



## UCISA Model Regulations for the Use of Institutional IT Facilities and Systems

[Introduction](#)

[Simplified model code](#)

[Model regulations](#)

[Scope](#)

[Applicable laws and policies](#)

[Infringement](#)

[Use](#)

[Disclaimer](#)

[Appendix A](#)

### Introduction

This document is designed to provide a brief, easily comprehensible set of regulations for the use of computing facilities in HE institutions.

It deliberately omits information which is deemed to be procedural or advisory, on the basis that such information would be available elsewhere and is more likely to be subject to change. It is assumed that the regulations will be subject to an approval process within the institution, and therefore change of the core regulations should be infrequent.

Institutions will need to change the regulations to suit their operation and local requirements. They are therefore strongly advised to consult their legal advisers before publication.


It is also assumed that delivery of these regulations will be online, via a pop-up on first use, requiring acceptance. Therefore, extensive use has been made to links to other documents, both internal and external to the institution. This approach paves the way for brevity, offering further information where required, and enables procedural changes to be managed without the need take the regulations through the approval process.

Where permissions are required for specific activities, it is recommended that contact details for the designated authority are available through a link to a mailbox or web form.

It is suggested that the simplified version of the rules should remain outside the approval process, so that it may be changed as required to draw the attention of new users to issues of the moment.

Consideration should be given to an annual confirmation. This would serve to:

- remind users of the regulations,
- allow topical insertions in the simplified version,
- ensure that any changes in secondary documents can be accepted.



Remote access to services is becoming more common. There is, therefore, a question as to whether the rules of the home institution, or those of the institution from which services are being accessed should be applicable.

In these regulations we have proposed that the regulations of the user's home institution should apply in addition to those of the visited institution, on the basis of the practical consideration that the home institution would be in the better position to apply any disciplinary action.

## UCISA Model I.T. Regulations.

### SIMPLIFIED MODEL CODE

These are the main points of our regulations – you need to confirm that you accept the *full* regulations (below) by clicking the *I accept* (link) button, before you can use our systems.

These rules apply to anyone using any of the University's systems, or any other system you have permission to access as a result of your relationship with the University, in addition to the rules of the visited institution.

---

- You must not try to access any information which you are not permitted to access.
  - You must keep your password secret – you could be in trouble if someone else misuses it.
  - Permission is needed to load new software.
  - Don't introduce, or risk introducing, viruses or anything similar.
  - Avoid interfering with other users or their data or software.
  - You must not send or view anything likely to offend others (e.g. porn, racist or insulting material).
  - We will not be responsible for any loss caused by your use of the computing facilities.
- 

If you break these rules you may be breaking the criminal or civil law and may be liable to disciplinary action. Use of the <institution's> systems may be logged to permit the detection and investigation of infringement of Policies.

---

## UCISA MODEL REGULATIONS

### 1. SCOPE

These regulations apply to:

- All users of services provided by, or for which access is facilitated by, the <institution>.
- Any equipment owned by the <institution>, or equipment for which access has been facilitated by the <institution>.
- Use of systems and services owned by other bodies, access to which has been provided by the <institution>. In such cases, the regulations of both bodies apply. In the event of a conflict of the regulations, the more restrictive takes precedence.

### 2. APPLICABLE LAWS AND POLICIES

Those who use the facilities in the UK are bound by the laws of the UK. A list is given in [Appendix A](#).

### 3. INFRINGEMENT

These regulations apply subject to and in addition to the law. Any infringement of these regulations may also be subject to penalties under civil or criminal law and such law may be invoked by the <institution>. Use of the <institution's> systems may be logged to permit the detection and investigation of infringement of Policies.

### 4. USE

- 4.1. Before using any I.T. facilities, users must be authorised by completing the registration process. See <link to local registration procedures.>
- 4.2. The <institution's> I.T. facilities must be used for the purposes and in the way they were intended to be used. Other use may be allowed as a privilege, not a right.
- 4.3. Use of the <institution's> I.T. facilities must not bring the <institution> into disrepute.
- 4.4. Users must not cause damage to the <institution's> I.T. facilities, nor to any of the accommodation or services associated with them.
- 4.5. Users must adhere to the terms and conditions of all licence agreements relating to I.T. facilities and information which they use including software, equipment, services, documentation and other goods.
- 4.6. Users must not infringe copyright works in any form including software, documents, images, or audio or video recordings.
- 4.7. Users must not load any software onto the I.T. facilities without permission from the <designated authority>.
- 4.8. Users must take all reasonable precautions to ensure that they do not deliberately or recklessly introduce any virus, worm, Trojan or other harmful or nuisance program or file into any I.T. facility. They must not take deliberate action to circumvent any precautions taken or prescribed by the <institution> to prevent this. They must take all reasonable precautions to avoid infection, by, for example, not opening email attachments of unknown source.
- 4.9. Users must not access, delete, amend or disclose the data or data structures of other users without their permission.
- 4.10. Users must not act in any way which puts the security of the I.T. facilities at risk. In particular, user credentials must be kept safe and secure and only used by those authorised to do so. See <security policy>.
- 4.11. Users must not in their use of I.T. facilities exceed the terms of their registration. In particular they must not connect to or attempt to connect to any computing I.T. facility without the permission of the <system owner>. This is known as hacking and is a criminal offence in terms of the Computer Misuse Act 1990, as amended.

- 4.12. Users may be liable for the cost of remedying any damage they cause.
- 4.13. The use of I.T. facilities or information for commercial gain must have the explicit prior permission of the <system owner> and may be subject to charge.
- 4.14. The use of I.T. facilities or information to the substantial advantage of other bodies, such as employers of placement students, must have the explicit prior permission of the <system owner> and may be subject to charge.
- 4.15. Except by prior arrangement users should not carry out activities that will significantly interfere with the work of other users.
- 4.16. Users must not attempt to conceal or falsify the authorship of any electronic communication.
- 4.17. Users must not send unsolicited electronic communications to multiple recipients except where it is a communication authorised by <institution>. Specifically, users must not use the <institution's> facilities to send spam or chain letters. If in doubt, advice must be sought from the <designated authority>.
- 4.18. The creation, display, production or circulation of material which is illegal, likely to cause offence or which promotes terrorism is forbidden. Where access to such material is deemed necessary, permission must be sought from the <designated authority>.
- 4.19. Any infringement of these regulations constitutes a disciplinary offence under the applicable procedure and may be treated as such regardless of legal action.

## **5. DISCLAIMER**

<Institution > makes no representations about the suitability of this service for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions, implied by statute, or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law.

<Institution > shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of the service, or with any delayed access to, or inability to use the service and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of *institution* > in providing this service.

## Appendix A.

### LAW

Applicable laws and policies include the following together with any amendments and any superseding legislation which may be enacted.

- a. [Obscene Publication Act 1959 & 1964 \(link\)](#)
- b. [Protection of Children Act 1978 \(link\)](#)
- c. [Police and Criminal Evidence Act 1984 \(link\)](#)
- d. [Copyright, Designs & Patents Act 1988](#)
- e. [Computer Misuse Act 1990](#)
- f. [Human Rights Act 1998](#)
- g. [Data Protection Act 1998](#)
- h. [Regulation of Investigatory Powers Act 2000](#)
- i. [Freedom of Information Act 2000](#)
- j. [Employment Code of Practice 2002 \(link\)](#)
- k. [Prevention of Terrorism Act 2005](#)
- l. [Terrorism Act 2006](#)
- m. [Police and Justice Act 2006](#)

Applicable policies include:

- a. [JANET Acceptable Use Policy](#)
- b. [Institutional I.T. Security Policy \(link\)](#)
- c. [Institutional Communications Policy \(link\)](#)
- d. [Chest Code of Conduct](#)

This list is not exhaustive and will be subject to change.