Policy for Use of Computer Systems and Networks at Birmingham City University

1. Introduction

The University provides computer workstations and communications network access to a variety of services which are hosted either by the University or by external agencies via wide area network facilities, e.g. JANET for Internet access. The conditions of use are: Computer systems and networking facilities shall be used only for work and activity approved by the University.

2. Scope

This policy applies to all the following groups of staff and students at Birmingham City University:

Anyone accessing the Birmingham City University **computer network**
Anyone using **computer equipment** that is the property of Birmingham City University
All Birmingham City University **Staff**
All Birmingham City University **Students**
Associate **Staff** (Visiting Lecturers, KTP Associates)
Visitors to the University who are issued with **temporary guest accounts**

3. Access

Access to University information systems, networks or databases is only permitted if the University has authorised this.

No attempt shall be made to access the systems and networks of other establishments either within the United Kingdom or elsewhere unless:

The service required is a public or open access facility.

Authorisation has been obtained from the system/network service provider.

4. Usage

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 Information Technology (IT).

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.

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.

The University has a statutory duty under Section 26(1) of the Counter-Terrorism and Security Act 2015, known as the Prevent duty, to have due regard to prevent people from being drawn into and supporting terrorism.

Computer systems and networks shall not be used to create, download, store or transmit extremism-related material with the intention of supporting or spreading terrorism. The University reserves the right to block or monitor access to such material.

When University networks are used to attempt access to material deemed as potentially breaching University policy a warning challenge page may be presented to the user. The user should only continue when authorisation has been provided for academic related access purposes.

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

The users of any software, computer readable dataset or courseware or other similar material, hereafter referred to as "the material" shall:

- Ensure that all the requirements of the agreements, contracts and licences under which the material is held by the 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);

- 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;

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

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

- 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;
- 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; and

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

The unauthorised usage or copying or distribution of any material including software in breach of licensing agreements may result in disciplinary action and may be reported to the relevant authorities.

The 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

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 must not share the details of this password information with any other person whomsoever.

Computer systems and networks which are used to hold personal information which is subject to the General Data Protection Regulation (GDPR), should not be set up without prior authorisation from the Data Protection Officer (DPO).

[1] The wording of section 4.1 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."

7. Data Backup

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.

Policy Review

This policy will be reviewed on an annual basis, or if there is a change in legal or other business related requirement.

Review Date	Description	Reviewer
11/03/2019	Policy for Use of Computer Systems & Networks at Birmingham City University	IT Security Manager

8. Document History

Version Date	Version	Description	Authors
29/11/2015	1.2	Policy for Use of Computer Systems & Networks at Birmingham City University 1.2 (Prevent Duty inclusion)	IT Security Manager
22/03/2016	1.2	Policy approved and accepted, by University Executive Group (UEG)	UEG approval
10/03/2017	1.3	Reference to firewall challenge page for certain web categories.	IT Security Manager
12/03/2018	1.3	Policy Reviewed – GDPR references added	IT Security Manager