconomy/eseconomy.htm>
- 'Inappropriate Use of Computers - the Technical Investigation Process' JISC Legal - <http://www.jisclegal.ac.uk/publications/Inappropriateuse.htm>
- Harassment Law in the UK - Information by Barrister Neil Addison at: <http://www.harassment-law.co.uk/>
- Effective Incident Response - Guidance Notes - UKERNA JANET - <http://www.ja.net/services/publications/technical-guides/index.html>
- Security Factsheets - UKERNA JANET - <http://www.ja.net/services/publications/factsheets/index.html>
- JANET Acceptable Use guidelines - UKERNA JANET - <http://www.ja.net/services/publications/policy/aup.html>
- Dealing with Computer Crime - UKERNA JANET - <http://www.ja.net/services/publications/factsheets/index.html>
- Internet Safety - Becta (British Educational Communications and Technology Agency) - <http://www.becta.org.uk/>
- Racially Aggravated Offences - The Crown Prosecution Service <http://www.cps.gov.uk/publications/communications/fs-racially.html>
- The BBC guide to the terms and buzzwords of hi-tech crime - <http://news.bbc.co.uk/1/hi/uk/5400052.stm>
- Association of Chief Police Officers (ACPO) - Good Practice Guide for Computer Based Electronic Evidence - http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

UK Legislation

- The Computer Misuse Act 1990 (CMA) - http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
- Police and Justice Act 2006 - <http://www.opsi.gov.uk/acts/acts2006/20060048.htm>
- Criminal Justice Act 1988 - http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880033_en_1.htm
- Criminal Justice and Public Order Act 1994 - http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm
- Sexual Offences Act 2003 - <http://www.opsi.gov.uk/ACTS/acts2003/20030042.htm>
- The Prevention of Sexual Offences (Scotland) Act 2005 - <http://www.opsi.gov.uk/legislation/scotland/acts2005/20050009.htm>
- Protection from Harassment Act 1997 - <http://www.opsi.gov.uk/acts/acts1997/1997040.htm>
- Crime and Disorder Act 1998 - <http://www.opsi.gov.uk/acts/acts1998/19980037.htm>

- Malicious Communications Act 1988 -
http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm
- Copyright, Designs and Patents Act 1998 -
http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm
- The Terrorism Act 2006 –
<http://www.opsi.gov.uk/acts/acts2006/20060011.htm>

John X Kelly

1 February 2007

© JISC Legal - www.jisclegal.ac.uk