IT Acceptable Use Policy and Guidelines

Originator name:	Andy Sherman
Section / Dept:	IT Services
Implementation date:	04/06/2015
Date of next review:	06/06/2018
Related policies:	The University of Surrey's Data Protection policy for handling personal, confidential or sensitive information, Information Security Policy, Social Network Policy, University Ethics Policy
Related Documents:	Your Guide to Using University IT Equipment, Health and Safety Guidance, University of Surrey's general regulations when using the IT facilities,
Policy history:	Updated version of the Acceptable Use Policy For the Use of Computing facilities at the University of Surrey

Version History

Version	Author	Revisions Made	Date
0.1	Andy Sherman	First Draft based on the UCISA Model IT Regulations Toolkit 2014.	21/10/2014
0.2-0.13	Andy Sherman	Various iterations of the draft document	06/11/2014 – 11/05/2014
1.0	Andy Sherman	Reviewed and approved by ISSG	04/06/2015
1.1-1.3	Andy Sherman	Updated to reflect Counter Terrorism Act 2015 requirements	11/08/2015
1.4	Andy Sherman	Reviewed	06/06/2017
1.5	James Newby	Updates to include GDPR references and automated and targeted monitoring	27/07/2017
1.6	Graeme Wilford	Updates to include filtering	3/10/2017
1.7	Graeme Wilford	Security zone variations	25/10/2017

Approval History

Equality Analysis

Version	Reviewed by	Comments	Date
0.9	Equality & Diversity Jo McCarthy-Holland	No negative impact on equality identified	31 March 2015

Committee Sign Off

Version	Committee Name	Date of Sign Off
1.0	Information Security Steering Group	04/06/2015

1	**Introduction**
1.1	**Purpose**
1.1.1	The aim of these regulations is to help ensure that the University of Surrey's IT facilities can be used safely, lawfully and equitably. These rules are in place to protect employees, students and associates of the University of Surrey. Inappropriate use exposes University of Surrey to risks including virus attacks, compromise of network systems and services, and legal issues. The issues covered by these regulations are complex and Appendix 1 forms part of this policy and provides more detailed information of this policy's requirements.
1.2	**Scope**
1.2.1	These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by the University of Surrey.
1.3	**Equality Analysis**
1.3.1	The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.
1.4	**Definitions**
1.4.1	**CHEST agreement** – agreements that have been negotiated by Eduserve for software and online resources on behalf of the UK higher education community **IT Infrastructure** - the underlying hardware, software, networks and facilities used to develop, operate and support the provision of IT. **Malware** - short for malicious software and includes viruses, Trojans and phishing. Malware is used to disrupt computer operation, gather sensitive information or gain unauthorised access to computer systems. **Your Guide to Using University IT Equipment** – the guidance notes that have been implemented with this policy in order to provide additional clarity on its requirements. These form part of this policy and everyone is required to comply with them.
1.5	**Legislative context**
1.5.1	Related legislation includes: • Counter Terrorism and Security Act 2015 • Telecommunications Act 1984 • Copyright, Designs and Patents Act 1988 • Computer Misuse Act 1990 • Data Protection Act 1998 • Freedom of Information Act 2000 • Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) • General Data Protection Regulations (from 25 May 2018) Full list of related legislation is included Appendix A – Guidance Notes
1.6	**Health & Safety Implications**
1.6.1	Guidance and support for use of IT facilities at the University is provided by the health and safety department.

2	**Policy**
2.1	**Principles**
2.1.1	**Overarching governance** It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct. • When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service. • You are bound by the University of Surrey's general regulations when using the IT facilities. • You must abide by the regulations applicable to any other organisation whose services you use or networks you access. • You must comply with all software licence obligations, including CHEST agreement s were these have been used. • A breach of any applicable law or third party regulation will be regarded as a breach of these IT regulations.
2.1.2	**Authority** These regulations are issued under the authority of the Chief Information Officer who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people. • You must not use the IT facilities without the permission of the Chief Information Officer or one of his/her delegates. • You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations
2.1.3	**Intended use** The IT facilities are provided for use in furtherance of the mission of the University of Surrey, for example to support a course of study, research or in connection with your employment by the institution. • Use of these facilities for personal activities (provided that it does not infringe any of the regulations, and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point. • Use of the IT facilities for non-institutional commercial purposes, or for personal gain is prohibited. Any such use requires the explicit approval of the Chief Information Officer or their delegated representative. • Use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST).
2.1.4	**Identity** You must take all reasonable precautions to safeguard any IT credentials (for example, a username and password, email address, smart card or other identity hardware) issued to you. • You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone. • You must not attempt to obtain or use anyone else's credentials. • You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.
2.1.5	**Infrastructure** You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval: • Damaging, reconfiguring or moving equipment; • Loading software on the University of Surrey's equipment other than in approved

	circumstances; • Reconfiguring or connecting equipment to the network other than by approved methods; • Setting up servers or services on the network; • Deliberately or recklessly introducing malware; • Attempting to disrupt or circumvent IT security measures; • Port scanning or testing the effectiveness of security measures.
2.1.6	**Information** When handling personal, confidential or sensitive information: • You must not infringe copyright, or break the terms of licences for software or other material. • You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the University of Surrey. This includes any non-public information that becomes inadvertently or temporarily accessible by you. • You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist in nature. The University of Surrey has procedures to approve and manage valid activities involving such material. • Users should be aware that the data they create on the corporate systems remains the property of The University of Surrey • You must take all reasonable steps to safeguard it and must observe the University of Surrey's Data Protection and Information Security policies and guidance, particularly with regard to removable media, mobile equipment and privately acquired devices or Cloud services. • You must only process personal or sensitive personal data (special category data from May 25 2018) for purposes authorised by the University. • You must always lock your University workstation screen when not in use. The University expects users to adopt a "clear screen" approach to computing equipment issued to them.
2.1.7	**Behaviour** Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Blogger and Twitter. • You must not cause needless offence, concern or annoyance to others. • You should also adhere to the University guidelines on social media. • You must not send spam (unsolicited bulk email). • You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables. • You must not use the IT facilities in a way that interferes with others' valid use of them.
2.1.8	**Monitoring** The University of Surrey monitors and records the use of its IT facilities at both client and infrastructure levels, for the purposes of the effective and efficient planning of the IT facilities. **Automated monitoring** For information security purposes, telephone and computer systems, and any personal use of them, may be continually monitored by automated software at both client and infrastructure levels. Automated monitoring will be carried out only for the purposes of • The effective and efficient planning and operation of the IT facilities; • Detection, mitigation and prevention of cyber security threats;

	Where criminal activity is detected as a consequence of this automated monitoring this may be disclosed to the police where it reveals activity that the University cannot reasonably be expected to ignore. **Targeted monitoring** Non-automated (targeted) monitoring of IT facilities and systems will be carried out if justified by the findings of automated monitoring or to the extent permitted or as required by law and as necessary or justifiable for the following purposes: • Detection and prevention of infringement of these and other policies and regulations • Investigation of alleged misconduct • Handling email and other electronic communications during an employee's extended absence • To find lost messages or to retrieve messages lost due to computer failure • To comply with any legal obligation. Where there are reasonable grounds for suspecting misconduct or for legitimate business reasons, authorisation to conduct targeted monitoring will be granted by; • The VP HR or Senior Information Risk Officer in their absence when the monitoring relates to a current or previous member of staff • The Director of Student Services and Administration or relevant Dean when the monitoring relates to a current or past student. Any monitoring will be proportionate and reasonable steps will be taken to protect staff or student members' private lives. The University will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime and ensuring national security. You must not attempt to monitor use of the IT facilities without explicit authority.
2.1.9	**Filtering** The University of Surrey may block network access to specific websites, network resources and IP addresses; • That are known to propagate malware, facilitate the compromise of sensitive or personal data or otherwise pose an information security threat • That provide or facilitate access to child abuse materials, in line with the University's Child Protection and Adults at Risk Policy • That provide or facilitate access to extremism materials in relation to the University's Prevent duty Staff and students wishing to view extremism material on external websites whose access has been disabled by targeted filtering should refer to the policy for Security Sensitive Research which outlines how access can be granted and any material acquired as a result should be stored. No attempt should be made to circumvent the filters without following the procedures in the Security Sensitive Research policy.
2.1.10	**Infringement** Infringing these regulations may result in sanctions under the institution's disciplinary processes. • Penalties may include withdrawal of services, fines or ultimately expulsion or termination of employment for severe infringements leading to University misconduct. • Materials and evidence may be secured and removed. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached. • The University of Surrey's reserves the right to recover from you, any costs incurred as a result of your infringement. • You must inform IT Services at if you become aware of any infringement of these

	regulations.
2.2	**Procedures**
2.2.1	Detailed procedures covering all University IT equipment and services and appropriate for all circumstances cannot be listed exhaustively in this section. Readers are asked to consult the associated guidance document "Your Guide to Using University IT Equipment" for further guidance on procedures and acceptable usage behaviour. These guidelines form part of this policy and will be updated by IT from time to time.
3	**Governance Requirements**
3.1	**Responsibility**
3.1.1	Overall responsibility for the University's strategic plans for the Acceptable Use Policy for IT Facilities rests with the Chief Information Officer.
3.1.2	All individuals who use University IT equipment must comply with the acceptable use rules. Line managers are responsible for ensuring that staff in their areas are aware of and have access to appropriate guidance and equipment to enable them to comply.
3.1.3	Responsibility for communication of the Acceptable Use Policy for IT Facilities rests with the IT Deputy Director (Service Management).
3.2	**Implementation / Communication Plan**
3.2.1	To be communicated in advance of an individual's anticipated use of Surrey's IT facilities, for example, prior to providing an IT account.
3.3	**Exceptions to this Policy**
3.3.1	**Use of the FEPS Applied Security Lab by authorised users** Exceptions to this policy for the use of the FEPS Applied Security Lab by authorised users is only provided once the 'FEPS Applied Security Lab consent form' has been read, understood, signed and counter signed by all required parties.
3.3.2	**High security zones** Specific systems and data may fall within the scope of a data sharing agreement and/or will expect to comply with a recognised security standard or level of compliance. Security zone policy will document any variations or additional clauses that apply to the use of equipment, services or access to data within the security zone. Acceptable use will inherit such variations or clauses.
3.3.3	**Other exceptions** There are no other exceptions to this policy unless formal documented approval has been provided by the CIO or their appointed deputy.
3.4	**Supporting documentation**
3.4.1	Appendix 1 - Guidance note