**Computer Related Legislation**

Version: 1.0
Date: 24/05/2018

## Introduction:

All institutions need to ensure that IT facilities (both corporate and local systems) are provided in accordance with relevant legislation and that users are aware of their legal obligations.

Below are details of some of the Acts of Parliament which govern the storage, use, transmission and collection of computer data. Any non IT related legislature also applies. Employees and students need to be aware of, and adhere to, the contents of this, and related documentation.

## 1. Computer Misuse Act

The Computer Misuse Act (1990) was introduced to secure computer material against unauthorised access or modification. Three categories of criminal offences were established to cover the following conduct:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer.
   Penalty: up to six months of imprisonment or up to a £5,000 fine.
2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking.
   Penalty: up to five years of imprisonment and an unlimited fine.
3. Unauthorised modification of computer material, which includes:
   i. intentional and unauthorised destruction of software or data;
   ii. the circulation of 'infected' materials on-line;
   iii. an unauthorised addition of a password to a data file.

   **Penalty:** up to five years of imprisonment and an unlimited fine.

**You must not:**

- display any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate unauthorised access);
- display any information which may lead to any unauthorised modification of computer materials (such modification would include activities such as the circulation of 'infected' software or the unauthorised use of a password);
- display any material which may incite or encourage others to carry out unauthorised access to or modification of computer materials.

## 2. Copyright

The Copyright, Design and Patents Act (1988) is applicable to all types of creations, including text, graphics and sounds by an author or an artist. This includes any which are accessible through the University's IT facilities. Any unloading, downloading or printing of information through on-line technologies, which is not authorised by the copyright owner will be deemed to be an infringement of his/her rights.

The application of the Copyright Act to electronic copying is even stricter than its application to photocopying, since the fair dealing arrangements which usually apply to libraries (i.e. one article per journal for the purposes of research or private study) do not exist for computerised materials.

Some types of infringement give rise to criminal offences, the penalties for which are up to two years imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by injunction.

**You must not:**

- make, transmit, print or store an electronic copy of copyright material on the University's IT equipment without the permission of the owner.

## 3. Data Protection

The Data Protection Act (1998) concerns the processing of information about living individuals. It gives rights to those individuals about whom information is recorded and demands good practice in handling information about people.

Every person or organisation holding personal data (data controller) must be registered with the Information Commissioner. The University of Greenwich is registered as a data controller. Any use of personal data beyond the descriptions listed in The University's registration is illegal. In order to find out whether your proposed use complies with The University's registration, contact the Data Protection Officer who can be contacted via email at L.K.Fincham@greenwich.ac.uk.

**You must:**

- only use personal data for a University related purpose;
- ensure that the use of University related personal data is restricted to the minimum consistent with the achievement of academic purposes;
- contact the University's Data Protection Officer before conducting any activity which involves the collection, storage or display of personal data through the University's IT facilities.

## 4. Official Secrets Acts

The Official Secrets Acts (1911) establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an unauthorised disclosure by a crown servant or government contractor. They also cover material which has been legitimately disclosed by a crown servant or government contractor on terms requiring it to be kept confidential or in circumstances in which it might reasonably be expected to be treated as confidential. This means that certain information handled by the University's departments may be covered by the provisions of the Acts, particularly if such information concerns a project specifically commissioned by a government office.

**You must:**

- Ensure that any such material is securely stored and avoid displaying it on the University's IT facilities.

## 5. Defamation

Defamation consists of the publication of an untrue statement (which can include an opinion), which adversely affects the reputation of a person or a group of persons. If such a statement is published in a permanent form, as is the case with statements published on the Internet, including messages transmitted by email, an action for libel may be brought against those responsible.

In accordance with the Defamation Act (1996), the University acknowledges the convention of academic freedom, but will take all reasonable care to avoid the dissemination of defamatory material and will act promptly to remove any such material which comes to its attention. Messages which have only one intended recipient may reach a vast audience through the Internet and as a result, the transmission of statements which discredit an identifiable individual or organisation may lead to substantial financial penalties.

**You must:**

- ensure that all published facts are accurate;
- ensure that opinions and views expressed in personal home pages or via bulletin boards do not discredit their subjects in any way which could damage their reputation.

**You must not:**

- place links to bulletin boards which are likely to publish defamatory materials.

Remember that your email communications are publications.

## 6. Obscenity

The University of Greenwich is committed to the prevention of publication through any of the University's IT facilities of any material which it may consider pornographic, excessively violent or which comes with the provisions of the Obscene Publications Act (1959), the Protection of Children Act (1978) or the Criminal Justice Public Order Act (1994). The University will regard any such publications as a very serious matter, which it will not hesitate to report to the law enforcement agencies. Users of the IT facilities are reminded that these are principally for use in connection with academic purposes, therefore any use of the IT equipment to publish or gain access to obscene, pornographic or excessively violent material is inappropriate, and you may be liable to legal proceedings.

**You must not:**

- disseminate, access or encourage access to materials which the institution deems to be obscene, pornographic or excessively violent through the University's IT facilities.

## 7. Communications

The Telecommunications Act (1984) and the Interception of Communications Act (1985) make it illegal to communicate any information of an indecent, obscene or menacing character by a public telecommunications system, or to misuse or tap a telecommunications system.

**You must:**

- ensure that use of institutional voice and data systems, i.e. telephones and networks, is operated in accordance with the provision of these acts.

## 8. Health and Safety

The Health and Safety at work Act (1974) regulates safety in the workplace and is supported by a number of sets of Regulations pertinent to the IT environment, such as the Health and Safety (Display Screen Equipment) Regulations (1992).

**You must:**

- operate in accordance with the University Code of Practice on Display Screen Equipment as detailed in the University Health and Safety Policy. Information is available on the Health and Safety pages. Advice is available from the Safety Unit.

## 9. Computer Evidence

The Police and Criminal Evidence Act (1984) limits the use of certain computer material as evidence in court.
Disclosure of computer held information to the law enforcement agencies may be covered by the provision of this act.

## 10. Discrimination

Both the Sex Discrimination Act (1975) and the Race Relations Act (1976) are guided by the same principle, which is the prevention of unfair discrimination. Placing discriminatory advertisements may in certain circumstances be regarded as a criminal offence under both Acts, which establish fines of up to £5,000 for those found guilty of causing such advertisements to be published. Inciting racial hatred by displaying any written material which is threatening, abusive or insulting is an offence under the Public Order Act (1986). Anyone found guilty of the offence of inciting racial hatred may be liable to imprisonment for up to two years.

In addition, European Union legislation can cover situations where discrimination takes place on the grounds of sexual orientation. Therefore, any material located on or disseminated through the University's IT facilities which may be considered discriminatory or may encourage discrimination on grounds of sex, gender, sexual orientation, race or ethnic origin may be unlawful. Any such material will also be against the University's Equal Opportunities Policy.

**You must not:**

- use the University's IT services to place or disseminate materials which discriminate or encourage discrimination on grounds of sex, gender, sexual orientation, race or ethnic origin.

## 11. Criminal Law

The incitement to commit a crime is a criminal offence in itself, regardless of whether a crime has actually been committed or not. This includes the provision of information via
IT equipment/services which facilitates any of the activities which this code has highlighted as criminal offences.

**You must not:**

- place links to sites which facilitate illegal or improper use;
- place links to sites where copyright protected works, such as computer software, are unlawfully distributed;
- place links to sites which display pornographic materials;
- place links to bulletin boards which are likely to contain discriminatory statements.
- post messages which would be in contempt of court.

## 12. Advertisements and Commercial Activity

The University's IT facilities must not be used for placing or distributing advertisements relating to any course or business other than those promoting the University's teaching and research activities or its own trading operations.

**You must:**

- remember that all advertisements should be 'legal, decent, honest and truthful' and comply with the Code of Practice for Advertisers issued by the Advertising Standards Authority.

## 13. International Law and the Internet

Since there is no international convention on Internet regulation, caution is necessary in considering what law may be applicable. As a basic rule, all users of the University's IT facilities must note that although certain materials may be considered legal in their places of origin, that does not prevent the application of UK law if those materials are considered to be illegal under the law in this country. Similarly, material transmitted world-wide is subject to the law of whichever country it is viewed in.

## 14. Regulation of Investigatory Powers Act 2000 & Lawful Business Practice Regulations

As required by UK legislation, The University of Greenwich, Information and Library Services draws to the attention of all users of the University's Data and Telephones Networks the fact that their communications may be intercepted as permitted by legislation.

The legislation allows an employer and or organisation to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecoms systems. The employer and/or organisation does not need to gain consent before intercepting for these purposes, although it does need to inform staff and students that interceptions may take place.

There is no intention to change practice at The University in the light of the legislation. Nor is there any intention to restrict academic freedom and debate. In the course of their normal duties some staff in Information and Library Services (ILS) do have the authority and indeed duty to carry out certain monitoring activities in order to ensure the correct operation of telecommunication systems. This does not imply that all communications are monitored, just that they may be for the above purposes.

## 15. Rules & Regulations for the Use of The University of Greenwich Information Technology Facilities and Systems

Refer to the full regulations for the use of IT facilities and systems.

## 16. Use of The University of Greenwich IT Systems

In accordance with relevant legislation you are advised that The University has the capability to lawfully monitor and record your activity from any workstation. Current regulations for the acceptable use of The University IT systems are displayed on the The University website. You will be liable for any action deemed necessary by The University of Greenwich as a result of contravening these regulations.

Remember that the use of the University's IT facilities in a way which contravenes the University's regulations may be treated as a disciplinary offence and lead to the penalties established by those regulations.