ICT ACCEPTABLE USE POLICY

1. PURPOSE

1.1. The purpose of this document is to specify the University of Wolverhampton (University) policy on the acceptable use of the information and communication technology (ICT) facilities. The document outlines accepted use and provides sanctions for non-compliance or malicious activity. The policy aims to addresses the dual need to protect the University and its Users' and also to protect the rights of the students, staff, partners, third parties and associates of the University (User).

2. SCOPE

2.1. The University of Wolverhampton ICT facilities are provided for the purposes of the University business. The ICT Acceptable Use Policy is a set of regulations that apply to:

2.2. All users of services provided by, or for which access is facilitated by, the University of Wolverhampton including students, staff, visitors, partners, third parties, contractors and associates.

2.3. Any equipment owned by the University of Wolverhampton, or equipment which access has been facilitated by the University of Wolverhampton.

2.4. Use of systems and services owned by other bodies, access to which has been provided by the University of Wolverhampton. In such cases, the regulations of both bodies apply. In the event of a conflict of the regulations, the more restrictive takes precedence.

3. LEGISLATION AND POLICY

LEGISLATION

3.1. Users of the University facilities are bound by the laws of the UK. An illustrative list is given in the Policy for Using University IT Resources, this is not an exhaustive list and additional policies, legislation and statutory instruments will be added where necessary.

ASSOCIATED POLICIES

3.2. Applicable policies include those listed below. This list is not exhaustive and will be subject to change.

JANET Acceptable Use Policy

Electronic Information Security Policy

Chest Code of Conduct

Policy on Using IT Resources

Regulation 6 Privacy and Electronic Communications (EC Directive) Regulations 2003

4. INFRINGEMENT

4.1. 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 University. Use of the University IT systems will be logged to permit the detection and investigation of criminal, malicious or reckless behaviour which places the IT network at risk, decreases performance or places the reputation of the University at risk.

4.2. Monitoring of emails, internet usage, telephone calls and other ICT will be carried out where appropriate and will comply with regulatory guidelines and legislation including the Regulation of Investigatory Powers Act (RIPA) 2000.

4.3. The University reserves the right to inspect any items of University owned/leased or loaned ICT equipment which is connected to the IT network. Any equipment deemed to be breaching policy or otherwise interfering with the efficient operation of the network may be removed and will not be allowed to reconnect without prior authority from IT Services.

4.4. Infringements of the AUP may be investigated under the University's appropriate disciplinary procedures. Associated sanctions (with approval from appropriate authorities) may include:

- Withdrawal of University ICT facilities
- Seizure of equipment that is in violation of the policy
- Initiation of relevant disciplinary procedure for staff or student
- Expulsion from the University
- Termination of contract

4.5. Where criminal offences are suspected or detected consideration will be given to the question of the appropriateness of referring the matter to external law enforcement agencies for a advice, guidance or prosecution under the relevant criminal law.

5. CONDITIONS OF USE

5.1. The following conditions apply to all Users of University IT facilities. Agreement to the University IT Terms and Conditions indicates acceptance of these provisions:

5.2. Before using any University IT facilities, users must be authorised by completing the University registration process. See the University's registration procedures.

5.3. The University IT facilities must only be used for the intended purpose relevant to the User's role with the University. All use must be for official business or research authorised by the academic supervisor or line manager of the user. Any IT activity outside this remit must be pre-approved with the Director of IT Services; permission for a set activity will be withheld if the proposed activity is deemed to have potential performance issues with the University IT network.

5.4. Use of the University IT facilities must not bring the University of Wolverhampton into disrepute or place the organisational reputation of the University at risk.

5.5. Users must not disrupt, interfere or cause damage to the University IT facilities, nor to any of the accommodation or services associated with them. Users may be liable for the cost of remedying any damage they cause either maliciously or recklessly.

5.6. Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and information which they use including software, equipment, services, documentation and other goods including items loaned to them by the University.

5.7. Users must not infringe copyright works in any form including software, documents and images, audio or video recordings. Sharing of illegally held media in contravention of licensing agreements is a criminal offence and may result in a fine and/or a criminal record.

5.8. Users must not load any software onto the IT facilities without permission from their Dean or Director and in consultation with IT Services.

5.9. 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 IT facility e.g. by not opening email attachments of unknown source. They must not take deliberate action to circumvent any precautions put in place by the University of Wolverhampton to prevent this. Breach of these requirements may be deemed a criminal offence under the Misuse of Computers Act 1990.

5.10. Users must adhere to the provision of the Data Protection Act 1998. Accessing, deleting, amending or disclosing data or data structures of other users without their permission is a criminal offence.

5.11. Staff users must not hold or process any personal data other than that defined in the University's registration under the Data Protection Act 1998. All other users must not hold or process any personal data unless expressly authorised to do so by a Dean, Head or member of University Executive.

5.12. Users must not act in any way which puts the security of the IT facilities at risk. In particular, user names and passwords must be kept safe, secure, and used only by those authorised to do so. Allowing unauthorised persons access to the University IT network by sharing passwords and user names is a criminal offence under the Misuse of Computers Act 1990.

5.13. Users must not disclose their passwords to any other parties. Users must not use login IDs or passwords not belonging to them. Users must not store passwords in mobile devices; university-owned mobile devices (e.g. smart phones) must be protected by PIN number.

5.14. Users connecting personally-owned IT equipment to the University wireless network are advised that it will be subject to security checks and certain pre-requisites before connection is allowed. These are detailed on the IT Services web site. Such use of University networks is at the owner's risk. The university does not accept responsibility for any loss or damage occurring to non-University equipment through the use of its network facilities.

5.15. Users must not establish or operate wireless access points within University premises. Equipment fitted with wireless capability must be used in “infrastructure mode” via a University wireless access point.

5.16. Users must not in their use of IT facilities exceed the terms of their registration. In particular they must not connect to or attempt to connect to any computing IT facility without the permission of the system owner.

5.17. The use of University IT facilities, resources, information or data for commercial gain must have the explicit prior permission of the Director of IT Services and may be subject to charge.

5.18. The use of University IT facilities or information to the substantial advantage of other bodies, such as employers of placement students, must have the explicit prior permission of the Director of IT Services and may be subject to charge.

5.19. Users must not attempt to obfuscate, conceal or falsify the authorship of any electronic communication or device connecting to the University IT network.

5.20. Users must not send unsolicited electronic communications to multiple recipients except where it is a communication authorised by University of Wolverhampton. Specifically, users must not use the University of Wolverhampton’s facilities to send spam or chain letters. If in doubt, advice must be sought from the Director of Marketing and Communication.

5.21. The creation, retention, display, production or circulation of material which is illegal, discriminatory, likely to cause offence or which promotes terrorism is forbidden. Where access to such material is deemed necessary, permission must be sought from the University Secretary.

5.22. The University of Wolverhampton reserves the right at any time and without notice to withdraw or withhold services to users where a breach of

policy, terms or conditions has been identified. This includes blocking devices or equipment from connecting to the University IT network.

5.23. The University of Wolverhampton provides IT accounts for the period that a formal relationship exists between the user and the university. Students can expect provision of an IT account for the duration of their study plus three months following the conferment of the award for which they are studying.

5.24. The university provides Microsoft SkyDrive storage area that comes with your Live@edu email account. Files saved here are stored on Microsoft servers outside the EU. The University takes no responsibility for files stored here; therefore this area should only be used for non-essential data.

5.25. Microsoft provides no guarantees for data stored in SkyDrive and you should note that there is no commitment to guarantee continuous access to your files, therefore loss of the service may deny access to important files at critical times.

5.26. You should be aware that it is both a breach of the SkyDrive contract and University terms and conditions to store any copyright material within this facility. This includes books, music or videos subject to copyright. Breach of these rules may result in your account being terminated by Microsoft without notification and result in the loss of all data within the account, loss of data may well be irretrievable.

5.27. On termination of employment or discontinuance of the relationship with the University the User account will be disabled as soon as practicable. All data/ information held in the Users disabled account will be deleted shortly after the User account has been disabled. The University will conduct regular account deletion procedures to ensure all University IT accounts are valid and authorised; unauthorised accounts will be disabled and removed in accordance with University policy and guidelines.

5.28. Any infringement of these regulations constitutes a disciplinary offence under the applicable procedure and may be treated as such regardless of legal action.

6. USER BEHAVIOUR TRACKING TECHNOLOGIES

6.1. The university will ensure that it complies with the regulations and legal obligations relating to tracking user behaviour whilst using technology to access services and resources from the university.

6.2. Information collected will be used to improve services for you through, for example:

- Enabling a service to recognise your device so you don't have to give the same information several times during one task.
- Recognising that you may already have given a username and password so you don't need to do it for every web page requested.
- Measuring how many people are using services, so they can be made easier to use and there's enough capacity to ensure they are fast

6.3. When the university provides services, it wants to make them easy, useful and reliable. Where services are delivered on the internet, this sometimes involves placing small amounts of information on your device, for example, your computer or mobile phone. These include small files known as Cookies as well as other tracking technologies. They cannot be used to identify you personally but may track your behaviour on our web sites.

6.4. In order to maintain an open and transparent service the University of Wolverhampton will maintain a Cookie Policy web page which will list cookies and other tracking technologies used by the university. Details of the university policy on Cookies and other tracking technologies may be found at Cookie Policy.

6.5. The University of Wolverhampton will carry out a periodic automated review of web pages associated with the university and will evaluate compliance with current legislation and guidance. Web pages reported or found to be non-compliant with the legal requirements for user tracking technologies will be

requested to review and amend their design in order to achieve compliance with the applicable law, regulations or rules.

6.6. Web page owners will be allowed a period of 30 days from receipt of the notification of non-compliance in which to take steps to modify/improve their web page design so that it is legally compliant.

6.7. Failure by the web page owner to address the issues identified in the notification will result in the university seeking reasonable remedies in order to remove the illegal web page from public access.

6.8. Should a non-compliant web page, which the university considers core to its core business activity, be hosted externally to the university network then the web page owner will be requested to resolve the compliance issues within a reasonable period of time. If the web page owner is a member of the university staff, then failure to comply with such a request may render the web page owner liable to internal disciplinary action by the university.

7. DISCLAIMER

7.1. The University of Wolverhampton 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.

7.2. University of Wolverhampton 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.

Approved date	11th July 2012	Author	Stephen Hill IT Security Coordinator
Review date	July 2013	Approved by	Mike Griffiths
Revisions			