University of Plymouth
General rules for the use of University Computing Facilities

This document represents the rules of use for the computing facilities at the University of Plymouth and is accompanied by a set of Guidance Notes that provide further clarification. The rules may be amended from time to time and are located, together with the latest versions of all other IT rules, regulations and guidance notes at http://intranet.plymouth.ac.uk/computing/policies/intranet.htm

These rules apply to any user using any kind of hardware or software for any purpose at the university. They apply even if the equipment is the user's own and even if it is only connected to the University via a network or modem (for example working from home or a remote site) or via a wireless connection.

In addition to these rules there are additional regulations that cover Data Protection, the use of E-mail and Internet Access and World Wide Web services. Users should ensure they have read and understood the relevant rules for these services and comply with them. Individual University service providers may also stipulate additional regulations.

Infringement of any of the rules will result in penalties for the offender, which may include disciplinary action.

Use of the computing facilities indicates that users have read and understood the rules and agree to abide by them.

The University accepts no liability for correctness of results, failure of equipment or consequential loss or damage arising from the use of these facilities.

See Section 2 for a list of the penalties for misuse that may be imposed.
See Section 3 for a list of the appropriate authorities authorised to administer these rules

---

Section 1. General rules of use.

1. Use of computing facilities is restricted to students and staff at the University. Other persons may only make use of the facilities where permission is given by the appropriate authorities.
2. Eating and drinking is prohibited in all computing rooms and open access areas unless there are special circumstances.
3. Computing facilities are provided for the purpose of normal business of the University. Use of facilities for commercial gain must not be undertaken without prior agreement from the appropriate authorities. A restricted (occasional and emergency) level of personal use of the University email and internet is currently permitted, provided it does not conflict with the performance of work duties or studies, incur additional expense for the University, constitute misuse within these rules or restrict the use of the system by other legitimate users. [see also “Rules for the use of University Electronic Mail and Internet Access”, and “Microsoft Live@edu Terms of Use” available at http://intranet.plymouth.ac.uk/computing/policies/intranet.htm].

4. Users may only use the computing facilities under the account name and password allocated to them. Access to or use of any other account is strictly prohibited even if the account owner has given their permission. The sole exception to this is where it is necessary for a support staff member, authorised by the appropriate authorities, to access an account in order to rectify technical problems with that account.

5. Users are expected to take all reasonable precautions to prevent unauthorised use of their account by another person. This includes, but is not limited to: safeguarding their username and password, changing their password on a regular basis and ensuring that they correctly log out of their account when they are not actively using it.

6 All users are directly responsible for the use of their accounts. Any and all actions carried out using that account are the direct responsibility of the account holder. This applies regardless of the person who actually carried them out.

7 Users may only make use of computing resources (hardware, software, data storage) directly permitted to them. Use of, or attempted access to, other resources without prior permission is strictly prohibited. The use of unauthorised wireless access points within the confines of the University is prohibited unless prior permission has been obtained via the support desk. Attempts to modify or otherwise alter the configuration of the facilities provided is also strictly prohibited however, where there is a genuine work requirement, users are allowed to connect additional peripherals to Desktop Leased PCs.

8 Users must not cause any form of damage or interruption, wilful or otherwise, to any part of the University computing resources. This includes, but is not limited to, any and all hardware, software or infrastructure resources or security systems associated with the computing facilities. Attempts to move the location of any Desktop leased PC is strictly prohibited.

9 Users must not knowingly, through use or personal behaviour, cause any annoyance, inconvenience, offence, distress or nuisance to other users of those facilities or individuals within or outside the University. Nor shall they do anything that may bring the University into disrepute.

10 Unauthorised viewing, storage or transmission of offensive or illegal material, including digital pornography, is prohibited. Written authorisation must be obtained from the appropriate authorities if there is a genuine requirement to view, store or transmit such material.

11 Users may only use the hardware and software authorised by the University and must adhere to the terms of licensing agreements as well as the conditions set out in the document "User Acknowledgement of Third Party Rights", available at http://intranet.plymouth.ac.uk/computing/policies/intranet.htm The dissemination, installation or use of any other software or hardware is strictly prohibited unless previously approved by the appropriate authorities. This includes any and all shareware, freeware or other publicly distributed software. The relevant authorities should be contacted to request the inclusion of additional resources. The sole exception to this is where staff, for academic reasons, wish to install properly licensed specialist software on Desktop leased PCs.

12 Any data which falls within the category of "personal data", as defined by the Data Protection Act 1998, must be declared to the appropriate authorities prior to its storage or processing where this is being processed for University business. All

principles of the Act must be complied with and practices relating to the data maintained in accordance with its data protection notification. Where you are processing personal data for personal purposes you will be responsible for this. Users should also be aware of the University policy with regard to the principals and protocols for data exchange as well as the processing of anonymised activity data regarding the use of bibliographic resources. Further detail is available in the accompanying guidance notes to these General Rules.

13 In order to carry out its normal business practice, the University retains the right for staff members, authorized by the appropriate authorities, to monitor network activity for the purpose of ensuring correct operation of computing and telecommunication systems and compliance with acceptable use policies. In addition, authorised staff may access and / or read any information stored on any device connected to the University network. Where necessary access to files may be denied or files may be moved, deleted or copies taken in order to safeguard the integrity of the computing facilities. [see also “Rules for the use of University Electronic Mail and Internet Access”, available at http://intranet.plymouth.ac.uk/computing/policies/intranet.htm].

Additionally users are expected to be aware of, and comply with University policies, JANET Acceptable Use Policy http://www.ja.net/services/publications/policy/aup.html Microsoft Live@edu Terms of Use (if applicable) and all existing UK legislation relevant to the use of the computing facilities.

This includes, but is not limited to:

- Obscene Publications Act 1959 & 1964
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Telecommunications Act 1984
- Interception of Communications Act 1985
- Public Order Act 1984
- Race Relations Act 1976
- Sex Discrimination Act 1975
- Defamation Act 1996
- Disability Discrimination Act 2005
- Special Educational Needs and Disability Act 2001
- Criminal Justice Act 1988
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000 & Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Terrorism Act 2006
- University Code of Practice on Freedom of Speech

Details of how to obtain these documents (in either electronic or paper format) are available from the University library or computing advisory points.

Section 2. Penalties for infringement of the rules of use.

In the event of any breach of the general rules of use, the University reserves the right to withdraw access to any or all computing resources on either a temporary or permanent basis without notice and without giving reasons. In this event the University will take no responsibility for and will not be liable for any adverse effect this may have on a student's ability to complete their programme or a staff member's ability to perform their duties. Depending on the severity of the infringement one or more of the following can additionally be expected to take place.

- Oral or written warning by the appropriate authorities.
- Departmental warning via the course programme manager / equivalent or line manager
- Invocation of the University's Disciplinary Procedure for Students or Disciplinary Procedure for Staff
- Where appropriate incidents will be reported to external authorities. e.g., the Federation Against Software Theft, copyright holders or the Police.

Section 3. Persons authorised to administer these rules.

The term "appropriate authorities" refers to the appropriate University staff responsible for the management of computing facilities whether forming part of the Information and Learning Services department or any other division, faculty or department. The "appropriate authority" will vary according to the location of the facilities being used and be publicised in computing labs and open access areas and available from local service support desks.