# *General Conditions of Use of Computing and Network Facilities*

| | |
|---|---|
| Document Title | General Conditions of Use of Computing and Network Facilities |
| Edition no. | 1.001 |
| Edition Issue Date | 13/04/2022 |
| Status | Approved |
| Owner | Head of Information Security |
| Unit | IT Services |
| Reference | ITS/InfoSec/SP002 |
| Classification | Open |

## Document Control

| Edition No. | Date | Description | Authors |
|---|---|---|---|
| 1.000 | 06/11/20 | Approved by ISMG | D.Deighton |
| 1.001 | 13/04/22 | Annual review approved by DAGIMAG – resulting in standardised document control and formatting. Data privacy references updated. | T. Lucas |

| Document Identification | |
|---|---|
| Full Title | General Conditions of Use of Computing and Network Facilities |
| Number of Pages | 14 |

# CONTENTS

# 1. INTRODUCTION AND SCOPE

1.1. The provisions of the General Conditions of Use of Computing and Network Facilities (Conditions of Use) are required to be observed by all members of the University, and constitute part of the Conditions of Employment for all Staff.

1.2. These Conditions of Use apply to all Staff, Registered Students and third parties such as collaborating organisation, external contractors, contingent workers, and other contributors, having access to the University's information resources, computing and/or network facilities.

1.3. For the purposes of Ordinances on Student Discipline, these Conditions of Use have the status of a Code of Practice approved by Council (Ordinance 5.5.2 (i) and 5.6.3 (a) (i)).

1.4. Unless otherwise stated, the Conditions of Use apply to all computer users and to all computer equipment and electronic devices that connect with the Universty's wired or wireless data communications networks within or operated by the University and its contractual associates.

1.5. In these Conditions of Use, 'computer', 'computer system' and 'network' mean those that fall into one or more of the following categories:

i. the property of the University or leased/rented to it;
ii. on loan to the University from third parties;
iii. the property of parties to University contracts located within the University, or attached to University computers, computer systems or networks;
iv. used within the University network, irrespective of ownership;
v. used to gain access to University computing and network facilities or systems, irrespective of ownership, and 'computing and/or network resources' includes any such property.

1.6. The University Network includes all communication equipment that transmits information electronically.

1.7. Section 11 defines Conditions of Use particularly relevant to centrally-provided computing and information facilities.

## 2. Data Protection and Privacy

2.1. All members of the University shall comply with the requirements of the Data Protection Act 2018 and the European Union General Data Protection Regulation 2016 (GDPR).

2.2. It is a criminal offence to disclose another individual's personal data, unless the disclosure is with consent or is allowable by one of the specified limited circumstances described in the Act.

2.3. Every person considering the collection, storage or use of personal data must consult the University Data Protection Officer before such collection, storage or use, and must follow the registration procedure adopted by the University. This applies irrespective of the ownership of the computer on which it is intended to store the data.

2.4. All members of the University must comply with the University's Data Protection Policy available at:

https://www.birmingham.ac.uk/documents/university/legal/data-prot-policy.pdf

## 3. Licence Registration and Prevention of Piracy

3.1. All licences concerning hardware and software must be registered with the University and, where appropriate, signed by an authorised signatory within the College, School or Budget Centre.

3.2. Where software has been electronically downloaded from IT Services computer systems requiring authentication, the user must read and comply with the licensing conditions for that software, and the act of downloading indicates acceptance of the licensing conditions pertinent to that software.

3.3. Similarly, where software has been electronically downloaded from elsewhere, such as the Internet, the act of downloading indicates acceptance of the licensing conditions pertinent to that software. Before downloading the software the user must ensure that the licensing conditions have been read and do not conflict with University policy or interests.

3.4. Where software is required by University staff, any legal queries must be referred to Legal Services prior to downloading.

3.5. Registration and signature will occur at Budget Centre or University level depending on the nature of the licence.

3.6. All persons who are licensed to use software or who control access to any computing and/or network resources must take reasonable care to prevent the illicit copying and use of software and documentation.

3.7. No person shall introduce any software or other material requiring a licence for which a valid licence is not in place.

3.8. The University reserves the right for access to be granted to computer audit staff without notice to enable them to check against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported to the Chief Information Officer, who may initiate disciplinary proceedings.

## 4. Commercial Exploitation of Inventions/Intellectual Property

4.1. The commercial exploitation of software or hardware developed using University computing and/or network resources must be referred to the University's Licensing Manager for the proper construction of a Licence, in accordance with the Terms and Conditions of Employment or, for students, in accordance with Regulation 5.3 or other such regulation as may be in force from time to time.

4.2. As specified in Regulation 5.3, copyright in software produced or developed by students will be assigned to the University. Students will, in consideration of such assignments, be afforded the same rights as members of staff as laid down in the University Regulation 'Patents and the Exploitation of Inventions'.

## 5. Security of Computer Information

5.1. All persons responsible for computer equipment of any kind must take adequate precautions to ensure that the physical environment is secure in order to prevent illegal access to equipment and/or theft. The level of physical security must be appropriate to the type and location of the equipment.

5.2. In all instances where sensitive information of any kind is held, irrespective of whether or not Data Protection legislation applies, every effort must be taken to ensure that adequate security measures are in place.

5.3. All information must be stored appropriately to guard against media or mechanical failure. A suitable backup strategy and implementation must be adopted, appropriate to the type and location of the equipment.

5.4. All computer procedures and data are subject to review by the University's Internal and/or External Auditors without notice, and in particular the Internal Auditor is responsible for periodically reviewing adherence to the Information Security and Management Policy and assessing the appropriateness of security measures at a local level.

5.5. Further guidance on security of information and what constitutes reasonable measures appropriate to various types of computer equipment can be found in the University's Information Security and Management Policy and associated Standards, Procedures and Guidance available at:

http://itsecurity.bham.ac.uk

5.6. The University's Information Security and Management Policy is a policy as defined in University regulations and its observance is mandatory for all computer users and for all computer equipment and electronic devices that connect with the Universty's wired or wireless data communications networks within or operated by the University and its contractual associates.

# 6. USE OF SOCIAL MEDIA (BLOGS, WIKIS, FORUMS, EMAIL, ETC.)

## INTRODUCTION AND SCOPE

6.1. Social media offer exciting and innovative ways for the University to expand and elevate its presence and to publicise, enhance and promote the positive activities of the University, its staff and its students. It also provides a medium through which to promote healthy academic debate about controversial subjects or areas of research. The University wholly supports and encourages the use of these media for such purposes by its staff and students subject to the rules outlined in this section and the principles of Academic Freedom as defined in the University's Statutes (Ordinance 3.18).

6.2. This section applies to all forms of social media and, for the avoidance of doubt, includes email. For the purposes of this policy, social media is defined as personally-provided material which is made available through web-based and other means over public and private networks. This would include collaborative projects, wikis, blogs, microblogs, content communities, social networking, virtual worlds, email, and any other media sharing similar characteristics.

6.3. This section applies to the use ("use" or "using", for the purpose of this policy, means providing, posting, uploading, inputting, sending, submitting, commenting or using) of social media when the content (including links) refers to or is related to the University and its activities or the University's staff or students or their activities, whether indirectly or directly. It applies whether a person is using this form of media for University purposes or other purposes, whether a person is acting independently or as part of a group, whether a person is acting on behalf of themselves or on behalf of a group or organisation, whether it is internal or external to the University and whether or not use is authorised or instructed by the University or its members.

## RULES

6.4. The author of the particular form of social media, for example a blog, is solely responsible for its content including the monitoring and checking of comments made on it by others.

6.5. Unless specifically stated, all views and opinions expressed by members of the University (within social media) are the individual's own, and do not reflect any official position of the University of Birmingham. The author must make it clear that they speak on their own behalf. The University will not be responsible for or hold any ownership over the content.

6.6. The University may make an exception to this rule in specific circumstances from time to time by giving written authority to a member of staff to use this form of media for University purposes. Written authority in accordance with this paragraph will be given by the Director of External Relations or nominee.

6.7. Social media content must not refer to or include material or information that:

i. is in conflict with, or jeopardises, the University's interests, is in any way inconsistent with the individual's contractual duties to the University or is in pursuance of unauthorised commercial activities;
ii. may damage the reputation of the University of Birmingham or any of its members;
iii. unfairly criticises, communicates grievance, complaint or discontent, with the University or any of its staff or students;

iv. publicly attacks an individual or organisation, whether or not that individual is a member of the University;

v. may cause offence, upset or harm to another individual or which may constitute bullying or harassment as defined in the University's Harassment and Bullying Policy accessible at:

http://www.equality.bham.ac.uk/policy/Policies/Harassment__Bullying_Policy.pdf

vi. may be defamatory, pornographic, obscene, indecent, offensive, threatening, injurious, illegal or objectionable save where there are Exceptional Circumstances as defined in paragraphs 9.8 i, 9.8 ii or 9.8 iii below;

vii. discriminates or is in breach of the University's Fairness and Diversity Policy accessible at:

http://www.equality.bham.ac.uk/policy/Policies/Fairness__Diversity_Policy.pdf

viii. is confidential to the University, or its members;

ix. constitutes personal data regarding the University of Birmingham's students or staff and/or the publication of which would constitute a breach of the University's Data Protection Policy, accessible at:

https://www.birmingham.ac.uk/documents/university/legal/data-prot-policy.pdf

x. invades an individual's privacy or seeks to impersonate another individual, organisation or entity, whether real or fictitious;

xi. the use of which constitutes a misappropriation or infringement of intellectual property rights;

xii. is in breach of the University's Codes of Practice on Plagiarism accessible at:

http://www.as.bham.ac.uk/legislation/docs/COP_Plagiarism.pdf

for students, and:

https://intranet.birmingham.ac.uk/as/registry/policy/conduct/plagiarism/staffinfo.aspx

for staff.

xiii. endorses or promotes any product, opinion, or cause, or represents personal opinions as endorsed by the University of Birmingham or any of its members, without express written authority from the Director of External Relations or nominee;

xiv. is in breach of the University's Code of Practice for Research, accessible at:

http://www.birmingham.ac.uk/Documents/university/legal/research.pdf

xv. may constitute or incite criminal activity, including but not limited to encouraging terrorism or inviting support for a proscribed terrorist organisation.

6.8. Nothing in this paragraph 6.7 is intended to have the effect of limiting academic freedom as defined in Ordinance 3.18 of the University's Statutes.

## THE USE OF SOCIAL MEDIA IN COURSES OR TEACHING

6.9. Social media provides a useful and creative tool through which to promote and facilitate learning. Any person who uses social media as an educational medium must provide students with clear instructions regarding how they are to use and contribute to it as part of their learning experience, including the application of this Code of Practice.

## MODERATION

6.10. In normal circumstances, the University does not screen, moderate, approve, review or endorse the particular content of social media except where express written authority is given and a written exception is expressly identified by the University.

## COMPLAINTS

6.11. Any complaints or concerns about content on these forms of media may be directed to IT Services via email at itsecurity@contacts.bham.ac.uk .

6.12. The University will respond to claims pertaining to material which is in breach of this policy by immediately removing any content. If the material is on a system to which the University does not have the necessary access to remove the content, the author or information owner will be required to remove it. Failure to remove the material may constitute a disciplinary offence.

6.13. The material may be reposted once the claim is evaluated if not found to be in breach of this Code or general law.

# 7. GENERAL CONDITIONS RELATING TO USE OF SYSTEMS

7.1. Every person who connects to and uses computing and/or network resources owned or controlled by the University shall abide by these Conditions of Use, the University of Birmingham Information Security and Management Policy and associated Standards, as well as satisfying the registration conditions currently in force in respect of the Budget Centre(s) controlling the use of the equipment or associated facilities.

7.2. The provisions in any local Conditions of Use which may be drawn up shall not override the provisions within the General Conditions of Use of Computing and Network Facilities.

University computing and/or network resources are provided for University purposes which means those concerned with undergraduate, postgraduate or other courses, research, personal education, development, administration, or other work authorised by the appropriate Head of Budget Centre. For the avoidance of doubt there are a range of duties that the University is subject to in providing computing and/or network resources that apply. They include but are not limited to the statutory duty "to have due regard to the need to prevent people from being drawn into terrorism."[1]

7.3. Persons connecting to and using computing and/or network resources external to the University must abide by any conditions of use and satisfy any registration conditions imposed by the external agency, such as the JANET UK Acceptable Use Policy.

[1] The Counter Terrorism and Security Act 2015 imposes the 'Prevent' duty on universities.

7.4. All users must act so as to cause as little inconvenience or nuisance to other users as possible and must co-operate with other users to ensure equitable use of shared resources.

# 8. Consent to Intercept and Disclose Data

8.1. All users of University information facilities consent to the examination, monitoring or interception of data, communications or contents of computers by the University for lawful purposes whenever deemed necessary, together with the authority to pass such data to third parties, either as required by law or to fulfil the University's contractual obligations. This work is normally carried out by IT Services, on behalf of the University, in order to meet operational and security needs of the University and related investigatory activities. The lawful purposes may include:

i. Compliance with legal obligation;
ii. Prevention or detection of crime;
iii. Prevention or detection of misconduct;
iv. Investigation of alleged misconduct;
v. Determining if communications are relevant to the University where an employee is absent, for whatever reason;
vi. Establishing whether the use of the email system or the Internet is legitimate and in accordance with the Information Security and Management Policy and its associated Codes of Practice and Standards; or,
vii. Ensuring the effective operation of email and Internet facilities.

# 9. Disciplinary Offences

## General

9.1. Breach of the Conditions of Use is a disciplinary offence which may result in the suspension of access to the University computing and/or network facilities, and further disciplinary proceedings. The following are also disciplinary offences:

i. Incitement to conduct leading to a breach of any provision of these General Conditions of Use shall itself constitute a disciplinary offence;
ii. Failure to comply with relevant local or international law while using or accessing the University computing or networking facilities constitutes a disciplinary offence;
iii. Failure to comply with the conditions of Section 11 (Centrally-Provided Computing Facilities) is also a disciplinary offence.

## Hacking and Viruses

9.2. Any person who wilfully and knowingly gains unauthorised access to a computer system or attempts to disable a computer system commits a disciplinary offence.

9.3. Any person who wilfully, knowingly and without authorisation introduces or attempts to introduce malware or other harmful or nuisance program or file, or to modify or destroy data, programs or supporting documentation residing on, or existing internal or external to a computer, computer system or network commits a disciplinary offence.

9.4. Any person who wilfully, knowingly and without authorisation denies access or attempts to deny access or otherwise interferes with the legitimate operation of computers or computer systems, or uses any University computer, computer system or network to carry out such actions against an external computer system, commits a disciplinary offence.

## INFRINGEMENT OF SOFTWARE LICENCES AND COPYRIGHT

9.5. Any person who wilfully, knowingly and without authorisation uses a computer, computer system or network to access, disclose, publish, take or copy programs data or supporting documentation or any other material or attempts to do so in infringement of intellectual property rights, licence conditions, contractual rights, copyright or confidentiality, wherever the act occurs, commits a disciplinary offence.

9.6. Where the University is rendered liable for any damages from such infringement, the University reserves the right to recover such damages from the person infringing the intellectual property rights, the licence conditions, the contractual rights, copyright or confidentiality.

## OFFENSIVE, INDECENT AND DEFAMATORY MATERIAL AND MESSAGES

### DISCIPLINARY OFFENCES

9.7. Any person who knowingly and without authorisation uses a computer, computer system or network to access or carry out any of the following activities commits a disciplinary offence, unless they are carried out under the provisions stated in "Exceptional Circumstances" below:

i. the creation, storage or transmission of any offensive, obscene or indecent images, data or other material;
ii. the creation, storage or transmission of material which is designed to or is likely to cause annoyance, inconvenience, distress or needless anxiety;
iii. the creation, storage or transmission of defamatory material.
iv. the creation, storage or transmission of terrorist materials prohibited by the Terrorism Act 2006 and/or in contravention of the Counter-Terrorism and Security Act 2015 including the statutory guidance issued pursuant to that Act.

### EXCEPTIONAL CIRCUMSTANCES

9.8. Activities described in the preceding paragraph may be allowable if performed by:

i. Staff specifically designated by the Chief Information Officer to investigate security and other incidents, when their activities are in connection with those incidents.
ii. Staff in the course of their recognised research, provided such research has been considered in advance and approval to access material given before its use. Approval is given by the University's PVC for Research and Knowledge Transfer or by the University Research Governance, Ethics and Integrity Committee in consultation with the relevant Head of College and, where appropriate, the Chief Information Officer.
iii. Students in the course of their supervised research provided such research has been approved in advance by the the University's PVC for Research and Knowledge Transfer or by the University Research Governance, Ethics and

Integrity Committee in consultation with the relevant Head of College and, where appropriate, the Chief Information Officer.

## NETWORK MANAGEMENT AND NETWORK SECURITY

9.9. Any unauthorised person who attempts to monitor traffic on the University Network or any person who attempts to connect an unauthorised device with the intention of monitoring traffic (i.e. eavesdropping) commits a disciplinary offence.

9.10. Any person who knowingly enters a restricted area without authorisation commits a disciplinary offence. For the purposes of this condition, restricted area includes all ducting and other containments or conduits carrying network equipment or cables.

## WILFUL DAMAGE

9.11. Any person who negligently or by any wilful or deliberate act jeopardises the physical integrity of any computing and/or network resource, computer equipment, associated environmental conditioning equipment or physical network and power connections associated accommodation commits a disciplinary offence.

## UNSOLICITED BULK EMAIL

9.12. Any person who sends unsolicited bulk email commits a disciplinary offence, unless it is for official University purposes, or being sent to a mailing list which has been set up with the consent of the list members and the email is consistent with the purpose of the mailing list. Care must be taken to ensure compliance with The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, the Data Protection Act 2018, and other such legislation, as may be enacted from time to time.

## HARASSMENT

9.13. Anyone who uses University computer and computer network facilities in order to carry out or facilitate racial, sexual or any other form of harassment commits a disciplinary offence.

## ACCESS TO DATA

9.14. Anyone who wilfully and knowingly acts to impede a security, disciplinary or operational investigation commits a disciplinary offence. This includes the removal or destruction of relevant data or hardware and/or withholding passwords and encryption keys.

## IMPERSONATION

9.15. Anyone who wilfully, knowingly and without authorisation makes use of a computer, computer system or network in order to impersonate another individual, company or entity, whether real or fictitious, commits a disciplinary offence.

## DISCIPLINARY OFFENCES COMMITTED EXTERNAL TO THE UNIVERSITY

9.16. Any person who wilfully, knowingly and without authorisation uses any computer, computer system or computer network originating in the University or connecting to any University computer, computer system or network to commit any of the actions listed above on a

computer, computer system or network external to the University commits a disciplinary offence.

### FURTHER ACTION

9.17. In addition to any other disciplinary penalties applying to staff and those provided for under Regulations for student discipline, the University reserves the right to:

i. deny all further access to relevant computer, computer systems and computer networks indefinitely or for a defined period of time;
ii. recover all reasonable costs howsoever incurred in investigating and subsequent restitution of computer, computer systems and computer networks resulting from any actions listed above;
iii. refer any possible criminal action to relevant law enforcement agencies or authorities.

## 10. OTHER MATTERS

### UNIVERSITY LIABILITY

10.1. The attention of all members is drawn to the fact that the University will not accept liability for claims made by third parties arising out of the application and use of data, information or results obtained from University computing facilities.

10.2. The University accepts no responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

10.3. Liability will only be accepted by the University for provision to third parties of computing and network resources where a contract to this effect has been negotiated and signed by the Registrar and Secretary.

### ADDITIONAL INFORMATION

10.4. The University Data Protection Officer is the Director of Legal Services.

10.5. Copies of University Regulations are available on the University's web pages.

## 11. CENTRALLY-PROVIDED COMPUTING FACILITIES

### INTRODUCTION AND SCOPE

11.1. This Section applies to any 'computer', 'computer system', 'network', or 'service' under the central management or control of the University through IT Services. All users of such equipment or services are required to abide by the provisions of this Section, and all services covered by this Section are also covered by the terms of this document as a whole.

### REGISTRATION AND USE

11.2. All use of computing and/or network facilities shall be made on the understanding that the use is for University purposes, and every registration of a user and subsequent allocation of

computing and/or network resources shall be made on the understanding that use is solely for the registered user who is allocated the resource. Use shall not be made of resources allocated to another user unless such use is specifically authorised by the Chief Information Officer. This Code of Practice prohibits a person from allowing a third party to make use of computing or network facilities in an unauthorised manner.

11.3. Where the University has specifically agreed that a contract or grant will involve the use of computing and/or network resources without payment, the level of resources to be provided must be agreed beforehand with the Chief Information Officer. Where the University has specifically agreed that a contract or grant will involve payment for the use of computing and/or network resources, the rate of payment must be agreed beforehand with the Director of Finance; and the level of resources with the Chief Information Officer.

11.4. Any other registered use may be the subject of a charge, to be agreed upon prior to registration, the user being personally liable to reimburse such charge. Failure to reimburse by the date specified will lead to the suspension of access for that use, until reimbursement is made.

11.5. Inappropriate use made by or authorised by staff or students of computing and/or network resources may constitute a disciplinary offence and may render the user or authoriser liable inter alia for reimbursement of charges incurred. This includes any activity which wastes significant University resources, including time of computer support staff.

11.6. Where registered users are allocated a computer identifier (such as a userID, password or other form of credentials), they must make all reasonable endeavours to ensure that its confidentiality and integrity are maintained. Registered users must report any suspected breach of such security to IT Services immediately.

## 12. EQUIPMENT

12.1. No computer equipment or associated facilities shall be removed from their location without authorisation. Authorisation must be obtained from the relevant Head of College, School or Budget Centre or their nominee. Users are responsible for and must take reasonable care of any equipment loaned to them and may be required to pay the value of any equipment damaged or not returned.

12.2. Users must not interfere with the use by others of computing and/or network resources. In the event of suspected misuse of facilities by a user, the Chief Information Officer may temporarily suspend use of or access to computing and/or network resources, pending further investigation.

## 13. FURTHER CONDITIONS

13.1. The above conditions may be supplemented from time to time by conditions relating to specific equipment made available to members of the University by special arrangement (e.g. Study Contracts with Computing Suppliers, etc.).