



**Conduct and Use of Computer Systems and Networks
at Birmingham City University**

-
1. Computer systems and networking facilities shall be used only for work and activity approved by the University.
 2. Access
 - 2.1. No attempt shall be made to access University systems, networks or databases unless legitimate authorisation has been granted.
 3. No attempt shall be made to access the systems and networks of other establishments either within the United Kingdom or elsewhere unless:
 - 3.1. The service required is a public or open access facility.
 - 3.2. Authorisation has been obtained from the system/network service provider.
 4. Usage
 - 4.1. Systems and networks are not to be used for commercial purposes, nor to obtain external funding unless written permission has been obtained from the Director of Corporate Information and Communication Technology (CICT).
 - 4.2. Computer systems and networks shall not be used to engage in any activity liable to cause offence or to obstruct other users of Birmingham City University systems or users elsewhere. This includes the deliberate introduction of viruses into University systems and networks.
 - 4.3. Computer systems and networks may not be used to access, display, print or distribute slanderous, libellous or knowingly untruthful information or material of an illegal nature.

4.4. Copyrights and intellectual property rights must be respected by all Birmingham City University computer system users and used only in accordance with the copyright protection conditions set out below.

5. Protection of Copyright

5.1. The users of any Software, Computer Readable Dataset or Courseware or other similar material, hereafter referred to as "the material" shall:

5.1.1. Ensure that all the requirements of the agreements, contracts and licences under which the material is held by Birmingham City University will be maintained (Copies of the relevant agreements, contracts and licences may be seen by application to the Faculty / Department / Central Service which made the material available);

5.1.2. Adhere to the regulations governing the use of any service involved in the provision of access to the material whether these services are controlled by Birmingham City University or by some other organisation;

5.1.3. Not remove or alter the Copyright Statement on any copies of the material;

5.1.4. Ensure the Security and Confidentiality of any copy released to the user(s) and not make any further copies from it or knowingly permit others to do so, unless permitted to do so under the relevant licence;

5.1.5. Use the material only for purposes defined, and only on computer systems covered, by the agreement, contract or licence;

5.1.6. Only incorporate the material, or part thereof, in any work, program or article produced by the user(s) where this is permitted by the licence or by "Fair Dealing" [\[1\]](#) ;

5.1.7. Only incorporate some part or version of the material in any work produced by the user(s) with the express permission of the Licensor or unless this is permitted under the agreement;

5.1.8. Not reverse engineer or decompile the software products or attempt to do so unless this is explicitly permitted within the terms of the agreement for the use of the material;

5.1.9. Return or destroy all copies of the material at the end of the module / unit / course/year or when requested to do so.

5.2. The unauthorised usage or copying of software in breach of licensing agreements may result in disciplinary action.

5.3. Birmingham City University reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of violation of its licensing agreements.

6. Security

6.1. A password is the personal property and responsibility of the individual to whom it is issued. When issued with a password allowing access to information on systems and networks, a user may not divulge such password information to any other person whomsoever.

6.2. Computer systems and networks which are used to hold personal information which is subject to the Data Protection Act, should not be set up without prior authorisation from the University Secretary and Registrar.

7 The University is not responsible for students own data and students should maintain their own backups. Although, the University will attempt to restore lost data it will not be held responsible if unable to do so.

I understand that failure to comply with the conditions of the University's Information Security Policy and Code of Conduct may result in suspension or withdrawal of access to University computer systems and network facilities and may also render me liable to disciplinary proceedings.

[\[1\]](#) The wording of section 5.1 has been derived from the CHEST (Combined Higher Education Software Team) Code of Conduct (Copyright Acknowledgement). The University has also sought assistance from CHEST in the clarification of the term "Fair Dealing". The following clarification of "Fair Dealing" has been recommended by CHEST and accepted by the University. In providing this clarification CHEST acknowledge their debt to the work by Professor Charles Oppenheim entitled "The Legal and Regulatory Environment for Electronic Information" from which this clarification has been derived.

"Fair Dealing means that an individual, or a friend or colleague of the individual, if sued for infringement, has as his/her defence the argument that he/she made the copy (or copies) of not too substantial a part of the literary work and that the copying did not damage the legitimate interests of the copyright owner. The legislation gives specified purposes where Fair Dealing applies, e.g. private research, commercial research, private study, criticism and book reviewing, reporting current events and educational purposes."