GENERAL REGULATIONS
Appendix 8 : Information Technology Regulations

Name of regulation :	Information Technology Regulations
Purpose of regulation :	To outline the main purpose(s) of the University IT facilities for use by University staff, students and other authorised persons (“users”)
Approval for this regulation given by :	Academic Board
Responsibility for its update :	Director of Student and Academic Services
Regulation applies to :	To all students registered on Staffordshire University awards, staff and other authorised persons
Date of Approval :	June 2016
Proposed Date of Review :	May 2017

The main purpose ("Main Purpose") for the provision by the University of Information Technology (IT) facilities is for use in connection with teaching, learning, research, and approved business activities of the University by its staff, students and other authorised persons ("Users"). The University wishes to encourage good and full use to be made of these facilities. With this in mind, for the protection and benefit of the community of Users, any person using IT facilities must abide by these regulations and observe the requirements of the University's IT policies, copies of which can be found on the University Website, www.staffs.ac.uk. To ensure that the IT facilities are not abused the University retains the right to monitor a selection of messages and materials sent across or stored on computers connected to its network and to take any appropriate action if it comes to the University's attention that access to the IT facilities is being abused. This may include referral to the Police in the event of suspected criminal activity.

1. IT hardware must be treated with care and used only in accordance with the proper operating instructions. No equipment shall be used which is labelled out of order. Any apparent fault with hardware should be reported promptly to Information Services personnel, or in the case of equipment based in a Faculty, to the appropriate technical personnel within the Faculty concerned. Equipment must not be used if there is reason to believe that it may not be in safe working order.

2. Users must not by any deliberate or careless act or omission jeopardise or seek to jeopardise the integrity of any IT equipment, and/or its software and/or any information stored within it and/or accessed through it.

3. Users must not access and/or attempt to access any IT equipment, software and/or data which they are not properly authorised to access. In particular, the confidentiality of data belonging to other Users must be respected.

4. Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. Users must not use access codes that belong to someone else. Passwords must be selected and changed as detailed in the University Password Policy, a copy of which can be found at http://www.staffs.ac.uk/assets/password_policy_february2015_tcm44-83668.pdf

5. Users must not use any IT facility for a purpose other than that for which they are authorised. Users must seek advice if they have any doubt about their authority to use any of the IT facilities.

6. The University has a statutory duty 'to have due regard to the need to prevent people from being drawn into terrorism'. The use of IT facilities to support terrorist activity is not permitted and may result in a criminal charge. Access to material promoting terrorism is not permitted, unless this access has been specifically allowed by the University Ethics Committee as part of an approved programme of research.

7. Users must comply with all their legal obligations affecting their use of IT facilities, including Contempt of Court, Copyright, Defamation, Computer Misuse Act, Data Protection Act, Official Secrets Act, Obscene Publications Act, Protection of Children Act and Equality Act 2010. Users are advised to refer to the *Guide to Legislation Relevant to Computer Use*, a copy of which can be found at http://www.staffs.ac.uk/assets/Appendix%2010%20Guide%20to%20Legislation%20Relevant%20to%20Computer%20Use%202016-17_tcm44-91282.pdf

8. The use of any IT equipment for storage and/or transmission of materials which the University considers to be obscene and/or offensive is strictly prohibited. Furthermore, IT facilities must not be used to download pornographic, obscene, excessively violent and/or offensive materials from the Internet.

9. Users must take all reasonable steps to exclude and avoid the spread of malicious software, e.g. viruses, and must co-operate fully with all measures instituted by Information Services to prevent the spread of such software. In particular, Users must not install or execute on a University computer any software obtained from a third party source, unless such software has been previously checked and cleared of the presence of malicious software by Information Services personnel or appropriate technical personnel within their Faculty/Service. Under the Computer Misuse Act 1990 it is an offence to knowingly corrupt a computer program or any of the data stored in the computer system.
    I. Any desktop or laptop computer connected to the University network or wireless network must have up to date antivirus software installed and enabled unless approved in advance as an exception by Information Services.

10. Computer programs on the IT facilities are protected by the law of copyright. The University has the appropriate licences to use these programs. Users must comply with all their legal obligations concerning copyright, and must not copy any software or other data without the prior authorisation from the copyright owner. Such action would be in breach of copyright law. Furthermore Users must comply with any contractual obligations imposed on the University concerning the use of any of the IT equipment or software.

11. Online library learning resources, including datasets and databases, ebooks and ejournals, which are subscribed to by Staffordshire University are protected by copyright and licence agreements. Users who are not covered by these licence agreements must not attempt to use these resources. If in doubt, Users are advised to seek advice at the Information Service desk points.

12. Users must comply with their legal obligations concerning data on living persons, as required by the Data Protection Act 1998 ("the Act"). Student Users must not store personal data on any of the IT facilities without consultation and the prior written approval from the member of the academic staff supervising their work. Any requirement students have to store or process personal data as defined within the Act must be undertaken under the direct supervision of a member of the academic staff.

    Any use of any of the University's IT facilities by Users to store personal data as defined in the Act may need to be registered in accordance with the Act. Consultation should be undertaken with the

University's Data Protection Officer, in such instances and approval obtained in advance.

13. The University permits the use of its IT facilities by Users for personal use, subject to the following limitations:

    I. a level of use that is reasonable and not detrimental to the Main Purpose for which the facilities are provided;

    II. priority must be given to use of resources for the Main Purpose for which they are provided;

    III. personal use must not be of a commercial or profit-making nature, including private consultancy, or for any other form of personal financial gain, unless prior written approval is obtained from the appropriate Dean of Faculty or Director of Service;

    IV. personal use must not be of a nature that competes with the University in business;

    V. personal use must not be connected with any use or application that conflicts with an employee's obligations to Staffordshire University as their employer;

    VI. personal use must not be connected to any purpose or application that conflicts with the University's rules, regulations, policies and procedures;

    VII. personal use must comply with the University's policies and regulations.

    In relation to the personal use of University IT facilities, if Users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance, in the case of members of staff, of their Manager, and in the case of students, of their Course Tutor.

14. Users must not connect any unauthorised equipment to the University network without consultation and the prior written approval from Information Services. If Information Services has reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of the performance of the network detrimental to other Users, then the User must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

15. Users must not set up or operate a server connected to the University network without consultation and the prior written approval from the

Director of Information Services and the appropriate Dean of Faculty or Director of Service.

16. When any of the University's IT facilities are used to access any external network and/or computer facilities, Users must also abide by any additional conditions pertaining to the external facilities, including those imposed by the external providers of such facilities.

17. A number of electronic applications, provided by the University (such as forums, wikis, blogs and chatrooms) are intended to promote academic discussion and debate amongst students. While it is the intention to allow freedom of expression in such applications, the University reserves the right to remove content which it deems to be unsuitable. The views and opinions expressed within such applications do not necessarily represent the views of the University.

18. Any desktop, laptop, tablet or mobile computing devices that are used to access sensitive or confidential data must locked to prevent unauthorised access when the User is away from the device and when not in use.

19. The hard drives of any Laptop devices used to access confidential or sensitive University material must be encrypted. The encryption method must be approved by Information Services.

20. Any loss of University data, distribution of confidential data beyond intended recipients/users, suspected unauthorised access to data, potential misuse of systems, or known vulnerability in a system must be reported to Information Services.

The University views the unauthorised access or interference with any of its IT facilities as an extremely serious disciplinary offence. Any breach of these regulations shall be dealt with in accordance with the disciplinary procedures of the University applicable to the User concerned. In the case of a serious breach, the authorisation of a User to use particular IT facilities may be withdrawn immediately, by a decision of the Director of Information Services, or the appropriate Dean of Faculty or Director of Service.

Information Services reserves the right to disable your IT user account if you do not adhere to the Student Regulations and/or the IT and Library regulations.

Equality issues have been taken into account during the development of this policy and all protected characteristics have been considered as part of the Equality Analysis undertaken.